Harvard Law School Forum on Corporate Governance

# The WeWork Decision and its Implications for Director Email Accounts

*Posted by Nicholas O'Keefe, Douglas F. Curtis, and Max Romanow, Arnold & Porter Kaye Scholer LLP, on Monday, May 24, 2021*

**Editor's note:** Nicholas O'Keefe is partner, Douglas F. Curtis is senior counsel, and Max Romanow is an associate at Arnold & Porter Kaye Scholer LLP. This post is based on an Arnold & Porter memorandum by Mr. O'Keefe, Mr. Curtis, Mr. Romanow, and Matthew J. Douglas, and is part of the Delaware law series; links to other posts in the series are available here.

## Introduction

A recent Delaware court decision, *In re WeWork Litigation*, put a spotlight on the risk of corporate employees and directors destroying privilege by communicating through email. Questions about the security and confidentiality of electronic communications have been around for a long time. But at least under Delaware law, the *WeWork* decision expanded the applicability of a test that was originally intended for evaluating privilege in the context of employer-employee disputes where the employee uses a work email address for communicating with his or her personal attorney. *WeWork* applied the test and held that privilege was destroyed where two employees of Sprint, a company then 84% owned by SoftBank Group Corp. (SoftBank), exchanged emails about The We Company (WeWork), which was another company in which SoftBank had a significant investment, using their Sprint email accounts. This broader application of the test has implications for whether companies communicating privileged information with their outside directors through email accounts held by those directors with their employers risks destroying privilege.

This post considers that issue in the context of both: (1) independent directors employed by entities that are not stockholders of the companies on whose board they sit, and (2) employees of investment funds who sit on boards of the funds' portfolio companies pursuant to designation rights held by the funds. For independent directors, there is a direct parallel to the *WeWork* decision: the companies on whose boards they sit should avoid communicating privileged information with them through their work-related email accounts. For board designees of investment funds, two separate legal doctrines relating to the right of the designating funds to access portfolio company information without destroying privilege suggest that use by the board designees of their fund email accounts should not generally undermine privilege.

Part II of this Advisory provides a brief overview of existing law and the *WeWork* decision. It first describes the attorney-client privilege under Delaware law and certain exceptions to the general rule that disclosure of otherwise privileged information to a third party waives that privilege. It then describes the framework for analyzing privilege waiver through email communications set forth in *In re Asia Global Crossing, Ltd*., the leading case that addressed the issue in the context of

employer-employee disputes. Part II then briefly describes the *WeWork* decision and its application of the *Asia Global* test.

Part III of this post analyzes the *WeWork* decision in the context of company communications with outside directors. It first briefly considers independent outside directors. It then focuses on board designees of investment funds, for which it considers two Delaware law doctrines—the first involving the right of board designees to share privileged company information with their designating stockholders, and the second involving the ability to preserve privilege in communications among companies belonging to the same corporate group. Part III then considers the relevance of these two doctrines in the context of board designee emails using a fund email account, and how the *Asia Global* test might apply in the analysis. It then considers certain limitations on the analysis. A brief conclusion is set forth in Part IV.

## Attorney-Client Privilege and the *WeWork* Decision

### Attorney-Client Privilege Generally

The attorney-client privilege protects against compelled disclosure of communications between an attorney and his or her client and between representatives of the attorney and the client. The purpose of the privilege is to encourage clients to speak openly with their attorneys and thereby facilitate the administration of justice. Different jurisdictions have different rules for privilege and confidential communications, but for our purposes, Delaware provides the relevant framework.

Delaware Rule of Evidence 502 governs the attorney-client privilege in Delaware. Rule 502(b) states the general rule:

> A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client (1) between the client or the client's representative and the client's lawyer or the lawyer's representative, (2) between the lawyer and the lawyer's representative, (3) by the client or the client's representative or the client's lawyer or a representative of the lawyer or a representative of a lawyer representing another in a matter of common interest, (4) between representatives of the client or between the client and a representative of the client, or (5) among lawyers and their representatives representing the same client.[1]

The rule only protects against compelled disclosure of *confidential* communications. According to Rule 502(a)(2), "[a] communication is "confidential" if not intended to be disclosed to third persons other than those to whom disclosure is made in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication."[2] The concepts of privilege and confidentiality are entwined: if a communication is not made in confidence (i.e., a third party is present when the communication is made, or possibly, as relevant here, where a third-party organization has monitoring rights over electronic communications transmitted through its email system), the privilege is generally waived as to

[1] Del. R. Evid. 502(b).
[2] Del. R. Evid. 502(a)(2).

those communications.[3] Unless the disclosure is inadvertent and the client took reasonable steps to prevent the disclosure and rectify the error, it is presumed that where information is shared with a third party the client no longer intended to keep the communication confidential and thus the privilege is lost.

