LexisNexis® Expert Commentaries

Kyle Bisceglie on

Privilege Issues in E-discovery under New York Law in *Scott v. Beth Israel Medical Center Inc.* *2007 NY Slip Op 27429*

2008 Emerging Issues 2112

In *Scott v. Beth Israel Medical Center Inc.*, 2007 NY Slip Op 27429, 847 N.Y.S.2d 436, 2007 N.Y. Misc. LEXIS 7114, Justice Charles E. Ramos of the New York County Supreme Court, Commercial Division, denied the motion of a hospital administrator, Dr. W. Norman Scott ("Dr. Scott"), for a protective order that would have required Beth Israel Medical Center ("Beth Israel") to return the e-mail correspondence between Dr. Scott and his attorneys that were sent through Beth Israel's e-mail system and presumably found on Beth Israel's server during discovery. The *Beth Israel* Court reasoned that sending the e-mails through the hospital's system with knowledge of its restrictive e-mail policy destroyed any reasonable expectation of confidentiality and, thereby, waived the attorney-client privilege.

Attorney-Client Privilege

The attorney-client privilege is the oldest recognized evidentiary privilege in Anglo-American jurisprudence, dating back to the 1600s, and fosters the open dialog between lawyer and client that is essential for effective representation. *See Delta Financial Corporation v. Morrison*, 13 Misc.3d 441, 444, 820 N.Y.S.2d 745, 748 (N.Y. Sup.Ct. 2006); *Swidler & Berlin v. United States*, 524 U.S. 399, 403 (1998); *United States v. Bilzerian*, 926 F.2d 1285, 1292 (2d Cir. 1991), *cert denied*, 502 U.S. 813, (1991). Its "purpose is to encourage full and frank communication between an attorney and his client and thereby promote broader public interests in the observance of law and the administration of justice." *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981). Thus, the burden of breaching the privilege is particularly onerous. *United States v. David*, 131 F.R.D. 391, 398 (S.D.N.Y. 1990). Nonetheless, privileges are not to be expansively construed, as they "are in derogation of the search for truth," *United States v. Nixon*, 418 U.S. 683, 710, 94 S. Ct. 3090, 41 L. Ed. 2d 1039 (1974), and the attorney-client privilege in particular, "applies only where necessary to achieve its purpose." *Fisher v. United States*, 425 U.S. 391, 403, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976); *see In re Grand Jury Investigation, United States v. Doe*, 399 F.3d 527, 531 (2d Cir. 2005).

In New York, "CPLR 4503(a) states that a privilege exists for confidential communications made between attorney and client in the course of professional employment, and CPLR 3101(b) vests privileged matter with absolute immunity." *Spectrum Sys. Int'l Corp. v. Chemical Bank*, 575 N.Y.S.2d 809, 814, N.E.2d 1055, 1060 (1991). For a "defi-

nition of what is encompassed by the privilege, courts still must look to the common law." *Id.* The burden of establishing the attorney-client privilege, in all its elements, always rests upon the party asserting the privilege. *Untied States v. Schwimmer*, 892 F.2d 237, 244 (2d Cir. 1989). To this end, the party asserting the privilege "must demonstrate that there was: (1) a communication between client and counsel, which (2) was intended to be and was in fact kept confidential, and (3) made for the purpose of obtaining or providing legal advice." *United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 473 (2d Cir. 1996); *See also Rossi v. Blue Shield*, 73 N.Y.2d 588, 593, 540 N.E.2d 703, 542 N.Y.S.2d 508 (1989).

Facts of *Scott v. Beth Israel*

Returning to *Beth Israel*, the extraordinary facts are a lesson for the wary practitioner to avoid. Dr. Scott and, seemingly, his attorneys sent emails over a seven-month period beginning in February of 2004 of such a sensitive legal nature that Dr. Scott and his attorneys later claimed they were all privileged and work-product. All were sent from or to Dr. Scott's employer-issued e-mail, and accordingly, over Beth Israel's e-mail server.

