Avoiding Inadvertent Privilege Waivers In E-Communications

By **Megan Barriger, Erika Schutzman and Jeffrey Schomig**

Megan Barriger

Erika Schutzman

Jeffrey Schomig

An evolution in how courts interpret the confidentiality prong of the attorney-client privilege, which requires that both the client and attorney have an expectation of confidentiality in the communication for which the client seeks to assert the privilege, has been underway for more than a decade.

The current trend suggests that a company's attorney-client privilege may be lost if the company transmits the otherwise privileged information using third-party email accounts or servers that are accessible to others.

In addition, company employees and directors may lose the attorney-client privilege for communications with their personal attorneys about issues that the employee, director and/or the company would have preferred remained private — e.g. officer discussions with personal attorneys about a dispute with the company.

In light of these developments and as discussed in more detail at the end of this article, there are several steps that prudent companies can take to shore up the protection of their privileged materials, including:

- Using only a company-provided email address when communicating with nonemployee directors, rather than using the director's personal email or the email of the director's employer;
- Using a dedicated board portal housed on servers under the company's control;
- Scrutinizing vendor policies when the company does not own the servers over which it communicates;
- Reviewing the security settings for the videoconferencing platform used to host virtual meetings; and
- Understanding and seeking to manage the risk that employees and directors may potentially waive privilege over communications by using company email for communications with their personal counsel.

The rapidly evolving coronavirus pandemic has accelerated changes already underway in how we work and communicate. Companies have moved their employees to remote working and are considering holding (or have already held) their annual meetings of shareholders online.[1]

Even after the current crisis subsides, many of these changes are likely to endure now that more companies have proved the concept of scaled-up remote working.

Data privacy is one issue that is widely discussed when factoring the risks of remote working. But there is another, related risk that general counsel, chief legal officers, and

corporate boards need to address: Nontraditional working arrangements raise significant challenges to a company's ability to maintain attorney-client and related privileges for their sensitive, legal communications given the greater reliance on email as the form of communication and other third-party technologies that facilitate remote working.

This article highlights developments in privilege law that impact how companies share privileged materials, particularly with outside directors, something that is even more important in a world where remote working conditions are increasingly widespread.

The Evolution of Confidentiality

An evolution has been underway for more than a decade in how courts interpret the "confidentiality" prong of the attorney-client privilege.[2] Attorney-client privilege protects communications between an attorney and client for the purpose of seeking or giving legal advice, but it only applies to communications that are confidential, i.e., solely between an attorney and her client.

In analyzing a privilege claim, this confidentiality prong of the analysis requires both that the communication at issue be given in confidence and that the parties to that communication reasonably understand the communication to have been given in confidence. In other words, both the client and attorney must have an expectation of confidentiality in the communication.

The U.S. Bankruptcy Court for the Southern District of New York decision in In re: Asia Global Crossing and its progeny stand for the proposition that electronic communications are not confidential — and therefore not privileged — when someone else has a right to monitor those communications, even if they do not monitor those communications constantly.[3]

Courts have applied the Asia Global test to a variety of circumstances, including corporate officers communicating with their personal attorneys, corporate legal teams communicating with outside consultants, electronic documents stored on a noncompany server, and officer communications with personal attorneys.

These cases demonstrate that courts are likely to continue applying the Asia Global factors when assessing privilege, including companies' sharing of their privileged materials with outside directors when someone else, such as the director's employer, has a right to monitor those communications.

Key Cases Reshaping the Privilege's Confidentiality Prong

Asia Global Devises Four-Factor Test to Determine Whether Expectation of Privacy in Email is Objectively Reasonable

In Asia Global, a federal court faced the question of whether an employee's use of his employer's email system to communicate with his personal attorney destroyed the attorney-client privilege applicable to those communications.[4] With respect to whether the employee had an expectation of confidentiality in his personal communications with his attorney, the court looked to whether the employee had an "objectively reasonable expectation of privacy" in his work email.[5]

To assess this, the court developed the following four-factor balancing test:

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?[6]

No one factor is dispositive in the analysis, and ultimately it comes down to "whether the [employee's] intent to communicate in confidence was objectively reasonable."[7]

Cases Applying Asia Global to Assess Employee's Claim of Privilege

The four-factor Asia Global test has developed a strong following among other courts across a variety of jurisdictions.[8] The test has a far-reaching impact in a variety of circumstances, despite the fact that it originated as a way to assess an individual employee's expectation of privacy in his communications with his personal attorneys via his work email account (and thus, whether those emails were confidential and privileged).