As with most legal rules, there are exceptions to this third-party waiver rule. For example, a court may consider the nature of the relationship between the parties sharing information before deeming the communications waived. Say an adverse party in litigation against Company A moves to compel communications between Company A's CEO and Company A's in-house counsel about the subject of litigation. This would fall squarely within Rule 502. But what if the CEO is chief executive not of Company A, but of a wholly or partially owned subsidiary of Company A, or of an independent organization that shares a common legal interest with Company A? How then do courts evaluate privilege as to the communications between the CEO and Company A's in-house counsel?

These illustrations are primarily addressed through two exceptions to the third-party waiver rule: the joint-client privilege (also known as the co-client privilege) and the common-interest doctrine (also known as the community-of-interest privilege). *In re Teleglobe Communications Corp*.[4] is the leading Third Circuit case on privileged communications in a corporate group and thoroughly analyzes both exceptions. *Teleglobe* sets forth the rule that the joint-client privilege generally encompasses the relationship between a parent and its wholly-owned subsidiary. Under this exception, the corporate entities are considered joint clients with a centralized legal department and communications between the department and employees in the corporate group are generally protected from disclosure.[5] This conclusion maintains because courts recognize that it often makes strong business and legal sense for companies in a corporate group to share in-house legal resources, and that as a practical matter, centralized legal services are often used as a matter of course.

In contrast, a communication between a parent and a minority-owned subsidiary or an independent company is likely to be analyzed under the common-interest doctrine. This doctrine applies when two or more companies represented by separate counsel share a common legal interest and the parties communicate about that common legal interest.[6] The contours of who can share privileged information with whom (i.e., lawyer-to-lawyer or executive-to-lawyer) and to what extent the interest must align (i.e., identical interest or similar interest) vary across courts. Importantly, and as expanded upon in part III.B.2, the common interest cannot be solely a common business interest for the doctrine to apply, and must relate to a common legal interest, risk or claim. For present purposes, it is sufficient to define the rule as where two corporations have a "substantial identity of legal interest in a specific matter," the privilege as between the companies as to the legal interest is not lost so long as it is otherwise confidential among the parties.[7]

---

[3] Del. R. Evid. 510 governs privilege waiver. For purposes of the parenthetical, "third party" refers to persons other than those specified in Rule 502.

[4] 493 F.3d 345 (3d Cir. 2007).

[5] Id. at 372.

[6] *Id.* at 364-66.

[7] *United States v. American Telephone and Telegraph Co*., 86 F.R.D. 603, 616-17 (D.D.C. 1979).

The waters become murkier in the case of a majority-owned subsidiary. While some courts set forth a bright-line rule that a majority-owned subsidiary shares a joint privilege with its parent,[8] the court in *Teleglobe* looked beyond the percentage ownership and considered the factual circumstances of the relationship and the practical effects of shared privilege. So if the parent company and its majority-owned subsidiary share in-house counsel, a court could use the same practical reasoning as *Teleglobe* to conclude that the companies should be considered joint clients with in-house counsel. And if the companies utilize separate counsel, a court could ask whether the companies' communications concern a common legal interest sufficient to satisfy the common-interest doctrine.

Separate from the joint-client privilege and common-interest doctrine, Delaware law has adopted a policy exception that the sharing of privileged information by a board designee with his or her designating stockholder generally does not destroy privilege. This exception is discussed further in part III.B.1.

The Delaware rules and the exceptions described above primarily concern with whom privileged information can be shared. A similar but slightly distinct issue is how this information can be shared and whether use of certain mediums destroys a privilege otherwise intact. This question is especially salient when employees conduct personal business via email accounts provided by their employers.

