UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

41st Annual Page Keeton
Civil Litigation Conference

November 2-3, 2017

Monitoring and Monitored Conversations

Steven Goode

University of Texas School of Law
Austin, TX

sgoode@law.utexas.edu
512.232.1331

Monitoring and Monitored Conversations:
The Danger of Communicating with Clients by Email

One of the common ways by which lawyers and clients may communicate may not be privileged. In the last dozen years, a substantial number of cases have addressed the privileged status of lawyer-client email communications where the client is either using an employer's equipment (e.g., a company laptop) or an employer's email system.[1] Many of the cases hold that the communications are not privileged.

The leading case is *In re Asia Global Crossing, Ltd*.[2] The court there focused on whether the communications were confidential. The Texas Rules of Evidence define the confidentiality of a communication for purposes of the attorney-client privilege in terms of intent to disclose to third persons.[3] The federal rules, however, lack a codified attorney-client privilege. In *Asia Global*, the court stated that "[c]onfidentiality has both a subjective and objective component; the communication must be given in confidence, and the client must reasonably understand it to be so given."[4] The court then held that the privileged status of the emailed attorney-client communications depended on whether there existed a reasonable expectation of privacy. To determine this, the court set forth a four-factor test:

> In general, a court should consider four factors: (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-mails7, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

Numerous courts have applied this test.[5] As should be expected with multi-factor tests, courts do not always apply the *Asia Global* test in a manner that is easy to predict. A reading of the cases indicates that the single most important factors are the clarity of the company policy regarding the use of email and its right to inspect the employee's computer or email. *In re Royce Homes, LP,*[6] a Texas bankruptcy case, illustrates this. The company's Employee Handbook stated,

---

1 See generally Fischer, Big Boss is Watching: Circumstances Under Which Employees Waive the Attorney-Client Privilege By Using E-Mail at Work, 12 Colo. Tech. L.J. 365 (2014); Levy, Employee E-Mails and the Concept of Earning the Privilege, 9 I/S: J. L. & Policy for Info. Soc'y 245 (2013); DeLisi, Employer Monitoring of Employee Email: Attorney-Client Privilege Should Attach to Communications That the Client Believed Were Confidential, 81 Fordham L. Rev. 3521 (2013).

2 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

3 Tex. R. Evid. 503(a)(3) defines a confidential communication in terms of the intent to disclose to third persons "other than those to whom disclosure is made (1) to further the rendition of professional legal services . . . or (2) reasonably necessary to transmit the communication."

4 322 B.R. at 255.

5 As of October 2017, Westlaw lists 60 cases that cite *Asia Global*.

6 449 B.R. 709 (Bankr. S.D. Tex. 2011).

"Employees are NOT to disseminate any confidential information over the company's system."[7] The court had no problem finding that the attorney-client privilege was inapplicable. In *Bingham v. Baycare Health System*, a Florida federal court recently concluded that "it appears that the majority of courts have found that an employee has no reasonable expectation of privacy in workplace e-mails when the employer's policy limits personal use or otherwise restricts employees' use of its system and notifies employees of its policy."[8]

Ambiguous (or no clearly articulated) policies are likely to lead to the opposite conclusion. In *Stengart v. Loving Care Agency, Inc.,*[9] another widely-cited case, the client used a company laptop to communicate with his attorney through a personal, password-protected Yahoo email account. The company's policy stated that the company may access "all matters on the company's media systems" and that emails are "considered part of the company's business . . . records." But the company policy neither defined "media systems" nor expressly addressed personal accounts. The court, therefore, found that the company policy was ambiguous as to whether personal emails were company property.[10]

But clarity or ambiguity does not also resolve the issue. A privilege proponent may overcome a relatively clear policy,[11] and a privilege opponent may overcome an ambiguous policy.[12]

---

[7] Id. at 738. See, e.g., Goldstein v. Colborne Acquisition Co., LLC, 873 F. Supp. 2d 932 (N.D. Ill. 2012) (policy stated "all messages . . . are Colbourne records"); United States v. Finazzo, 2013 WL 619572 (E.D.N.Y. Feb. 19, 2013) ("[y]ou should have no expectation of privacy" and "[a]ll information . . . may be monitored, accessed, deleted, or disclosed at any time without your permission"); In re Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 282 (Del. Ch. 2013) (employees "should assume files and Internet messages are open to access by IMS staff"); Farris v. Int'l Paper Inc., 2014 WL 6473273, at *1 (C.D. Cal. Nov. 17, 2014) ("employees' activities on company computers are not private."); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 442 (N.Y. Sup. Ct. 2007).

[8] 2016 WL 3917513 *4 (M.D. Fla. 2016). The court cites numerous cases. Anyone looking for a quick entry to the case law on this issue should consult this opinion.

[9] 990 A.3d 650 (N.J. 2010).

[10] Id. at 659. See, e.g., Maxtena, Inc. v. Marks, 2013 WL 1316386 (D. Md. Mar. 26, 2013) (no evidence of company technology policy or that company monitored emails); United States v. Hudson, 2013 WL 4768084 (D. Kan. Sept. 5, 2013) (policy did not ban personal use of workplace equipment or specifically mention that technology use would be monitored); Ferrer v. Stahlwerk Annahutte Max Aicher GMBH & Co. KG, 2014 WL 2593519 (N.J. Super. Ct. Ch. Div. June 2, 2014) (company "never enacted *any* policy regarding computer access or email accounts"); Convertino v. U.S. Dep't of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (citing the fact that the policy did not ban personal use as one reason the employee's expectation of privacy was reasonable); United States v. Hatfield, 2009 WL 3806300 (E.D.N.Y. Nov. 13, 2009) (counting the fact that the policy did not "expressly prohibit" personal use in the employee's favor even though the policy stated that employees were "expect[ed]" to use company computers "solely for business purposes").

[11] E.g., Pensacola Firefighters' Relief Pension Fund Bd. of Trustees v. Merrill Lynch Pierce Fenner & Smith, Inc., 2011 WL 3512180 (N.D. Fla. July 7, 2011) (although Merrill Lynch's email policy stated "E-mail is not confidential; employees have no right to privacy for any e-mail messages transmitted through the firm e-mail system," court found, "it is objectively reasonable for an employee to believe his frequent inter-office and extra-office email communications between Merrill's counsel, employee counsel, accountants, and other people necessary to effect a common litigation strategy [are private] when Merrill's 'First Vice President, Assistant General Counsel' endorsed and participated in the communications.").

[12] E.g., Hanson v. First Nat. Bank, 2011 WL 5201430 (S.D.W. Va. Oct. 31, 2011) (no privilege even though policy stated "[i]ncidental and occasional personal use of company computers and our voice mail and electronic mail systems

Title search: Monitoring and Monitored Conversations

Also available as part of the eCourse
2017 Page Keeton Civil Litigation eConference

First appeared as part of the conference materials for the
41st Annual Page Keeton Civil Litigation Conference session
"Monitoring and Monitored Conversations"