

Seyfarth eDIGital

In this Issue

Employee Attorney-Client Communications and Monitoring	1
Waiver	1
Ethical Considerations	2
Inadvertent Disclosure vs. Discernment	3
Key Takeaways	3

Attorney-Client Privilege and Waiver in Employee Email on Company Systems

In this issue of Seyfarth eDIGital, Seyfarth Shaw's eDiscovery and Information Governance practice group newsletter, we will continue the discussion of employee privacy in communications transmitted on company servers. This issue explores the discovery of communications between an employee and his or her attorney on company systems.

The last issue of Seyfarth eDIGital examined an employee's reasonable expectation of privacy in personal communications transmitted on company devices and servers. Where emails or other messages to and from an employee's attorney are involved, the situation becomes much more complicated. The issue becomes whether the employee has waived the attorney-client privilege with respect to those messages.

As discussed in the last newsletter, there are several factors that determine whether an employee can reasonably expect those communications to be private. When the potential for waiver of attorney-client privilege is involved, however, there are additional factors and ethical considerations that come into play.

Employee Attorney-Client Communications and Monitoring

Where the employer has an established email and/or internet usage monitoring policy in place, the employee's communications to his or her attorney arguably constitutes a waiver of the attorney-client privilege. A key element of the attorney-client privilege is the client's expectation that the communication is private and confidential. One can assert that, if the employee knows his or her communications may be monitored, there can be no expectation that the message will be private. However, the degree of protection afforded to attorney-client communications has resulted in a number of opinions examining this issue.

Waiver

When courts examine whether privilege has been waived, they consider whether the employee took reasonable steps to protect

the privileged communications, and whether there was an objectively reasonable expectation of privacy in the chosen medium of communication. Courts often employ the four factors first particularized in a New York federal bankruptcy case, *In re Asia Global Crossing Ltd.*¹ In *Asia Global Crossing*, executives used corporate email to communicate with their attorneys about actual or potential litigation involving the corporation (their employer). The judge concluded that the attorney-client privilege would be inapplicable if: 1) the company or organization had a policy that prohibited personal use; 2) the company regularly monitored the use of computers and email; 3) third parties had a right to access computers and emails; and 4) the company notified the employee that monitoring was taking place, or the employee was otherwise aware of the use and monitoring policies.

These four factors, with some variation, have been cited by courts around the country when examining whether privilege exists or has been waived in employee email communications with counsel. In *Convertino v. U.S. Department of Justice*, the court, applying the four factors, held that employees actually had a reasonable expectation of privacy where the employer's computer policy did not ban personal use of email, and where employees were unaware that their messages were regularly accessed and retained.²

As the four factors suggest, the examination of privilege waiver is a fact-intensive inquiry. In *Holmes v. Petrovich Development Corp.*, the court found that there was no privilege in email communications where the employee had: 1) been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail; 2) been warned that the company would monitor its computers for compliance with this company policy and thus might "inspect all files and messages ... at any time;" and 3) been explicitly advised that employees using company computers to create or maintain personal information or messages have no right of privacy in the contents of the information created or maintained.³

In contrast, other opinions have taken a different view relating to password protections and external email, and found these precautions to be evidence of the employee's reasonable privacy expectation, and their efforts to protect what they believe to be a privileged communication. The court in *Stengart v. Loving Care Agency*, found that privilege was not waived where the employee communicated with her attorney

using her password-protected personal email account, which she accessed with a company-issued laptop from home because of the precautions the employee took to safeguard the communications.⁴

Ethical Considerations

Discovery of potentially privileged communications between an employee and his or her attorney also raises a number of ethical questions. Once discovered, can counsel read the emails? Are you required to notify the employee's attorney of the discovery?