### Privilege Waiver Through Use of Email—*In re Asia Global*

Since the advent of email as a popular means of communication, the legal profession has been vexed by the questions whether and when electronic communications could be considered "confidential," thereby satisfying the key prerequisite to the existence of the privilege. Early critics noted that electronic communications were subject to interception, and so might not be reliably confidential at all. By 1999, however, the ABA made the determination that a lawyer and client could transmit information relating to the representation by email sent over the Internet without violating the Model Rules of Professional Conduct, "because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[9] Still, situations continue to arise where parties to an electronic communication arguably do *not* have a reasonable expectation of privacy.

*In re Asia Global Crossing, Ltd.*[10] established a leading test on privilege waiver in a commonly recurring circumstance: when one party to the communication is using a company email account for non-company communications. The primary issue in *Asia Global* was whether an employee's use of his employer's email system to communicate otherwise privileged information with his personal attorney destroyed the attorney-client privilege where the employee and his former employer's trustee in a bankruptcy proceeding became adversarial. The court noted the dearth of precedent that considered the confidentiality of an employee's emails in the context of the

[8] *See, e.g., id.* at 615 (defining the "client" for purposes of the attorney-client privilege as the named defendants, the wholly-owned subsidiaries, and the majority-owned subsidiaries, but not the minority-owned or formerly affiliated companies); *Weil Ceramics & Glass, Inc. v. Work*, 110 F.R.D. 500, 503 (E.D.N.Y. 1986) ("the attorney-client protection provided for corporate clients includes, the corporation who retained an attorney, its parent, and its wholly owned and majority owned subsidiaries considered collectively.").

[9] ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

[10] 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

attorney-client privilege and devised the following test based largely on the right to privacy and the Fourth Amendment's "reasonable expectation of privacy" analysis:

"(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?"[11]

The *Asia Global* test was developed in the context of an employer-employee dispute. *In re Information Management Services, Inc. Derivative Litigation*,[12] a leading Delaware case to analyze privilege waiver under the *Asia Global* factors, noted that other jurisdictions had applied the *Asia Global* test in disputes where the employer was not a litigant, but, in dictum, the court questioned whether that was appropriate. Vice Chancellor Laster noted in that decision that third parties outside the corporation cannot routinely access work email accounts, and that "[t]he corporation and its employees should be on different and stronger ground when those outside the corporation seek to compel production of otherwise privileged documents that employees have sent using work email."[13] However, that ship has now sailed in Delaware. In *WeWork*, Chancellor Bouchard held that the *Asia Global* test is not restricted in application to litigation between the employer (or its successor in interest) and employees.[14]

## The *WeWork* Decision

In *WeWork*, the Delaware Court of Chancery found that the use of Sprint email accounts by Sprint employees doing WeWork-related work for SoftBank caused the communications between SoftBank and those individuals to lose the privilege that might otherwise have attached to them. The decision involved a ruling on a motion to compel defendant SoftBank to produce documents in litigation stemming from the alleged breach by SoftBank of its contractual obligation to complete a tender offer for shares of WeWork. During the period relevant to the litigation, SoftBank owned 84% of Sprint, and some of the Sprint executives and employees performed services for SoftBank related to WeWork. Two individuals used their Sprint email accounts to receive legal advice from SoftBank's internal and external counsel that was relevant to the WeWork litigation and that did not relate to Sprint's business. The motion turned on whether they nonetheless had a "reasonable expectation of privacy" sufficient to preserve the attorney-client privilege.

In finding that they did not have a reasonable expectation of privacy in the use of the Sprint email accounts, the court analyzed the four-factor test set forth in *Asia Global,* which, as noted above, had been used to analyze privilege waiver through the use of work email accounts for non-work purposes.[15]

The court noted that Sprint's Code of Conduct provided that employees should have no expectation of privacy in information transmitted via Sprint's computer systems or network, and that Sprint reserved the right to review employee emails. The court viewed this as the type of

---

[11] *Id.* at 257 (internal citations omitted).
[12] 81 A.3d 278 (Del. Ct. Ch. 2013).
[13] Id. at 296.
[14] *In re WeWork Litigation*, 2020 WL 7624636, at *5 (Del. Ch. Dec. 20, 2020).
[15] The *WeWork* court noted that this was the test used in *Info. Mgmt. Servs.*

clear policy restricting personal use of emails, and reserving employer monitoring rights, that has been considered—for purposes of the first *Asia Global* factor—to weigh in favor of requiring document production.

