KING & SPALDING

Client Alert

Special Matters & Government Investigations Practice Group

June 8, 2017

Attorney-Client Privilege and Corporate E-Mail: Navigating the Morass of Personal Communications in Investigations

Experienced practitioners know that the purpose of the attorney-client privilege is to protect the confidentiality of client communications. Thus, as company policies that allow monitoring of emails or provide third party access may undermine any reasonable expectation of confidentiality, they may determine whether the privilege applies to personal communications sent on a company server. While many courts have rejected privilege claims for employee-personal counsel communications sent through the company's email system on this basis, the law in this area continues to develop. Accordingly, to be prepared, counsel should familiarize themselves with the current law in their jurisdiction.

The evolving nature of this analysis was recently highlighted in *Peerenboom v. Marvel Entertainment LLC,*[i] where the Supreme Court of New York held that emails sent to personal counsel via the company's computer system were not subject to the attorney-client privilege, but could be subject to the attorney work product privilege.

The Supreme Court of New York's Decision in Perenboom

In *Perenboom*, Isaac Perlmutter, Marvel's CEO, sought a protective order barring Marvel from producing certain personal emails in response to a civil trial subpoena because the emails were between him and his personal attorney, and between him and his wife. The party who had served the subpoena contended that Marvel's computer usage handbook allowed the company to monitor emails and that monitoring established a privilege waiver. The Supreme Court disagreed and upheld Perlmutter's claim of marital privilege for communications with his spouse, but denied his other privilege claims. In considering Perlmutter's appeal, the appellate division applied the four-factor test from *In re Asia Global Crossing, Ltd.*,[ii] a 2005 landmark privilege decision in this area. While the key holding of *Asia Global* was that the attorney-client privilege is not necessarily waived when an employee corresponds with personal counsel over a company's email system, the most important aspect of *Asia Global* was its four-factor analysis.

That analysis, derived from Fourth Amendment reasonable expectation of privacy cases, applied four factors to determine if content is privileged: 1) whether corporate policy bans personal or other objectionable

For more information, contact:

Alec Koch
+1 202 626 8982
akoch@kslaw.com

Kevin Dinan
+1 202 661 7916
kdinan@kslaw.com

Christopher Burris
+1 404 572 4708
cburris@kslaw.com

Katherine Kirkpatrick
+1 212 556 2113
kkirkpatrick@kslaw.com

King & Spalding
Washington, DC
1700 Pennsylvania Avenue NW
Washington, D.C. 20006
Tel: +1 202 737 0500
Fax: +1 202 626 3737

www.kslaw.com

use; 2) whether the company monitors employee computer or email usage; 3) whether third parties have a right of access to the computers or emails; and 4) whether the employee received notice of, or was aware of, the use and monitoring polices.

Ultimately, in *Perenboom*, Perlmutter's senior status worked against him on appeal. In affirming waiver of the attorney-client privilege, the court ruled that as Marvel's CEO, Perlmutter was, at a minimum, constructively on notice of the company's email policy. While the policy allowed receipt of personal emails, it also permitted the company to assert ownership over all emails on its system by reserving the right to audit the networks and systems, and by reserving the right to access, review, and disclose to third parties any emails on the system. However, given the lack of evidence that Marvel viewed Perlmutter's emails or disclosed them to a third party, the court held there was no waiver of the attorney work product privilege – a decision consistent with the general rule that the attorney work product privilege will only be waived if the disclosure is to an adversary or to one who makes it more likely the information will be disclosed to an adversary.

Key Takeaways

What does this mean for counsel navigating potential privilege claims in connection with internal investigations? While the *Peerenboom* decision demonstrates that the four factor *Asia Global* test is still applied by courts, it also shows that courts may reach different conclusions in how they apply those factors. Those conclusions may depend, for example, upon the relationship of the email communications between the employee and personal counsel, and company matters. It is also possible that a court may be more inclined to find an expectation of confidentiality for communications wholly unrelated to company business, especially if sent under circumstances where it was unclear whether company policy allowed the monitoring or retrieval of such correspondence.[iii] *Peerenboom* also shows that when it comes to the employees' knowledge of use and monitoring policies, courts may be more inclined to impose constructive notice upon senior management, even when lack of actual notice can be shown.