While these cases all still involve an employee or director sharing information with their personal attorney, they highlight the increased risk that companies may face when it is senior personnel, such as officers and directors, whose privileged communications are at issue, as those communications may involve issues that could pose contagion risks for the company and thus that the company would prefer to keep private.

Officer Communications With Personal Attorneys

In re: Information Management Services Inc. Derivative Litigation, a case in the Delaware Chancery Court, involved emails sent by company executives to their personal attorneys about allegations that they had mismanaged the company.

Shareholders argued that these communications were not privileged because the company's ability to monitor employees' email communications eliminated any objectively reasonable expectation of confidentiality the executives could have had in their emails to their personal attorneys.

The court agreed; after applying the Asia Global factors, the court found that the executives' use of their work email to communicate with their personal attorneys destroyed their privilege over those communications because there was a clear policy indicating that "work emails were not private," the employer had a right of access, and employees were aware of the company's policies.[9]

The court made clear that company executives were not entitled to special treatment.[10]

Communications Stored on a Noncompany Server

In Lynch v. Gonzalez, another Delaware Chancery Court case, the case turned on ownership of the server on which a party's emails were stored.[11]

The court found that the plaintiff did not have an expectation of privacy in communications with his personal attorneys made using his work email address because these emails were

hosted on a noncompany server owned by the defendant and thus could be accessed by nonemployer parties.

Unlike many of the other cases applying the Asia Global factors, the "facts here [were] more complicated than a standard employee-employer relationship."[12] The plaintiff whose emails were at issue and one of the defendants co-owned and co-managed a company. The plaintiff was also an employee of the jointly owned company.

The litigation concerned whether the plaintiff had properly acquired a controlling interest in the jointly owned company. In connection with this acquisition, the plaintiff used his work email address to communicate with attorneys about personal legal advice related to the acquisition.[13] The plaintiff argued that these communications were privileged.

However, the email addresses that the jointly owned company used, including the plaintiff's, were hosted on a server that was owned by a company that in turn was owned solely by the defendants. The defendants argued that the plaintiff did not have an expectation of privacy in his communications with attorneys concerning personal legal advice because he sent and received these emails on a server owned by and accessible to defendants.

The court agreed, explaining that the Asia Global factors suggested that the emails in question were not confidential, and therefore the attorney-client privilege did not protect them.[14]

Officer Communications With Personal Attorneys

In In re: Oracle Corporation Derivative Litigation, the Delaware Chancery Court found that even someone as senior as an officer or director may lose privilege when communicating with his personal attorneys.

Oracle involved a shareholder derivative action, in response to which the company formed a special litigation committee of the board to evaluate the claim. The special litigation committee concluded that the original plaintiff should proceed with the claim derivatively.

At issue, in part, was whether the derivative plaintiff was entitled to the documents made available to or relied on by the special litigation committee in reaching this determination, and, if so, whether those documents were subject to any privileges.

The court found that the derivative plaintiff was entitled to the documents on which the special litigation committee relied. This included Oracle's privileged materials on which the special litigation committee relied given the "identity of interests among Oracle, its [special litigation committee] and the [derivative plaintiff]."[15]

This reasoning did not apply to claims of privilege by the individual defendants, including Oracle's officers, because there was not a similar identity of interest.[16] The court emphasized that the privilege claims of the individual defendants were still subject to arguments that privilege had been waived.

With respect to waiver, the court acknowledged "that any emails on Oracle's email servers [may] not [have been] privileged to begin with" because the individual defendants may have lacked the requisite expectation of privacy when using work email accounts to communicate with their personal attorneys.[17]

Cases Applying Asia Global to Assess Company's Claim of Privilege

The four-factor Asia Global test has also been applied to situations where a company's privilege was at issue. Application of the test to challenges to a company's attorney-client privilege underscores that the legal principles articulated in Asia Global would likely be applied to companies' sharing of privileged materials with their outside board members.