The court found that the second *Asia Global* factor also weighed in favor of requiring document production because Sprint reserved the right to monitor employee emails, regardless of whether there was any indication that they had ever exercised that right. The court found that the third *Asia Global* factor was duplicative of the first two, thus also weighing in favor of document production, because Sprint had the right to access the computer or emails. The court found that the fourth *Asia Global* factor also favored requiring document production because, as officers and senior employees of Sprint, the two individuals were presumed to have knowledge of Sprint's email policies and the record indicated that they were aware of them.

## Implications of *WeWork* for Communications with Outside Directors

In *WeWork*, privilege was lost because the privileged communications between SoftBank and two Sprint employees relating to WeWork matters were transmitted through the employees' Sprint work email accounts, and those employees were held not to have a reasonable expectation of privacy in those accounts due to Sprint's email monitoring policy. It is common for employers to have monitoring rights over employees' emails through their work email accounts.
Thus, *WeWork* may have broad applicability. One need change the facts only slightly to highlight potentially significant questions about the implications of *WeWork* for communications between a company and its outside directors. Does *WeWork* mean that all of a company's outside directors must avoid communications through their own employers' email accounts? Should a company issue email accounts to all of its outside directors and insist that all electronic communications between the company and those directors should be conducted through those email accounts or some other secure medium, such as a board portal?

### Independent Outside Directors

The easier case to consider is an outside director who has a full time job with an employer that is unrelated to the company on whose board the director sits—an "independent director." If the independent director communicates with the company using his or her employer's email account, this is a parallel situation to that addressed in *WeWork*. If the employer has monitoring rights over the email account, then there is a significant risk that use of the email account to exchange privileged information between the company and the independent director will result in the privilege being deemed waived. As part of their director onboarding procedures, companies could review the email monitoring rights of employers of such individuals to assess the likelihood of a privilege waiver problem. But that would be onerous and impracticable. It would be simpler for companies to have a policy that no email should be sent to such independent directors using their employers' email accounts. The simplest approach would be to issue the independent directors company email accounts and communicate through those. An appropriately secure personal email account, such as Gmail, is also not likely to cause a privilege waiver.[16]

[16] *See In re WeWork Litig.*, 2020 WL 7624636, at *2.

## Board Designees

The more complex case involves a director who is a stockholder's designee to the board. Consider a hypothetical private equity or venture capital fund that typically obtains one or more board seats in connection with its portfolio investments. Its board designees are usually its investment professionals who typically communicate using fund email accounts. These investment professionals often sit on a large numbers of boards, and so having a separate email account for each company on whose board they sit could be extremely cumbersome. Does *WeWork* suggest that they nonetheless need one, because using a fund email account is likely to result in a deemed waiver of privilege? As discussed below, this appears to extend *WeWork* too far.

The analysis for the board designee is different from the analysis for the independent director because the board designee's employer—the fund—is a stockholder of the company. If the fund as a stockholder can legally access privileged company information without such access causing the privilege to be deemed waived, then there is reason to believe that the board designee's use of a fund email account may also not cause a privilege waiver, even if the fund has comprehensive email monitoring rights. This is discussed further in part B.3 below. First, parts B.1 and 2 consider two lines of cases which recognize the right of stockholders to access privileged information, under the circumstances described, without causing the loss of privilege.

### *Communications Between a Stockholder and Its Board Designee*

Delaware courts recognize that directors have broad information access rights and that board designees are generally free to share that information with their designating stockholders. The issue has arisen in a line of cases where corporations tried to limit information provided to the board designee where there was actual or potential adversity between the board designee, the designating stockholder, or both, and the other board members. The cases make clear that a director's right to access company information is "essentially unfettered in nature"[17] and that this right "extends to privileged material."[18] Three recognized exceptions limit this right: (1) where there is an *ex ante* agreement restricting access, (2) where the information is made available to a special committee of which the director at issue is not a member, and (3) where sufficient adversity exists between the director and the board.[19] In *Kalisman v. Friedman*, the court considered an argument by board members that they could withhold information from a board designee because the designee might share the information with his designating stockholder, which in turn might use the information to harm the corporation. Rejecting this argument, Vice Chancellor Laster held that "[w]hen a director serves as the designee of a stockholder on the board, and when it is understood that the director acts as the stockholder's representative, then the stockholder is generally entitled to the same information as the director."[20] In a later article, Vice Chancellor Laster expanded on this point:

