Attorney-Client Privilege in the Digital Boardroom: What Companies Need to Know About the Delaware Court of Chancery's Recent Applications of the *Asia Global* Test to Better Protect their Directors' Privileged Communications

Boards of directors of companies incorporated in Delaware and elsewhere typically have "independent" or "outside" directors who are unaffiliated with that company, except through their board membership. Outside directors play important roles in corporate governance, providing fresh eyes for, and critical assessments of, board decisions big and small. But when an outside director communicates with fellow directors and company officers using an email account affiliated with another company, like her primary employer, recent precedents suggest that she may risk waiving the board's attorney-client privilege.

Under the four-factor test first set out in the U.S. Bankruptcy Court for the Southern District of New York in *Asia Global*,[1] outside directors' use of external email accounts can waive the attorney-client privilege. This article outlines important facets of the *Asia Global* test and the steps that can be taken to avoid a privilege waiver. It begins by explaining what the *Asia Global* test is, how it works, and its widespread adoption in other jurisdictions, including Delaware. It then discusses the Delaware Court of Chancery's adoption, refinement, and application of that test in recent cases. And it concludes by outlining important lessons that companies incorporated in and beyond Delaware can learn from these cases to protect the attorney-client privilege in the corporate boardroom in the digital age.

I. *Asia Global*'s Four-Factor Test

The *Asia Global* test determines when a company's right to manage or oversee the digital platforms that it provides undermines the confidentiality necessary to maintain the attorney-client privilege.[2] Thorny issues can arise under this test when an someone uses those digital platforms to communicate about privileged matters unrelated to the company hosting that digital platform. Companies oversee myriad digital platforms, from email accounts, web browsers, and servers, to the computers, tablets, and phones that they provide to their employees. The use of a company's digital platform for unrelated legal matters "does not, without more," destroy the confidentiality essential to a privilege claim.[3] But the nature and extent of the company's oversight of those digital platforms can provide the "more" that courts require to find a waiver. The *Asia Global* test allows courts to assess when "more" becomes "enough" to pierce the attorney-client privilege.[4]

In *Asia Global*, an insolvent company's bankruptcy trustee moved to discover emails among company insiders and their outside counsel about financial mismanagement that they had sent or received using the

---

[1] *In re Asia Glob. Crossing, Ltd.*, 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

[2] *See id.* at 251 (at issue "is whether an employee's use of the company email system to communicate with his personal attorney destroys the attorney-client, work product, or joint defense privileges in the emails"); *see generally, e.g.*, *Buttonwood Tree Value Partners, L.P. v. R. L. Polk & Co.*, 2021 WL 3237114, at *7 (Del. Ch. July 30, 2021) ("For the attorney-client privilege to attach, the communications between client and lawyer must be confidential.").

[3] *Asia Glob.*, 322 B.R. at 251.

[4] This article discusses only the attorney-client privilege, not the attorney-work-product privilege, because *Asia Global* treats them differently because of their distinct aims. *See id.* at 262–63 (discussing those two privileges separately because "[t]he work product privilege, unlike the attorney-client privilege, does not depend upon an expectation or intent that the communication will remain confidential"); *see also Billups v. Penn State Milton S. Hershey Med. Ctr.*, 2015 WL 7871029, at *3–4 (M.D. Pa. 2015) (noting *Asia Global*'s focus on attorney-client privilege).

company's email accounts, and which remained on the company's servers.[5] The trustee claimed that "the use of the corporate e-mail system waived any privileges that otherwise existed" in two ways. *First,* the trustee argued that the "mere use of the company's e-mail system" to conduct personal business "destroyed or waived any privilege." *Second,* the trustee claimed that because the company allegedly "maintained a corporate policy" allowing it to monitor those emails, that policy undercut any claim of confidentiality by the insiders.[6]

Because "[c]onfidentiality has both a subjective and objective component," the *Asia Global* court determined that the insiders had to show that they sent the emails in question "in confidence" and that they "reasonably underst[ood]" or expected that their confidentiality would be maintained.[7] Thus, the court had to decide whether the insiders' use of the company's email system—either on its own or under the company's policy on the use of that system—undermined the *reasonableness* of the insiders' expectation of privacy. The court began by noting the "prevailing view" that "lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality and privacy."[8] But the court recognized that because the insiders' emails did not "involv[e] company business," but "personal" matters, including matters potentially adverse to the company, the case raised thornier questions of confidentiality.[9]