Company Communications With Outside Consultants

In re: High-Tech Employee Antitrust Litigation involved emails sent to a consultant and part-time employee of a large tech company who also was the chairman of the board at another large tech company. The consultant used his board email address for communications with his consulting client.

In a litigation involving allegations of collusion to avoid employee poaching, the company that hired the consultant redacted and withheld some of its emails (and their attachments) with the consultant on the basis of privilege. The plaintiffs argued that by sending these documents to the consultant at his board email address, the company that had hired the consultant had waived privilege.

The U.S. District Court for the Northern District of California engaged in the fact-intensive Asia Global balancing test and found the four factors evenly split. The company that hosted the consultant's board email, for example, had a policy stating that, as a general rule, use of corporate resources should be for company business.[18] But it did not ban personal use of company email entirely.

The consultant was aware of the company's policy concerning email use. In addition, the company also reserved the right to monitor emails and had a right of access to the emails; but it did not actually monitor them.

To resolve the even split of the four factors, the court concluded that "the importance of the attorney-client privilege as well as the lack of evidence that [the company] in fact monitored [the consultant's] emails support[ed] the preservation of the privilege in this case."[19]

How Developments in Confidentiality Impact Companies Today

While the context in which many of these cases arose concerns an individual employee corresponding with their personal attorney, the underlying principles that the courts apply suggest potentially further-reaching implications, especially as companies increasingly transition to remote work and virtual meetings.

One common situation where these principles would likely be applied is companies' sharing of privileged materials with their outside board members. Indeed, the Northern District of California's decision in High-Tech Employee underscores the likelihood that courts would look to the Asia Global four-factor test when dealing with challenges to a company's privilege over materials shared with outside directors via those directors' employer-email accounts.

Take the following scenario: Company A has three outside directors, out of five total. Each of these three outside directors is employed, and they rely on email addresses provided by their employers for communications. Company A does not provide its outside directors with a Company A email address, and its communications with these three directors occur

through email accounts and on servers controlled by their employer.

Company A is sued. The plaintiff requests all documents provided to the board, including all board minutes and materials. Responding to these requests, Company A redacts privileged materials, but the plaintiff challenges these redactions, arguing that Company A waived privilege because it knowingly provided materials containing the privileged information to the outside directors via their employer-controlled email accounts.

The underlying principles in the cases described above come into play at this juncture. A threshold issue is whether use of the outside directors' employer email accounts to share privileged information renders those communications nonconfidential. If even just one of the outside directors' employer email accounts is subject to ongoing monitoring by their employer — a relatively common practice[20] — or is governed by a policy that bans personal use, or gives the employer or another third-party a right of access, there is a risk that courts could find that Company A waived privilege when it sent the board materials to the outside director.

How to Mitigate Threats to Privilege

There are several steps that prudent companies can take to shore up the protection of their own privileged materials.

- Ensure that all directors, including independent directors, have a company email address. Use that address to communicate with these directors for all company business, but especially for all business that is confidential and privileged.

- Consider using a dedicated board portal housed on servers under the company's control for communications with directors for company business, especially for business that is confidential and privileged.

- Carefully scrutinize policies from its vendors, if the company does not own the servers over which it communicates, to ensure that those policies specifically provide for confidentiality for communications between the company and its employees. The agreement should also be explicit about who may have access to the server and under what circumstances.

- Review security settings for the videoconferencing platform when holding virtual board meetings (or any other company meetings). Remind participants to be mindful of who else might be able to view confidential and privileged information on the screen and be aware of whether recordings of the virtual meeting can be made (either intentionally or inadvertently) and the locations in which they may be stored.