"This rule reflects the practical reality that director representatives in both public and private companies routinely share confidential corporate information with colleagues at their affiliated

---

[17] *Schoon v. Troy Corp.*, 2006 WL 1851481, at *1 (Del. Ch. Jun. 27, 2006).
[18] *Kalisman v. Friedman*, 2013 WL 1668205, at *4 (Del. Ch. Apr. 17, 2013).
[19] *Id.* at *4-5.
[20] Id. at *6.

investment funds. The managing directors of these funds regularly meet to monitor their investments, and they routinely receive reports from their director designees on the performance of their portfolio companies. In most cases, the . . . directors themselves are managers or fiduciaries of the fund that made the investment, and the managers of the fund are often fiduciaries of the limited partners or other investors in the fund. A bright-line rule *against* information sharing would create the potential for breaches of duty at two levels: first at the corporate level by preventing the director representatives from engaging in behavior that is currently a normal part of the investment and monitoring process, and second at the fund level by preventing the director who was a fund fiduciary from sharing information that was material to the fund. Such a rule only would be honored in the breach. Rather than an actual rule to guide conduct, a rule against information sharing would put a cause of action in the hands of the corporation to use at its discretion. And if a corporation were to try to enforce it, a seemingly bright-line rule would turn out in practice to involve fact-laden litigation about the degree to which other directors knew about and consented to the sharing or engaged in similar information sharing themselves. The better approach, which Delaware has adopted, is therefore to permit information sharing and allow corporations to address risks by contracting with the affiliate and by enforcing the directors' fiduciary duties."[21]

More recently, the 2018 decision *In re CBS Corp. Litigation* endorsed Vice Chancellor Laster's position that designating stockholders have broad access rights to company information in line with those of their board designees.[22] In *CBS*, Chancellor Bouchard denied a litigant's request to prohibit director-designees from sharing privileged information with their designating stockholder as part of a larger ruling. Citing *Kalisman*, Chancellor Bouchard noted that the weight of precedent supported this conclusion.

### *Intra-Group Communications*

As noted in part II.A., there are two main exceptions to the privilege waiver rule that can apply in the context of intra-group communications. The first exception is the joint-client privilege, which under *Teleglobe* encompasses the relationship between a parent and its wholly-owned and sometimes majority-owned subsidiary. In our hypothetical involving a fund, a board designee, and a portfolio company, a fund that wholly owns its portfolio company and shares centralized legal counsel would be entitled to portfolio company information as joint clients under *Teleglobe*. The same analysis should apply if the fund shares a legal department with a majority-owned portfolio company. But as previously noted, a court might examine the mechanics of legal representation between the fund and the majority-owned subsidiary before deciding to apply the joint client framework.

The second exception is the common-interest doctrine. If the fund owns a minority stake in the portfolio company and is represented by separate counsel, a Delaware court would evaluate whether the fund and the portfolio company share a common legal interest and the parties communicate about that common legal interest. The portfolio company would need a unity of *legal* interest to satisfy this exception, not merely shared commercial objectives. For example, a court may find unity of legal interest sufficient to satisfy the common-interest doctrine if the fund

[21] J. Travis Laster & John Mark Zeberkiewicz, The Rights and Duties of Blockholder Directors, 33 The Business Lawyer, Vol. 70, Winter 2014/2015, at 55-56 (internal citations omitted).

[22] In re CBS Corp. Litig., 2018 WL 3414163, at *7 (Del. Ch. Jul. 13, 2018).

and the portfolio company share information about a joint defense or strategy in litigation,[23] or seek to enforce a joint patent.[24] Courts are more skeptical of arguments where the common interest is business-related, such as two parties receiving joint legal advice designed to further a business transaction between the two.[25] In our hypothetical, the analysis would be the same: the board designee would have to show that his or her communications to the fund concerned a matter of common legal interest. One significant implication of this is that a board designee who shares with his or her designating fund privileged communications from the portfolio company in which the fund has a minority stake about a matter in which the fund does *not* have a common legal interest could cause the privilege to be waived, unless another waiver exemption exists.[26]

### *What about Asia Global?*

Parts B.1 and B.2 describe two theories under which the fund can access privileged information of a portfolio company without destroying privilege. But how does this relate to the board designee using a fund email account and to the *Asia Global* test?