To determine whether the insiders' emails remained confidential on company's system, the court turned to "'actual office practices or procedures'" and "'legitimate regulation[s],'" which the Supreme Court had held can "'reduc[e]'" an "employee's expectation of privacy in his office, desk, and files."[10] In so doing, the court set out four factors that "measure" the "expectation of privacy in [an employee's] computer files and email" in the workplace:[11]

1. Does the company maintain a policy banning personal or other objectionable uses?
2. Does the company monitor the use of employees' computer or email?
3. Can third parties access the computer or email?
4. Did the company notify the employee, or was the employee aware, of any such use and monitoring policies?

The court then applied those factors and made two findings: *First*, the court found that Asia Global "clearly had access to its own servers and any other part of the system where e-mail messages were stored,"

---

[5] *Asia Glob.*, 322 B.R. at 252 (noting that the trustee sought "the production of any electronic documents generated or received on Asia Global computer systems" (emphasis omitted)).
[6] *Id.*; *see id.* at 255 ("A communication is confidential when the circumstances indicate that it was not intended to be disclosed to third persons . . . ." (citation omitted)).
[7] *Id.* at 255 (emphasis omitted) (quoting *United States v. Schwimmer*, 892 F.2d 237, 244 (2d Cir. 1989)).
[8] *Id.* at 256 (citing, among other sources, ABA Formal Ethics Op. 99-413 (March 10, 1999)).
[9] *Id.*
[10] *Id.* at 257 (quoting *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987)). In *O'Connor*, the Supreme Court held that an employee had a reasonable expectation of privacy in his personal office because, among other things, "there was no evidence that the [employer] had established any reasonable regulation or privacy discouraging employees" from using company platforms for personal use. 480 U.S. at 719. The Court cautioned, however, that "the absence of such a policy does not create an expectation of privacy where it would not otherwise exist." *Id.*
[11] *Asia Glob.*, 322 B.R. at 257 (collecting cases assessing similar factors); *see also id.* at 259 ("[T]he objective reasonableness of [a user's] intent will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees.").

and so "sending a message over [the company's] email system was like placing a copy of that message in the company files."[12]

Second, despite the company's ability to access its employees' emails, the insiders' claims of confidentiality remained reasonable because the company's purported policy limiting email use for personal purposes had not been communicated clearly to employees.[13] In so holding, the court relied on a declaration from the company's former general counsel, who attested that "Asia Global did not enact or enforce a policy that e-mails on the company server belonged to the company," that "he never told anyone that Asia Global had such a policy," and that "he did not monitor any employee's email."[14] The court did so despite the existence *on paper* of "two corporate statements [that] set forth a policy banning personal use of the email-messaging system, and authorizing access and monitoring."[15] The court declined to credit those statements because they may have applied only to an affiliate,[16] and because the trustee had not shown that employees had actual or constructive notice of those policies.[17]

As a result, while the company perhaps *could* look at employees' personal emails on its servers, employees lacked adequate notice of the company's right to do that. Thus, the court held that the insiders' expectations of confidentiality remained objectively reasonable under the court's four-factor test for protecting the attorney-client privilege covering their digital documents.[18]

II. Delaware's Articulation of the *Asia Global* Test

Insert text Other jurisdictions have since adopted the reasoning of *Asia Global*.[19] In 2013, Delaware's Chancery Court joined those jurisdictions in *Information Management*,[20] in which the court gave stockholder plaintiffs access to executives' emails in which they "consulted with their personal lawyers and advisors about the[ir] alleged mismanagement using their work email accounts."[21] In doing so, the court elaborated on and helped clarify the four-factor test described in *Asia Global*—and applied it to corporate executives' communications in the digital boardroom. This section outlines Delaware's articulation of each *Asia Global* factor.