The e-mails were sent during a time when Beth Israel's e-mail policy was in effect. The policy was comprehensive and unambiguous, stating in relevant part:

- "This policy applies to everyone who works for the Medical Center including employees …"
- "All Medical Center computer systems … Internet Access Systems, related technology systems, and the wired or wireless networks that connect them are the property of the Medical Center and should be used for business purpose only."
- "Employees have no personal privacy right in any material created, received, saved or sent using Medial Center communication or computer systems. The Medical Center reserves the right to access and disclose such material at any time without prior notice."

At Beth Israel, Dr. Scott was the Chairman of the Orthopedics Department, worked closely with the Human Resources administrator responsible for disseminating the electronic communication and privacy policy, and, beginning in 2002, required newly hired doctors under his supervision to sign a written form acknowledging their review and fa-

miliarity with the policy. While Dr. Scott never signed such an acknowledgment, he received an employee handbook that contained a brief summary of the policy before enacting the written acknowledgment requirement for his subordinates.

Dr. Scott and his attorneys argued the e-mails in question remained confidential for at least two reasons. First, he claimed to be unaware of Beth Israel's email policy. Second, relying on N.Y. C.P.L.R. 4548 (McKinney 1999), he claimed that the emails were made in confidence.

Not surprisingly, the Court rejected both contentions. As an administrator and one who required written acknowledgment of the policy from his subordinates, he had constructive knowledge of the policy.

As to his confidentiality claim under CPLR 4548, that section provides: "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." The Court reminded us that the modest purpose and effect of CPLR 4548; it simply acknowledges the widespread use of e-mail and that use of e-mail by itself will not abrogate the privileged nature of a communication. However, it also doesn't "absolve an attorney of his or her responsibilities to assess the risk of communicating by e-mail with a client." The holder of the privilege and his or her attorney must protect the confidential communication if they expect it to remain privileged. Dr. Scott's attorneys simply failed to assess the risk of the employer's e-mail policy and, therefore, failed to adequately protect the privilege. In this case, the Court analogized the effect of the employer e-mail policy to having someone watching over its employee's shoulders as he typed.

Confidentiality

The most-critical question for applying the attorney client privilege is whether a communication remains confidential. Because no New York state case had addressed e-mail confidentiality in the attorney-client context, the *Beth Israel* Court looked for guidance to a federal bankruptcy case, *In re Asia Global Crossing, Ltd.* 322 B.R. 247 (S.D.N.Y. 2005). The *Asia Global* court iterated four factors to determine whether an employee's e-mail communications with his or her attorney remains confidential: (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 email, (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?" *Id.*, at 257. If these four factors are met, the attorney-client privilege certainly does not apply. *Asia Global*, 322 B.R., at 258; *Beth Israel*, 847 N.Y.S.2d at 442. Both the *Asia Global* and *Beth Israel* courts characterized these factors as "requirements" but ultimately applied them like "guidelines" intended to determine whether the holder of the privilege intended to keep her communication private. As noted by the New York Court of Appeals, the determination of confidentiality requires an inquiry that is necessarily fact-specific. *Rossi*, 73 N.Y.2d at 593.

Beth Israel suggests that waiver may be found where only some of the *Asia Global* factors are present. Indeed, the *Beth Israel* court focused primarily on the client's intent, finding that C.P.L.R. 4548 makes the third party right of access inapplicable in New York. Additionally, the *Beth Israel* Court devitalized the second *Asia Global* factor, a company's monitoring of its employee's computer use, by equating a policy allowing for monitoring with actual monitoring. 847 N.Y.S.2d at 442.

Analysis of Dr. Scott's and his attorney's intent clearly shows failure to adequately safeguard their e-mails. Dr. Scott's awareness and administration of Beth Israel's e-mail policy and use of the company's e-mail server signify carelessness by the doctor and his attorney sufficiently extreme to vitiate any claim to privilege. Of note to the practitioner, the boilerplate notice included in each e-mail sent from the law firm - that the message "may contain information that is privileged and confidential" – will not save privilege. *Id.*, at 443. This language may preserve a privilege if one exists, but it will not regain privilege once it has been lost.