*Asia Global* addressed whether an employee had a reasonable expectation of privacy when using his employer's email account in a dispute between the employee and the employer's successor in interest. *Asia Global* is relevant to our fund hypothetical because, in subsequent decisions, it was extended beyond the employer-employee context. There are two plausible readings of *Asia Global* outside the employer-employee context, and both indicate that privilege should not generally be deemed waived in our hypothetical where the board designee uses a fund email account.

The first interpretation of *Asia Global* involves a narrow reading that turns *Asia Global* into the second part of a two-part test, i.e., first whether the employer's access to communications would defeat privilege, and only if so does part two of the test apply, which evaluates whether the employee has a reasonable expectation of privacy in light of the employer's ability to access the emails. This two-part test seems logical when you consider the nature of the Asia Global four factor test: it is used to evaluate whether the employee has a reasonable expectation of privacy from the employer, but that necessarily begs the threshold question of whether the employer's access to the communications would defeat privilege in the first instance. If it would not, because the employer is "inside" the coverage of the privilege, then one should not even have to consider the *Asia Global* test. It would be like disclosing privileged information in a conversation in a sound-proof room among people who could all receive the information without destroying privilege. This is entirely consistent with Rule 502(b) of the Delaware Rules of Evidence and there is no need to consider the *Asia Global* four-factor test. But if, on the other hand, the employer's access to the communications would defeat privilege, a court would then apply the *Asia Global* test to determine whether the employer's monitoring of the account is sufficiently lax and the account sufficiently secure from the employer such that the employee maintains a reasonable

[23] *See, e.g., Coring Inc. v. SRU Biosystems, LLC*, 223 F.R.D. 189 (D. Del. 2004); *MobileMedia Ideas LLC v. Apple Inc.*, 890 F.Supp.2d 508 (D. Del. 2012).

[24] *See, e.g., Rembrandt Technologies, L.P. v. Harris Corp.*, 2019 WL 402332 (Del. Super. Ct. Feb. 12, 2009).

[25] See, e.g., Titan Inv. Fund II, L.P. v. Freedom Mortg. Corp., 2011 WL 532011 (Del. Super. Ct. Feb. 2, 2011).

[26] Note that the communication could nonetheless still be deemed privileged under *Kalisman* and *CBS*, as described in part III.B.1 above.

expectation of privacy from his or her employer. So this turns *Asia Global* into the second part of a two-part test.

*WeWork* appears consistent with this narrow interpretation of *Asia Global*. There was no meaningful discussion of the threshold question (i.e., the first part of the two-part test) of whether the employer's (Sprint's) access to the emails would destroy privilege, but it is clear that the court assumed it would. For example, Chancellor Bouchard noted that "[i]t is undisputed that none of the Documents concern the business or affairs of Sprint or any legal advice rendered for Sprint's benefit."[27] So Chancellor Bouchard assumed away the first part of the two-part test and proceeded directly to the second part, which is the *Asia Global* test. There is some further implicit recognition of a two-part test towards the end of the decision. There, Chancellor Bouchard rejected an argument of SoftBank on the basis that the cases cited by SoftBank all involved communications between parents and wholly-owned subsidiaries. That can be seen as an implicit endorsement of a two-part test: the *Asia Global* test may have been unnecessary had Sprint been a wholly-owned subsidiary of SoftBank such that information exchanges between SoftBank and Sprint would not have lost privilege.

Viewing *Asia Global* as the second part of a two-part test is not the only way to interpret it. It can instead be interpreted more broadly as a comprehensive test that evaluates whether an employee's use of an employer's email account destroys privilege. This interpretation involves no threshold question and proceeds straight to *Asia Global*'s four-factor test to determine whether the factors indicate that the employee's use of the email account destroys privilege. Doing so with our hypothetical, the first *Asia Global* factor asks whether the fund "maintain[s] a policy banning personal or other objectionable use." But whether the fund has such a policy would be irrelevant in our board designee case because the employee is not using the email account for personal use but for work use. The first factor, then, clearly does not indicate that privilege has been waived.