---

[12] *Id.* at 259.
[13] *See id.* at 259–61 ("The evidence is equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring employee e-mails.").
[14] *Id.* at 259.
[15] *Id.* at 260.
[16] *See id.*
[17] On constructive knowledge, the court cautioned that the company's "failure to warn the employees of an existing e-mail policy does not necessarily mean that the employees . . . were not on notice of the e-mail policy." *Id.* at 261. Among other things, the trustee could have (but had not) shown that the company posted notices of the policy on its on computers or required affirmative assent to those policies to access company computers. *See id.*
[18] *Id.* at 260–61.
[19] *See, e.g.*, *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 660–63 (N.J. 2010) (adopting and applying the *Asia Global* test and citing cases from New York, Pennsylvania, and Massachusetts applying similar tests); *Kannan v. Apple Inc.*, 2019 WL 5589000, at *3 (N.D. Cal. Oct. 30, 2019) ("Other courts in this district have applied the four-factor analysis described in *In re Asia Global* . . . for determining whether the attorney-client privilege or other protection may apply to an employee's communications transmitted or stored on an employer's computer.").
[20] *In re Info. Mgmt. Servs., Inc. Derivative Litig.*, 81 A.3d 278, 287 (Del. Ch. 2013) ("Numerous courts have applied the *Asia Global* factors or closely similar variants when analyzing the attorney-client privilege."); *see also id.* at 285 (before *Information Management*, "Delaware courts ha[d] not addressed whether an employee has a reasonable expectation of privacy in a work email account").
[21] *Id.* at 287 ("In the current case, the *Asia Global* factors weigh in favor of production.").

A. Clarity of Use and Monitoring Policies

Delaware focuses this factor on "the nature of specificity of the employer's policies regarding email use and monitoring," and favors production "when the employer has a clear policy banning or restricting personal use, where the employer informs employees that they have no right of personal privacy in work email communications, or where the employer advises employees that the employer monitors or reserves the right to monitor work email communications."[22] Although "'[a]n outright ban on personal use would likely end the privilege inquiry at the start,'" a "complete ban on personal use is not required."[23] By contrast, this factor favors employees' reasonable expectation of privacy when the company's policies are either nonexistent or unclear.[24] The court held that the company's policies at issue could have been more detailed, but still "sufficiently put [its] employees on notice that their work emails were not private."[25]

B. Policy Enforcement

Delaware has refined this factor "to focus on the extent to which the employer adheres to or enforces its policies and the employee's knowledge of or reliance on deviations from the policy."[26] While company monitoring policies are not 'use it or lose it,' an employee can "rel[y]" reasonably on a company's "specific representations or . . . actions inconsistent with the monitoring policy."[27] Even so, a company's reservation of the right to monitor cannot be undermined by "the absence of past monitoring or a practice of intermittent or as-needed monitoring."[28] The *Information Management* court ultimately treated this factor as neutral because while the company reserved the right to monitor, and employees recognized that their work accounts were "not confidential," the company had no history of enforcing its monitoring policy.[29]

C. Third-Party Access

Delaware treats this factor as duplicative of the first two factors in most cases.[30] Its effect is most pronounced "when analyzing webmail or other electronic files that the employer has been able to intercept, recover, or otherwise obtain."[31] In those cases, it focuses on two sides of one sword: the steps that the employee could have taken to maximize the privacy of his communications and the invasiveness of the company's actions to pierce that privacy.[32] In *Information Management,* the court gave this factor little weight because the case involved "work email" that the company could access on its own, and although the employees used subject lines notifying readers that their emails were privileged, "they failed to take more significant and meaningful steps to defeat access," like using a private email account unaffiliated with the employer or encrypting their communications.[33]

---

22 *Id.* at 287–88.
23 *Id.* (quoting *United States v. Finazzo*, 2013 WL 619572, at *8 (E.D.N.Y. Feb. 19, 2013)).
24 *Id.* at 288.
25 *Id.*
26 *Id.* at 289.
27 *Id.*
28 *Id.*
29 *Id.* at 290.
30 *Id.*
31 *Id.*
32 *Id.* at 291.
33 *Id.*

D. Employees' Actual or Constructive Notice of any Policies

Delaware has not changed this final factor. Employees' expectations of confidentiality remain reasonable when they lack actual or constructive knowledge of an access or monitoring policy.[34] For corporate executives, officers, and senior-level employees, courts "have readily imputed knowledge" of those policies to corporate executives, officers, and senior-level employees.[35] In *Information Management*, the employees at issue were among the company's "most senior officers," and they admitted knowing about the company's monitoring policies.[36] So the court found that the executives' expectations of confidentiality were objectively unreasonable.