- Understand that even senior personnel, such as officers and directors, have potential to waive their privilege over communications with personal counsel under the Asia Global test. While the company's privilege is not directly at issue, waiver of privilege for senior personnel carries enhanced risks for the company. Allowing discovery of sensitive legal communications that may prove embarrassing, or worse, for directors and officers could pose contagion risks for the company and — for publicly traded companies — to its stock value. Companies may then be faced with the Hobson's choice of allowing discovery of these personal emails, or arguing against the company's own personal use polices in an effort to help the officer or director maintain privilege pursuant to the Asia Global test. The latter path could open the

floodgates to all of the company's employees claiming an expectation of confidentiality over their personal use of the company's email system.

Conclusion

The requirement that clients have a reasonable expectation of confidentiality when communicating with their lawyers has taken on increased importance as privilege protection is weighed against evolving modes of communication and nontraditional workplaces — an evolution that the COVID-19 pandemic has accelerated. Companies can expect courts to continue applying the Asia Global factors when assessing the confidentiality prong of attorney-client privilege for communications and documents subject to third-party access.

Fortunately, many of the privilege concerns raised by the Asia Global factors can be addressed by understanding the requirements of the confidentiality prong of the attorney-client privilege, being aware of how courts have applied it to the latest communication modes and working arrangements, and taking reasonable, proactive steps to address these concerns as part of the company's internal communications policy.

Megan Barriger is counsel, Erika Schutzman is a senior associate and Jeffrey Schomig is an attorney at WilmerHale.

[1] See, e.g., Jamie Gorelick et al., COVID-19: Key Considerations for Directors, WilmerHale (Mar. 23, 2020), https://www.wilmerhale.com/en/insights/client-alerts/20200323-covid-19-key-considerations-for-directors; Lillian Brown et al., Conducting Your Annual Meeting During a Health Pandemic, WilmerHale (Mar. 16, 2020), https://www.wilmerhale.com/en/insights/client-alerts/20200316-conducting-your-annual-meeting-during-a-health-pandemic.

[2] The trend began with In re: Asia Global Crossing, 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

[3] The United State Supreme Court has not addressed this issue directly, and when it addressed the related issue of whether employees have a reasonable expectation of privacy in communications on employer-provided electronic devices, it left that question unresolved. See City of Ontario v. Quon, 560 U.S. 746, 760 (2010). Quon did not involve claims of attorney-client privilege. In Quon, the court assumed, without deciding, that the employee had a reasonable expectation of privacy in text messages sent on a pager provided to him by his government employer because it recognized that "[a] broad holding concerning employees' privacy expectations vis–à-vis employer-provided technological equipment might have implications for future cases that [could not] be predicted." Id.

[4] Some courts have distinguished between communications sent using a company email system and communications sent using a personal, web-based email account on a company device and have found a lesser expectation of privacy in the former. See Sengart v. Loving Care Agency, Inc., 990 A.2d 650, 662–63 (N.J. 2010) (collecting cases).

[5] 322 B.R. at 258–59.

[6] Id. at 257–59. After a fact-intensive assessment of the four factors, the court found that the third factor weighed against an expectation of privacy because "sending a message over the [company's] e-mail system was like placing a copy of that message in the company files," but that the evidence related to the three other factors was equivocal. Id. at 259. As a result, the court "w[as] unable to conclude as a matter of law" that use of the company's email system in these circumstances destroyed the attorney-client privilege. Id. at 261.

[7] Id. at 258–59.

[8] See, e.g., In re: Info. Mgmt. Servs., Inc. Deriv. Litig., 81 A.3d 278, 287 (Del. Ch. 2013) (explaining that "[n]umerous courts have applied the Asia Global factors or closely similar variants when analyzing the attorney-client privilege" and collecting cases); In re: Reserve Fund Sec. & Deriv. Litig., 275 F.R.D. 154, 159–60 & n.2 (S.D.N.Y. 2011) (describing Asia Global four-factor test as "widely adopted" and collecting cases); see also Goldstein v. Colborne Acquisition Co., LLC, 873 F. Supp. 2d 932, 935 (N.D. Ill. 2012) (describing Asia Global as "the most oft-quoted case on the subject" of "[w]hether use of work e-mail to communicate with an attorney destroys the [attorney-client] privilege"). The substance of the Asia Global test also has been applied by other courts, even when not cited directly. See, e.g., Holmes v. Petrovich Dev. Co., LLC, 119 Cal. Rptr. 3d 878, 896 (Cal. Ct. App. 2011) (finding privilege waived and observing that "[plaintiff] used her employer's company e-mail account after being warned that it was to be used only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy").