The third factor asks whether third parties have a right of access to the computer or emails. For *Asia Global* to be a comprehensive test, this factor must be interpreted as relating to third parties to whom disclosure would destroy privilege. For it to encompass third parties to whom disclosure would not destroy privilege would make the third factor irrelevant. For example, if the employee's attorney had a right to access the employee's computer or emails, that could not possibly indicate that privilege has been waived. Applying this logical interpretation of the third factor to our fund hypothetical, no third parties to whom disclosure would destroy privilege have a right of access to the employee's emails. So the third factor also does not indicate that privilege has been waived. Thus, two of the four factors indicate that privilege has not been waived. The second and fourth factors, which relate to the company's policy for monitoring emails and the employee's knowledge of such policies, considered on their own do not seem to support an argument that privilege has been waived, as they consider only the theoretical, as opposed to the actual, disclosure of potentially privileged communications. In sum, both the narrow and comprehensive interpretations of *Asia Global* indicate that a board designee's use of a fund email account should not generally destroy privilege.

[27] *In re WeWork Litig.*, 2020 WL 7624636, at *1.

### *Certain Limitations*

The foregoing analysis sets forth general principles that are subject to limitations. For example, use of a fund email account could cause privilege to be lost if the interests of the fund and the portfolio company become sufficiently adverse. This situation could arise if the adversity would cause the fund's receipt of privileged company information to destroy the privilege.
Under *Teleglobe*, the intra-group privilege exceptions may cease to apply to communications between the fund and the portfolio company if they become sufficiently adverse. Similarly, under *Kalisman*, the board designee is no longer entitled to receive privileged information if he or she becomes sufficiently adverse to the portfolio company's board "such that the director could no longer have a reasonable expectation that he was a client of the board's counsel."[28] By implication then, the fund would no longer be entitled to the information that the company board could now withhold from the board designee.[29] If the fund is no longer entitled to receive privileged information, the analysis would then turn on whether the board designee nonetheless had a reasonable expectation of privacy in his or her fund email account under *Asia Global*.

Also, the fund's email monitoring policy should include strict controls and procedures to ensure that the emails were never disclosed to a party who would destroy the privilege. For example, it could stipulate that email monitoring is performed solely by the fund's legal or compliance department or outside counsel. If, for example, the fund has lax monitoring controls under which company employees outside of the counsel's office can view the email contents or the email contents would otherwise become publicly available, a situation could be created in which privilege is lost.

It is also important to note that this post specifically analyzes information sharing under Delaware law and policy. Other jurisdictions may not recognize the same liberal information access for funds through their designees.[30] And privilege law is an inherently gray area. The contours of what can be shared with whom vary across jurisdictions and few cross-jurisdictional bright-lines exist to guide practitioners on inter-corporate communications.

This post focuses on use of an employer email account. Use of a personal email account like Gmail should not defeat the privilege of communications conducted through that account, assuming the user does not share the account and takes reasonable steps to ensure the confidentiality of the account.

## Conclusion

The above analysis concludes that directors appointed by investment funds should be able to communicate privileged information through their fund email accounts. This is good news for the many fund investment professionals who often sit on several portfolio company boards. It would be impractical to have a different email account for each portfolio company. And even if a different email account was used for each portfolio company, it would be difficult to keep the

---

[28] *Kalisman*, 2013 WL 1668205, at *5.

[29] There could also be an issue as to whether communicating with the board designee in and of itself, regardless of the method of communication, destroys privilege where there is sufficient adversity between the board designee and the board.

[30] See, e.g., Argos Holdings Inc. v. Wilmington, N.A., 2019 WL 1397150 (S.D.N.Y. Mar. 28, 2019).

accounts separate and ensure the correct account was always used for the correct portfolio company. As indicated at the end of Part III, portfolio companies and investment funds should be aware of the limits to this analysis. For example, investment funds should ensure that their email policies appropriately restrict which individuals are granted access to monitored emails.

Most of this post describes implications for investment funds with board designation rights. The discussion is also relevant for other types of investors, such as corporate venture investors with board designation rights. Many corporate venture investors obtain only observer rights instead of board designation rights, to which the *Kalisman* line of cases would not apply. Emailing privileged information to a board observer may result in the loss of privilege, regardless of which email account the observer uses.

This post also considers independent directors. The discussion for them is brief because the best practice for them is clearer: companies should not email privileged information to independent directors at their work email addresses.