III. The Delaware Court of Chancery's Recent Applications of the *Asia Global* Test

Insert In three recent cases, the Chancery Court has applied the *Asia Global* test, as refined in *Information Management*, when stockholder plaintiffs have sought to pierce the attorney-client privilege in the digital boardroom. This section discusses each case in turn.

A. *DLO Enterprises, Inc. v. Innovative Chemical Products Group, LLC*[37]

This discovery dispute arose from an asset acquisition after which one of the sellers' officers continued working for the post-acquisition entity and sent purportedly privileged emails *after* the acquisition to the sellers' lawyers using an email account that came to be acquired by the buyers.[38] In litigation, the buyers sought those emails, arguing that any expectation of confidentiality between that officer and the sellers' lawyers was unreasonable because "those emails have always been in the [b]uyers' possession," and so no privilege attached.[39]

Applying *Asia Global*, Vice Chancellor Zurn found that the four factors favored the emails' production.[40] *First*, the court found that while the post-acquisition entity "did not place an outright ban on personal use," its employee handbook said that "employees did not have an expectation of privacy and . . . that the company reserved the right to access employees' email accounts at any time."[41] Thus, the court looked to multiple sources to determine the company's policies on use and monitoring. *Second*, the court found that the buyers had not shown that they ever exercised the company's rights under the policy, and so that factor remained "neutral" since the sellers bore the burden to show that the privilege applied.[42] *Third*, the court found that in this "straightforward work email case," when the sellers' officer continued working for the buyers after the acquisition, third parties' rights of access were "largely duplicative of the first and second factors" and thus also favored production.[43] *Fourth*, the court found that the sellers' officer had notice of the company's use and monitoring policies because "at the bottom of the numerous emails that the [sellers] sent, [the company] applied a disclaimer stating that 'messages sent to and from employees in our organization may

---

34 *Id.*
35 *Id.* at 292.
36 *Id.*
37 2020 WL 2844497 (Del. Ch. June 1, 2020).
38 *Id.* at *2
39 *Id.*
40 *See id.* at *7–9.
41 *Id.* at 8.
42 *Id.*
43 *Id.* at *9.

be monitored.'"[44] Although the emails apparently did not cite or link to any policies or handbooks, they warned users that such policies existed.

The court ultimately found that no privilege applied and so the emails at issue had to be produced, reasoning that each *Asia Global* factor either favored production or was neutral.[45]

B. *In re WeWork Litigation*[46]

This decision grew from a high-profile litigation between WeWork's founder (Adam Neumann) and SoftBank (a WeWork investor) over an unconsummated additional multi-billion-dollar investment by the bank in the company.[47] Around the time of that potential investment, Softbank also had a controlling interest in the cell-phone carrier Sprint.[48] Like many directors of affiliated companies, some of SoftBank's document custodians "wore multiple hats" at SoftBank, Sprint, and WeWork.[49] While it is common for officers and directors to play different roles for different entities, SoftBank's custodians sent purportedly privileged emails about SoftBank business using email accounts that *Sprint* controlled, not WeWork or SoftBank.[50] And those custodians did so despite having "access to email accounts other than their Sprint email accounts that they could [have] use[d] for [SoftBank]-related matters."[51] WeWork's founder claimed that the custodians' use of Sprint's email domain eliminated the confidentiality necessary for SoftBank to assert that the emails at issue were privileged.[52]