Analysis of Commonly Encountered Fact Patterns

Since C.P.L.R. 4548 makes third party access to e-mails or employee computers irrelevant in New York, only the remaining three *Asia Global* factors affect the attorney-client privilege. The presence of all three remaining factors to some degree evidences an intent to waive any privilege. 847 N.Y.S.2d at 447. This may not be true outside New York. *See, e.g., Sims v. Lakeside School*, 2007 U.S. Dist. LEXIS 69568 (W.D.Wash. 2007) (holding that e-mails sent from an employer provided computer and an employer provided e-mail account were privileged on public policy grounds). In order to provide guidance to practitioners applying New York, consider the following common scenarios.

Company E-Mail Policy Forbids Personal Use of Company E-Mail and Computers, but the Company Does Not Actively Monitor its Employees. *Beth Israel* overlooked any distinction between policy and action, perhaps because the policy was so clear and unambiguous. A court may be more vigilant in this distinction with an ambiguous or halfhearted policy. Under such circumstance, employees may rightly claim a legitimate expectation of maintaining the confidentiality of e-mails. In *Curto v. Medical World Communications, Inc.*, 388 F. Supp. 2d 101, 2005 U.S. Dist. LEXIS 27088 (E.D.N.Y. 2006), the court upheld the privilege because the company failed to actively monitor. *Curto* involved a tepid employee e-mail policy where "employees understand that [the employer] may use human or automated means to monitor use of computer resources", and an employer that only enforced the policy four times in very limited circumstances. The court noted that the lack of monitoring "created a false sense of security which lulled employees into believing that the policy would not be enforced." *Id.*, at 3 (internal quotations omitted). This lull created a reasonable expectation of privacy that allowed for the maintenance of the attorney-client privilege.

E-Mails are Sent Using a Personal E-Mail Account While Using a Company Computer. In *Curto*, the employee also took reasonable steps to safe guard the communications, including sending the e-mails through her personal AOL account. *Id.* Although the court considered other factors, sending e-mails through a web-based e-mail may protect attorney-client communications in New York, as web-based emails are not typically routed through an employer owned e-mail system. Sending e-mails through a personal e-mail account that is not web-based, such as using Microsoft Exchange to access a personal account, diminishes arguments for privilege.

This result is consistent with other jurisdictions. *See, e.g.*, *National Economic Research Associates, Inc. v. Evans*, 2006 Mass. Super. LEXIS 371 (Mass. Supr. 2006), the employee communicated with his attorney while using a company computer and his personal, web-based and password-protected Yahoo account. The company's internet and e-mail policy that noted that a log may be kept of users' network activities to monitor network usage" did not put the employee on notice that "screen shots" of his e-mails would be logged and accessible by the company.

The Policy Exists but an Employee Claims That They Were Unaware of the Email Policy. As shown in *Beth Israel*, this is in most circumstances a desperation argument at best. If the employee claims ignorance, the court will perform a fact-based analysis and impute actual or constructive knowledge as appropriate. In *Long v. Marubeni America Corp.*, 2006 U.S. Dist. LEXIS 76594 (S.D.N.Y. 2006), the employee claimed that he

did not violate the company's Electronic Communications Policy ("ECP") when he sent e-mails to his attorney from a password-protected and employer-provided e-mail account. The court rejected the employee's claim of ignorance, when he helped prepare the Employee Handbook that contained it. The Court found the e-mails were not privileged. *Id*., at 3.

Another claim of ignorance made by employees that has been rejected by courts is that the employee ignored flash-screen notices that required them to click "yes" on a screen displaying the ECP and a warning that the computer was subject to monitoring. *See United States v. Etkin*, 2008 U.S. Dist. LEXIS 12834 (S.D.N.Y. 2008) (rejecting assertion of marital privilege for e-mails).

Attorney Communicates With Their Client Using Encrypted E-Mails and a Company's E-Mail System. Encrypting e-mails enhances the arguments for the attorney-client privilege. Simply put, it is strong evidence of an employee's desire to maintain confidentiality even if he is at the same time demonstrating his intent to contravene company policy. The confidentiality test focuses on the client's intent to impede their employer's access. *See Baptiste v. Cushman Wakefield, Inc*. 2004 U.S. Dist. LEXIS 2579 (S.D.N.Y. 2004) (finding that e-mail was maintained where the party came into possession of the communication as the result of improper conduct of another). Taking this additional affirmative step shows the intent of both attorney and client to maintain the confidentiality of the communication. Encrypting communications will not stop an employer from hacking the encrypted file, but this additional step would put the employer on par with a thief or eavesdropper, which does not destroy the privilege. *Prink v. Rockefeller Center, Inc.*, 48 N.Y.2d 309, 315 n. 2, 398 N.E.2d 517, 520, 422 N.Y.S.2d 911, 915 (1979). Additionally, adding encryption protects the practitioner by conforming to the opinion of the New York Bar Committee on Professional and Judicial Ethics, which noted that:

