I Can Read All My Employees' Emails, Right? Not Necessarily – Privilege May Limit A Company's Access

Julie Rodriguez Aldort
Robert Catmull

IT'S 3:00 PM ON A MONDAY AND AN employee needs a break from work. So the employee takes five minutes and sends some personal emails from the company email account. People usually believe these emails are private conversations. But in the workplace, they may be more public than one would expect and this can become an especially tricky issue when those communications are with the employee's attorney.

It is now commonplace for employers to have a technology policy that permits the employer to monitor an employee's inbox. Nevertheless, employees exchange what they believe to be privileged communications with their attorney over their work email. Those emails can be captured by discovery requests in litigation against the company, in subpoenas on the company by third parties or, more directly, in affirmative searches by the company for helpful information in its disputes against the employee. As a result, there is an increasing amount of litigation over who may legitimately access what would otherwise be privileged communications between an employee and her attorney.

I. Courts Typically Apply A Multi-Factor Test To Assess Whether An Employee Reasonably Believed Her Emails Would Remain Confidential.

Normally, a confidential communication loses its privileged status when either the attorney or client exposes the communication to a third party. An employer's right of access would seem to be the type of third party exposure that would extinguish privilege. However, courts addressing the issue have generally applied a more complex analysis, assessing whether an employee could reasonably believe her communication would remain confidential. The most common approach was articulated by the federal district court in New York in *In re Asia Global Crossing, Ltd.,* 322 B.R. 247 (Bankr. S.D.N.Y. 2005). In *Asia Global*, the employees sent emails over the work server to their personal attorneys. The company eventually filed for bankruptcy, and during discovery, the company's attorney subpoenaed emails related to employees' transactions. The employees asserted that these emails were privileged, and the court agreed, holding that merely using a work email account for attorney-client communication does not destroy privilege. *Id.* at 261–62. In its analysis, the court articulated four factors to consider when assessing whether the employee reasonably could expect the email to her attorney to remain 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 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?

Id. at 257. Answering yes to any of these questions does not necessarily defeat a claim of privilege, although one factor may weigh more heavily in the analysis than the others depending upon the particular issue at hand. *See id.* at 258 (comparing *Garrity v. John Hancock Mutual Life Ins. Co.,* No. Civ. A. 00–12143–RWZ, 2002 WL 974676, at *1–2 (D. Mass. May 7, 2002) ("no reasonable expectation of privacy where, despite the fact that the employee created a password to limit access, the company periodically reminded employees that the company e-mail policy prohibited certain uses, the e-mail system belonged to the company, although the company did not intentionally inspect e-mail usage, it might do so where there were business or legal reasons to do so, and the plaintiff assumed her e-mails might be forwarded to others"), with *Leventhal v. Knapek,* 266 F.3d 64, 74 (2d Cir. 2001) ("employee

had reasonable expectation of privacy in contents of workplace computer where the employee had a private office and exclusive use of his desk, filing cabinets and computers, the employer did not have a general practice of routinely searching office computers, and had not 'placed [the plaintiff] on notice that he should have no expectation of privacy in the contents of his office computer'")). As a general rule, however, the more affirmative responses, the more likely that the communications will *not* be found privileged.

The federal court for the Northern District of California applied the *Asia Global* factors to its analysis of whether an employee had waived privilege in work emails. *See, e.g., In re High-Tech Employee Antitrust Litig.,* No. 11-CV-2509-LHK-PSG, 2013 WL 772668 (N.D. Cal. Feb. 28, 2013). In *High-Tech,* two factors favored retaining privilege and two factors favored waiving privilege. The court ultimately held that the emails retained their confidentiality because of the importance of the attorney-client privilege and the lack of evidence that the employer in fact monitored emails. *Id.* Similarly, a California state appellate court, applying the *Asia Global* factors, held that an employee has an objectively reasonable expectation of confidentiality when the employee puts privileged documents in a password-protected folder—even if that folder is maintained on a work computer. *People v. Jiang,* 33 Cal. Rptr. 3d 184, 207–08 (Cal. Ct. App. 2005).

The federal district court for the Western District of Washington, however, has preferred a strict "no-waiver" rule over the *Asia Global* approach. *Sims v. Lakeside School,* No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007). Though the court ruled that the employee had no reasonable expectations of privacy in emails he sent and received on his email account provided by his employer, the court nevertheless held that web-based emails generated by the employee are protected by privilege, citing public policy concerns and the importance of encouraging free and candid communications between clients and their attorneys. The Washington federal court appears to be in the minority, as even Washington state courts seem to engage in a more nuanced analysis akin to the *Global Asia* test. *See, e.g., Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1110 (W.D. Wash. 2011) (citing Washington state law and stating that a non-waiver rule contradicts Washington's policy).

II. My Employee Wrote "Privileged" Emails at Work. Now What?

If the employer wants to use employee "privileged" emails itself, there are several steps an employer can take to increase the likelihood of full access to its employees' emails: (1) create a clear policy explaining that the employer will review its employees' emails and the employees should expect no privacy in those emails; (2) consistently apply this policy; and (3) keep a paper trail evidencing the employees' acceptance of the technology policy. Still, even if the employer takes these precautions, a court may uphold a claim of privilege and prevent the employer from disclosing or using the emails against the employee's wishes.

If a third-party seeks the employee emails through a subpoena, caution is advised. A Delaware court recently cautioned that a presumption of privilege might be even stronger where a third-party serves the employer with a subpoena for its employee's emails. *See In re Info. Mgmt. Servs., Inc. Derivative Litig.,* 81 A.3d 278, 296 (Del. Ch. 2013). This is not to say that an outsider can never access personal emails sent over a work server. But because of this presumption, the employer should think twice before simply handing over all of an employee's emails. A prudent course would be to notify the employee and her personal attorney of the third-party's request or to seek judicial review before providing privileged emails. *See, e.g., Stengart v. Loving Care Agency, Inc.,* 201 N.J. 300, 326, (N.J. 2010) (holding that the employer's counsel violated ethics rules by failing to alert the employee's attorneys that it possessed the employee's potentially privileged emails before reading them).

Julie Rodriguez Aldort is a partner at Butler Rubin Saltarelli & Boyd LLP, a national litigation boutique based in Chicago, where she arbitrates and litigates complex commerical disputes, including reinsurance. Robert Catmull is a third-year student at the University of Chicago Law School and was a summer associate at Butler Rubin. The views expressed are personal to the authors.