To resolve the motion to compel, Chancellor Bouchard applied the *Asia Global* factors, as refined in *Information Management*, finding that "each of the[ ] four factors weigh in favor of production."[53] For the first factor, the court found that Sprint—which maintained the email accounts at issue—had a code of conduct that warned employees that they had "no expectation of privacy," that Sprint reserved the right to monitor their communications, and that the clarity of the code of conduct outweighed the lack of an express ban on personal use of email.[54] As for the second factor, the court noted that neither party had submitted evidence of Sprint's enforcement of its use and monitoring policies, which it weighed against SoftBank, who had the burden.[55] The court further noted that, under *Information Management*, the code of conduct's clear reservation of the right to monitor employee emails made "the absence of past monitoring" less relevant.[56] On the third factor, the court noted that it is usually "duplicat[ive]," but found that it weighed against SoftBank because its custodians could have, but did not, seek to thwart third parties' access by, among other things, using an unaffiliated email account or encrypting their communications.[57] And on the fourth factor, the court made

---

[44] *Id.* (quoting disclaimer).
[45] *See id.* at 9 ("[T]here of the four *Asia Global* factors point towards production and one is neutral."). The court did not immediately order production. Instead, it requested supplemental briefing on "a potential statutory override of the *Asia Global* analysis," *id.* at *10, which this article discusses below in Section V.
[46] 2020 WL 7624636 (Del. Ch. Dec. 22, 2020). Please be advised that Quinn Emanuel Urquhart & Sullivan, LLP served as counsel to defendant SoftBank Vision Fund (AIV M1) L.P. in this litigation.
[47] *Id.* at *1.
[48] *Id.*
[49] *Id.* For example, SoftBank's chief operating officer also served as a chair of both WeWork and Sprint, and Sprint's CEO assisted SoftBank's chief operating officer on WeWork-related matters. *Id.*
[50] *Id.* ("The [d]ocuments [at issue] were sent to or from Sprint email accounts . . . . It is undisputed that none of the[se] [d]ocuments concern the business affairs of Sprint or any legal advice rendered for Sprint's benefit.").
[51] *Id.* at *2 (one custodian had a "WeWork-related Gmail account," and the other had a "softbank.com" email account).
[52] *Id.* ("Neumann's motion turns on one issue: Did [the SoftBank custodians] have a reasonable expectation of privacy when using their Sprint email accounts for [SoftBank]-related purposes such that the [d]ocuments [at issue] would constitute 'confidential communications' under Delaware Rule of Evidence 502?" (emphases omitted)).
[53] *Id.*
[54] *Id.* at *2–3 (quoting code of conduct).
[55] *Id.* at *3.
[56] *Id.* (quoting *Info. Mgmt.*, 81 A.3d at 289).
[57] *Id.* at *4.

three findings against SoftBank: (1) the custodians at issue—two of Sprint's senior-most executives—had constructive notice of the code of conduct,[58] (2) the custodians had actual notice of confidentiality concerns over their use of Sprint email accounts for SoftBank-related purposes, and (3) SoftBank itself "was aware of the risks to maintaining privilege when commingling the resources of separate corporate entities, including email accounts."[59]

Because each factor cut against SoftBank, the court ordered that the emails be produced.[60] In so doing, the court also "decline[d] to deviate from the *Asia Global* framework simply because the party seeking to overcome the privilege is not the corporation whose email system was used for non-work related purposes," but a third-party litigant adverse to the company asserting the attorney-client privilege.[61]

C. *In re Dell Technologies Inc. Class V Stockholders Litigation*[62]

Finally, this recent discovery dispute, which arose during a multi-billion dollar stockholder class action against the controlling stockholders of Dell Technologies,[63] concerned privilege assertions potentially undermined by one of Dell's outside director's use of an outside email account to conduct business on behalf of Dell and a special committee that Dell created to evaluate the transaction at issue. Outside director William Green had used an email account maintained by Accenture, the company that he had once been CEO of, to conduct his duties as an outside director of Dell.[64] Although Green had retired from Accenture, the company allowed him to keep using his email account, and Green continued to use it for myriad purposes "unrelated to the business of Accenture."[65]

The stockholder plaintiff moved to compel the production of those emails and challenged Dell's and Green's attorney-client-privilege assertions under *Asia Global*.[66] Vice Chancellor Laster (who also wrote the *Information Management* decision) denied the motion to compel, finding that Green's use of his Accenture account following his retirement meant his expectation of confidentiality in that account was objectively reasonable.[67]

In so holding, the court stressed that the first factor—the existence and nature of a company's use and monitoring policies—"is the dominant factor" under *Asia Global*.[68] The court held that while Accenture had clear use and monitoring policies,[69] a company "can have a policy that would not lead to a reasonable expectation of privacy under some circumstances and would allow for a reasonable expectation of privacy in