The defendant employer's attorney in *Stengart* faced this situation in the discovery of emails between the employee and her attorney using a password-protected personal email account. The New Jersey ethics rule stated: "[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender." The appellate court criticized the attorney for unilaterally deciding that the attorney-client privilege was waived, then reading and later using the emails in discovery.⁵ The New Jersey Supreme Court found that while the attorneys did not act in bad faith in discovering the emails (rather, they acted in good faith by preserving the data), the error was in not setting aside the emails and notifying opposing counsel or seeking permission from the court to proceed further.⁶ As a result, the Court remanded the case for a hearing to determine whether the employer's attorney should be disqualified from the case or some other sanction should be imposed.⁷

The *Stengart* case further demonstrates that reasonable minds, indeed courts, may differ on the issue of privilege waiver in an employee's attorney-client communications transmitted on company systems. In determining the appropriate course of action, the first step is to consult the rules of professional conduct of the jurisdiction. Even with a good faith determination that privilege has been waived, the safest approach is to notify the employee's attorney of the discovery, and allow them an opportunity to assert attorney-client privilege before reviewing the emails. The issue may still be litigated before the court, but a quick letter to opposing counsel can avoid motion practice and affords the opportunity to take the high road on the issue before it is brought to the Court's attention.

Where the emails or electronic documents containing potentially privileged information are discovered pre-litigation, the situation may call for a different approach. One option is to sequester the emails and hold them to notify opposing counsel or submit for judicial review pending the filing of the complaint. This follows the cautious approach of refraining from reviewing the emails until a waiver determination is made. Another approach is to make a similar proactive notification of the opposing party (or preferably their counsel, if they have engaged an attorney), and allow them a reasonable time to assert privilege before inspecting the contents of the email or documents.

Inadvertent Disclosure vs. Discernment

Some practitioners and judges have drawn a distinction between documents which are disclosed inadvertently in discovery responses, and documents which are unearthed by an employer or organization in the course of their own internal investigation, and not produced in the course of written discovery. Federal Rule of Evidence 502 addresses the issue of inadvertent waiver of attorney-client privilege, but the circumstances of disclosure contemplated by Rule 502 do not always apply in the employer-employee context. The adoption of Rule 502 resolved splits among federal jurisdictions and created one rule for analyzing both privilege and work product waiver issues resulting from their inadvertent production. Rule 502 adopted the majority view, namely, that inadvertent disclosure of protected communications or information does not constitute a waiver if the holder took reasonable steps to prevent disclosure and also promptly took reasonable steps to rectify the error. Rule 502, however, only applies to inadvertent

waiver through *production* of privileged material. The discovery of potentially privileged employee documents and communications in the course of an internal investigation is arguably different from the inadvertent production of information to an opponent by the party asserting a privilege. For example, *Long v Marubeni America Corp.*, involved the employer's discovery of potentially privileged documents in the course of their investigation, after litigation had begun.⁸ The judge in *Marubeni* found no attorney-client privilege or work product protection existed in emails exchanged over the employer's email system where the employer had a "no personal use" policy, despite the fact that password-protected external messaging was used. In analyzing the pre-502 inadvertent disclosure rule, the judge explained that "the party asserting the doctrine must be the party that made the disclosure."⁹

Key Takeaways

Whether an employee has waived attorney-client privilege in communicating with his or her attorney on company systems is a very fact-intensive inquiry that is not easily resolved. The factors for determining whether an employee can maintain an expectation of privacy in the emails, as well as local ethics rules, will all come into play in analyzing the issue. The decision to review these messages should be carefully documented and considered to avoid legal and ethical pitfalls.

Please contact the members of Seyfarth's eDiscovery and Information Governance practice group with any questions related to this newsletter.

¹ 322 B.R. 247 (S.D.N.Y. 2005).

² 674 F. Supp. 2d 97 (D.D.C. 2009).

³ 119 Cal. Rptr. 3d 878 (Cal. Ct. App. 2011)

⁴ 201 N.J. 300 (2010). See also *National Economic Research Associates, Inc. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006) (no waiver of the attorney-client privilege by an employee who communicated with his attorney using a password-protected Yahoo! Mail account from a company-issued laptop computer).

⁵ *Stengart v. Loving Care Agency, Inc.*, 973 A.2d 390, 403 (N.J. Super. 2009).

⁶ *Stengart*, 201 N.J. at 325.

⁷ *Id.* at 327.

⁸ No. 05 Civ. 639(GEL)(KNF), 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

⁹ *Id.* at *4.



Breadth. Depth. Results.

www.seyfarth.com