Further, more than ten years after *Asia Global*¸ most large entities and public companies have updated their policies to account for the need to have access to emails on the company's systems, including rights to review and audit almost all emails. But attorneys conducting internal investigations should be cognizant of the variety of privilege and confidentiality claims that may exist in the context of certain subject-matter specific investigations,[iv] which could implicate transmittal or discovery of protected materials. Finally, attorneys conducting internal investigations should also be aware of ethical requirements that may apply when the company's files contain employee emails that may be subject to a claim of privilege.[v]

Because of *Asia Global's* focus on a reasonable expectation of confidentiality when using the company's email system, the analysis may increase in complexity when the employee's emails with personal counsel are not sent via company email on a company server, a scenario that is increasingly common when employees use multiple devices and personal email accounts to send work-related emails. A number of courts have confronted various scenarios that offer baseline guidance, but are nowhere near as fluidly applicable as *Asia Global*. For example, in *Cotton v. Costco Wholesale Corp.*,[vi] the plaintiff sued his employer for racial discrimination and sought text messages from his manager's personal cell phone. The court rejected the plaintiff's request, ruling that Costco had no right to the content, as the company did not have "possession, custody, or control," of employees' personal cell phones. The court's reasoning, however, hinged on the fact that Costco did not issue the phones and employees did not use them for business, which raises the question of whether the result would have differed if the plaintiff's manager had sent work-related text messages. Also illustrative of the bounds of text messaging review is *In re Pradaxa (Dabigatran Etexilate) Products Liability Litigation*,[vii] where the court fined defendants nearly $1 million in punitive sanctions for preservation issues involving the failure to preserve text messages on employees' company-issued *and* personal cell phones.

Other lines of caselaw surround liability under the Stored Communications Act ("SCA"),[viii] which regulates unauthorized access to email, and the Computer Fraud and Abuse Act, which does the same for unauthorized access to computers.[ix] Although this precedent is not often on point for privilege considerations, it can be relevant nonetheless if a company were to attempt to access personal devices without employees' permission. And even if an entity theoretically has access to content – like access to email through a stored password on an employee's computer or device – at least one case has ruled that this does not necessarily grant permission to access the personal data, and can give rise to penalties under the SCA.[x]

Practical, logistical impediments are also implicit in the access analysis. From an e-discovery perspective, many third-party email providers have sophisticated encryption that makes it difficult or impossible to gain access to an individual's email without their authorization. For example, if a corporate employee downloaded the messaging program WhatsApp—known for its sophisticated encryption—to a work device and sent inappropriate, privileged, or potentially criminal communications, the company and its attorneys (and ultimately, the government) may never gain access to the content. Thus, the privilege evaluation would be frustratingly moot. The lesson learned is that as companies attempt to increase their data security and privacy firewalls, limitations on downloads could also end up protecting them from a messy situation where they have no privilege quandary, but no ability to provide responsive, cooperative content in a government investigation.

Conclusion

The caselaw on privilege in the context of corporate email will likely only proliferate in parallel with the rapid increase of data and electronic communications, and ultimately, the embrace of FinTech and other high-tech mechanisms for monitoring content. At this point in time, however, it appears that most courts will continue to start their analysis with the stalwart *Asia Global* four-factor test.

---

[i] 50 N.Y.S.3d 49 (N.Y. App. Div. 2017).
[ii] 322 B.R. 247 (Bankr. S.D.N.Y. 2005).
[iii] In *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), the court concluded that a former employee's emails to her attorney were privileged, as they were sent from a *personal* email account, albeit on a company computer, and were subject to an "ambiguous" policy that only prohibited certain uses of "the email system" and did not address personal email accounts. Employees were also unaware that their personal email accounts were stored by the company computers. As a result of the case, the company in question updated its e-mail use policy.
[iv] For example, in conducting an internal investigation into a healthcare company, counsel could very well be dealing with HIPAA-protected materials.
[v] When an attorney representing the entity discovers potentially privileged communications between an employee and his or her personal attorney, the attorney must determine whether the emails can be reviewed, and whether they must promptly notify the employee's attorney of the discovery. As ethics rules delegate terms of action based on inadvertent *disclosure* of privileged content – not necessarily inadvertent discovery of privileged content while conducting review – this is not always clear cut. For example, in *Stengart,* 990 A.2d 650, the appellate court criticized the defendant employer's attorney for independently determining that the privilege was waived upon discovery of counsel emails, then reading and using the emails.
[vi] No. 12-2731, 2013 WL 3819974, (D. Kan. July 24, 2013).
[vii] No 2385 3:12–md–02385., 2013 WL 6486921, at *2 (S.D. Ill. Dec. 9, 2013).
[viii] 18 U.S.C. § 2701 (2012).
[ix] 18 U.S.C. § 1030 (2012).
[x] *See Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d. 548 (S.D.N.Y. 2008). In *Pure Power Boot Camp*, the court allowed recovery under the SCA when an employee left the company and then learned that an unidentified colleague had accessed and printed emails from his personal email accounts. The employee, who had saved his usernames and passwords on company computers, alleged that this unauthorized access violated the SCA. The court agreed, thereby affirming certain employee privacy rights that could come into play during attorney review of employee email.