---

[58] *Id.* ("[SoftBank] has not submitted any evidence that [the custodians] were unaware of the . . . Code of Conduct, and it is hard to imagine that they would have been unaware [given their senior positions].").
[59] *See id.* (one custodian warned the other that "the confidentiality of [SoftBank] information was at risk if it was not walled off from Sprint," which "negate[d] any reasonable expectation of privacy . . . [when] using [the] Sprint email account for [SoftBank]-related purposes"); *id.* at *5 ("[M]ultiple [SoftBank] employees . . . raised concerns about protecting [its] information and, more importantly, its legal privileges.").
[60] *See id.* at *5.
[61] *Id.*; *see id.* at *5 n.40 (collecting cases in which courts applied the *Asia Global* test and pierced companies' attorney-client privilege when the party seeking production was an outsider).
[62] Consol. C.A. No. 2018-0816-JTL (Del. Ch. Sept. 17, 2021) (TRANSCRIPT) ("*Dell Class V*"). Please be advised that Quinn Emanuel Urquhart & Sullivan, LLP currently serves as Co-Lead Counsel to Lead Plaintiff in this litigation.
[63] *See generally In re Dell Techs. Inc. Class V Stockholders Litig.*, 2020 WL 3096748 (Del. Ch. June 11, 2020) (denying in part defendants' motion to dismiss).
[64] *Dell Class V*, at 44–45.
[65] *Id.* at 45.
[66] *See id.* at 44–45.
[67] *See id.* at 48 (noting that *Asia Global* motions are "not a situation where [courts] can establish bright-line rules").
[68] *Id.* at 55.
[69] The parties disagreed on which policies applied: those in effect when Green was active at Accenture, or those in effect when the emails at issue were sent. The court found that the later policies mattered most under *Asia Global*. *Id.* at 50 ("[W]hat matters is the policy that's in place when the person is using the system.").

other circumstances, *depending on the nature of the use*."[70] The applicable Accenture policy did just that: although it encouraged employees to use personal emails or protective language for confidential or privileged external matters,[71] it respected personal use except in certain specifically enumerated circumstances, like using the email account for illegal activity or activity that implicated the company.[72] The court found that none of those exceptions applied Green's emails, particularly because as a since retired executive, nearly all his emails on that account were for personal use.[73] Thus, the court held, for Green, Accenture functioned less like an email monitor and more like "a third-party [email] provider" like "Google" or "AOL."[74] As a result, Green could use his Accenture email account for non-Accenture business while reasonably expecting that those communications would remain confidential.[75]

The court continued by evaluating the remaining *Asia Global* factors. For the second factor, the court held that while Accenture claimed that it never monitored Green's emails, the relevant inquiry is whether the company monitors generally, and not just the specific person(s) at issue.[76] So that factor favored production. The third factor also cut slightly in favor of production, because Green could have, but did not, use a "remote" or "web-based" email system like a Gmail account to conduct non-Accenture business.[77] And on the fourth factor, the court noted that Green admitted knowing generally of Accenture's monitoring policies, and that as the company's former CEO, he also had constructive knowledge of those policies.[78] Thus, while the remaining *Asia Global* factors favored production slightly, the first factor proved dispositive for Green's emails.

IV. How Companies can Protect the Attorney-Client Privilege in the Digital Boardroom

This final section outlines suggestions for steps that may be taken to protect the attorney-client privilege in the digital boardroom, taking lessons from *Asia Global*, *Information Management*, and their recent progeny in Delaware's Chancery Court. Although each motion under the *Asia Global* test is decided on a "case-by-case basis,"[79] companies that follow these steps with their outside directors can help better position themselves to defeat litigants' attempts to pierce their privilege. These steps can be broken into two broad categories: affirmative steps that companies may take to better protect their attorney-client privilege, and investigative