> it would be advisable for [practitioners] to advice its clients and prospective clients that the security of communications over the Internet is not equal to that of other forms of communication that are generally accepted as secure, such as the U.S. Mail, express delivery, or the telephone. This technologically developing area has attracted the attention of professional snoopers who can exploit sniffer software and powerful search engines to find messages of interest.

N.Y. Comm. Prof. & Judicial Eth., Formal Op. 1998-2 (1998); *see also* ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

No ruling in New York has directly addressed the issue of an employee who encrypts communications and sends them using his employer's e-mail system in derogation of an express and unambiguous policy preventing such encryption, but *People v. Jiang*. 131 Cal.App.4th 1027, 33 Cal.Rptr.3d 184 (Cal. Ct. App. 2005) provides the most germane law to analyze this issue. In *Jiang*, the prosecution attempted to discover files prepared by the defendant for his lawyer that pertained to a criminal trial and were protected by individual passwords created by the defendant. The company's computer policy stated: "I have no expectation of privacy in any property owned by the company. . . . I further understand that such property, including voicemail and electronic mail, is subject to inspection by Company personnel at any time." *Id.*, at 197-98. This policy is not iron-clad and the court noted that the policy did not bar employees from using company computers for personal matters. Accordingly, the court's analysis turned on whether the employee took best efforts to preserve the privilege and not on the specific wording of the policy. The court found that creating password-protection and placing the data in a folder called "Attorney" for the explicit purpose of protecting it from disclosure satisfied the burden imposed on the privilege claimant. *Id*, at 203. Adding this additional level of security does not guarantee the privilege, but it is recommended if e-mails are to be sent using a company's e-mail system.

A Client Communicates With His Attorney Via a Password-Protected, Employer-Provided E-Mail Account. Using a password-protected, employer-provided e-mail will not protect privileged information from disclosure. In *Long v. Marubeni America Corporation*, 2006 U.S. Dist. LEXIS 76594 (S.D.N.Y. 2006), the Court found that that employees did not maintain confidentiality when they elected to use work computers to communicate with their attorney. The employees were aware of their employer's electronic communications policy that allowed monitoring of all e-mails and prohibited the use of the system for personal purposes. The court rejected the employees claim that using private password-protected e-mail accounts to communicate with their attorney was sufficient to maintain confidentiality. *Id.*, at 3.

If None of the *Asia Global* Factors are Satisfied

If none of the factors can be satisfied, the communications are privileged. *See In re Asia Global*, 322 B.R. at 259-61. In *Global*, the record before the court was insufficient to conclude that Asia Global employee's use of the e-mail system waived the attorney-

client privilege. *Id.*, at 261. The Court was unable to determine if the company had an electronic communications policy or if the company monitored its employee's computer use. Since the court was only able to determine that the employees sent e-mails and they were stored on the company server, the court could not find waiver of the attorney-client privilege. *Id.*, at 253.

Recommendations

The consequences of waiver can be far-reaching extending not only to disputes between employer and employee but to all litigants who use their employer's e-mail system improperly to communicate with their attorney for non-work related matters.

Practitioners Should Counsel Employers to

(1) establish or review their electronic communications and computer usage policies to ensure they clearly notify employees that their private use of the employer provided system is monitored;

(2) introduce click-through screens that display their electronic communications policy whenever an employee logs in;

(3) include an electronic communication policy in all employee handbooks distributed to employees and require all employees to give written notification that they are aware of, and will comply with, the policy;

(4) enforce electronic communications policies by actually monitoring employee Internet usage and e-mails on a regular basis.

Practitioners Should Counsel Their Clients to

(1) *never* communicate with personal attorneys over an employer provided e-mail address;

(2) use a web-based, password-protected e-mail, such as g-mail or yahoo, if they must communicate with personal attorneys while using a company issued computer;

(3) employ encryption software if forced to communicate with their clients to their work e-mails. (Preferably, an employee should never communicate with their attorney while at work.)