[9] See 81 A.3d at 287–92. The court acknowledged that there was the potential for a "statutory override that could alter the common law result," but concluded that there was no applicable statutory override in this case. Id. at 292–96.

[10] Id. at 290 (rejecting executives' argument that "because they [were] the senior officers at [the company], they would decide whether or not [the company] would monitor an employee's email" and thus they had "a unique expectation of privacy").

[11] However, the analysis is fact-specific, and in In re Grand Jury Subpoena, JK-15-029, the court concluded that a former public official had reasonable expectation of privacy in, and could assert privilege over, communications with his personal attorneys sent using his personal email address, even the communications archived on state's computer server without his knowledge. See 828 F.3d 1083, 1086, 1090, 1092 (9th Cir. 2016).

[12] Lynch v. Gonzalez, 2019 WL 6125223, at *6.

[13] The attorneys were also employed by the jointly owned company, and they used their work email addresses to communicate with the plaintiff. Id. at *3. In addition to representing the plaintiff in his personal capacity, the attorneys also worked for and represented the jointly owned company, but communications related to their work for the jointly owned company were not at issue in the litigation. Id.

[14] Id. at *6; see also Hr'g Tr. at 22–25, Lynch v. Gonzalez, No. 2019-0356-MTZ (Del. Ch. Oct. 15, 2019) (finding that while there was no policy banning personal use of company email, employees knew that their email was under defendant's control and subject to his monitoring, the company had a right to the emails, and plaintiff did not deny knowing that

defendant could access his emails, which weighed against a finding of confidentiality). The court went on to consider whether there was a statutory override to this outcome, pursuant to In re Information Management Services Inc. Derivative Litigation, 81 A.3d 278 (Del. Ch. 2013), and concluded that, under Argentine law, plaintiffs had a reasonable expectation of privacy in the emails. See 2019 WL 6125223, at *6, *10.

[15] See In re Oracle Corporation Derivative Litigation, 2019 WL 6522297 (Del. Ch. Dec. 4, 2019), at *1, *12, *19. While the court clarified that the "matter [was] not under the Garner doctrine," its analysis was "informed by the analysis done by the Garner court itself." Id. at *19. The court found it persuasive that Oracle had chosen to establish the special litigation committee and provide it with documents, including potentially privileged ones, for the purpose of determining whether to prosecute the claims brought by the derivative plaintiff. Id. The court emphasized that because the special litigation committee, based on its review of those documents, determined that the claims should be "prosecuted, not by the [special litigation committed], but by the [derivative plaintiff]," and Oracle had "not advanced a single reason why . . . [its] corporate interest in nondisclosure of those same communications," including any that were privileged, "outweigh[ed] its interest in vindication of the [litigation] asset," the derivative plaintiff was entitled to the privileged communications relied upon by the special litigation committee. Id.

[16] Specifically, the derivative plaintiff was not their fiduciary, and nobody acting on their behalf concluded it was in their own best interest to provide those documents to the special litigation committee. Id. at *21.

[17] Id. Ultimately, the court concluded that it could not decide the privilege issues as presented because they were in the abstract. Id. at *22. The court signaled that it would scrutinize claims of privilege on a case-by-case basis, considering among other things the factors from the Asia Global test. Id. This privilege question remains a live issue in this case.

[18] In re High-Tech Employee Antitrust Litigation, 2013 WL 772668 (N.D. Cal. Feb. 28, 2013) at *6.

[19] Id. at *7 (emphasis added).

[20] See 2007 Electronic Monitoring & Surveillance Survey, ePolicy Inst., http://www.epolicyinstitute.com/2007-survey-results (last visited Apr. 17, 2020) (finding that 43% of employers monitor email, and that for those that do, it is more common to monitor external emails).