Practitioners Should Consider the Following for Themselves

(1) train junior attorneys at your firm about the perils of communicating with a client by e-mail;

(2) avoid use of e-mail all-together for certain peculiarly sensitive communications;

(3) insert in the subject line "Privileged attorney client privilege and confidential work product" or facsimile. This won't "save a privilege" but might ensure the document is not inadvertently turned over during document production;

(4) demand disclosure of the domain name addresses for e-mails identified on a privilege log. Where the litigant uses a work e-mail address to litigate a non-work matter including personal and unrelated business claims, seek discovery (including subpoena to the employer if applicable) of the litigant's employer's e-mail policy and practices to undertake the *Beth Israel* analysis.

For additional discussion of Privilege Issues in E-discovery under New York Law, *see* Marjorie A. Shields, *Application of Attorney-Client Privilege to Electronic Documents*, 26 A.L.R. 287 (2007); John Gergacz, *Employees' Use of Employer Computers to Communicate with Their Own Attorneys and the Attorney-Client Privilege*, 10 Comp. L. Rev. & Tech. J. 269, 276 (2007) (most thorough analysis of e-mail and attorney-client privilege); Elise M. Bloom, *Ownership of E-mail is Not Clear Employees Retain Some Rights Over Confidential Writing Sent From Work*, 30 Nat'l L.J. 18, S1 (2008) (Analysis of *In re Asia Global* factors); Paul H. Aloe, *'Scott' Is Dire Warning About E-mail Communications*, 238 N.Y. L.J. 4 (2007) (criticism of and arguments against *Beth Israel*); John K. Villa, *Emails Between Employees and Their Attorneys Using Company Computers: Are They Still Privileged?*, 26 NO. 3 ACC Docket 102 (2008) (additional counter arguments against *Beth Israel* and practice suggestions); Audrey Jordan, Note, *Does Unencrypted E-mail Protect Client Confidentiality?*, 27 Am. J. Trial Advoc. 623 (Spring 2004) (discussion of encryption).

For application of Privilege Issues in E-discovery outside of New York, *see City of Reno v. Reno Police Protective Ass'n*, 118 Nev. 889, 59 P.3d 1212 (Nev., 2002) (government documents sent over e-mail are still privileged because the disclosure policy was not meant to effect them); *Geer v. Gilman Corp*, 2007 U.S. Dist. LEXIS 38852 (D.Conn. 2007) (attorney-client communications remained privileged when reviewed by boyfriend because plaintiff requested they remain confidential and took active steps to ensure confidentiality); *Ball v. Versar, Inc.*, 2005 U.S. Dist. LEXIS 24351 (S.D.Ind. 2005) (finding waiver of privilege extended to all work *and home* computer systems known to have been used by plaintiff).

About the Author. Kyle C. Bisceglie, a Partner at Olshan Grundman Frome Rosenzweig & Wolosky LLP in New York City, counsels corporations, partnerships, and individuals with respect to complex commercial litigation, Alternative Dispute Resolution ("ADR"), contracts, business advice and litigation avoidance. He has tried numerous cases without loss and has been involved in litigations, arbitrations, mediations and settlement negotiations. He also serves as general counsel to various entrepreneurial ventures and businesses in technology infrastructure, advertising, event production, dental and medical instruments, insurance, chemical distribution, fashion and consulting fields. Mr. Bisceglie has complex litigation experience in a variety areas including commercial, financial, insurance, employment, race and sex discrimination, harassment and retaliation, copyright and trademark, defamation, and business tort. He has participated in the investigation of the worldwide derivatives trading practices of a New York based merchant bank, representation of US policyholders in the largest insurance insolvency in North American history, and coordination of negotiation over and litigation for the transfer of a major beverage and spirit company's most valuable brand. Mr. Bisceglie also spent five years in the litigation department of Cadwalader, Wickersham and Taft; two years trying cases as an assistant prosecutor; and one year as a law clerk to Judge Alfred M. Wolin, United States District Court for the District of New Jersey. He can be reached by phone at 212-451-2207 or by email at Kbisceglie@olshanlaw.com.