---

[70] *Id.* at 49 (emphasis added).
[71] *Id.* at 51.
[72] *Id.* at 50–53.
[73] *Id.* at 53 ("This is particularly pertinent to Green, who, because of his retirement from [Accenture], was essentially only engaged in non-company-related business. One could say that it was all personal for him at that point."); *see id.* at 54 (explaining why it was objectively reasonable for Green to understand that none of Accenture's monitoring triggers applied to his emails post-retirement).
[74] *Id.* at 55.
[75] *See id.* at 58 ("[A]n objectively reasonable view of this relationship is that Green had good reason to think that his emails would not be accessed and would remain confidential, vis-à-vis the world and people like the plaintiff, unless he was engaging in some behavior that would raise suspicions at Accenture and cause them to have to do some type of investigation.").
[76] *See id.* at 55–56.
[77] *See id.* at 56–57. The court admonished Green for not taking these other steps to preserve the confidentiality of Dell's or other companies' communications. *See id.* at 57.
[78] *See id.* at 57–58.
[79] *Asia Glob.*, 322 B.R. at 257.

steps that companies can pursue. Both sets of steps aim to make companies' and their directors' expectations of confidentiality more reasonable under the *Asia Global* test.[80]

A. Affirmative Steps

1. Provide outside directors with an email account in the company's name and require that they can use to conduct business with and on behalf of the board of directors.

2. Require outside directors to conduct board business using personal email accounts unaffiliated with any other company (e.g., a Gmail account).

Under *Asia Global* and its progeny, these two protective measures can help ensure that outside directors' expectations of confidentiality will be found objectively reasonable.[81] When an outside director conducts board business using an email account maintained by the company for which she is an outside director, no third party to the attorney-client relationship has access to the digital boardroom in the first place, preserving confidentiality and thus the attorney-client privilege. Even when this measure would, for whatever reason, be difficult to implement or enforce, companies can still protect their privilege by (i) requiring outside directors to use personal email accounts maintained by email "common carriers" like Google for official board business (particularly carriers that offer encryption options), and (ii) encouraging outside directors to mark privileged communications as "privileged" and "confidential" in their subject lines and putting them into clearly marked folders. Whichever policy a company adopts, it should take care to memorialize that policy in writing, documenting the mandate that outside directors take these steps to preserve the confidentiality of the company's communications.[82]

3. When outside directors cannot be made to conduct board business using protected email accounts, require that they take affirmative steps to keep communications about board business as confidential as possible.

When outside directors are unable to conduct board business using a company email account or a secure personal account like a Gmail account, companies may also opt to protect themselves by requiring outside directors to underscore the privacy of their board-related communications when possible by (i) encrypting their confidential emails; (ii) marking them "privileged," "private," or "confidential"; and (iii) keeping those communications in separate, explicitly labeled folders. Delaware courts have pointed to these protections as among the "lesser things" that outside directors can do to retain the attorney-client privilege.[83]

---

[80] These steps each involve companies' relationships to other corporations or third parties, and not relationships between parents and wholly owned subsidiaries, which are different for purposes of the attorney-client privilege. *See WeWork*, 2020 WL 7624636, at *5 n.41 (collecting cases).

[81] *See Dell Class V*, at 59 ("I think a strong argument can be made that the better course is for outside directors to have an email account that they can be confident is not subject to potential monitoring. One can debate whether that's one for each board or one for all of their boards, or whether it's a Gmail account or some other type of more-secure provider. Regardless, that type of corporate hygiene goes a long way to avoiding these types of motions.").

[82] When necessary, such formal policies can also provide penalties for outside directors' breaches—*e.g.*, if an outside director auto-forwards company emails to accounts maintained by other companies. *See WeWork*, 2020 WL 7624636, at *2 (noting that SoftBank's custodians could have, but did not, use other, more-confidential email accounts, like a "WeWork-related Gmail account" or a "softbank.com" email account).

[83] *Dell Class V*, at 42 ("[E]ven the lesser things that Green could have done weren't done in this case. He didn't specifically mark things private. He didn't specifically put anything in the [subject] line to say it was confidential. He didn't put emails in a separate folder. He didn't use encryption."); *WeWork*, 2020 WL 7624636, at *4 ("[SoftBank] has

4. Require outside directors to conduct board business digitally by email and prohibit conducting board business by text message.

Although *Asia Global* and its progeny concern the confidentiality of emails that third parties could monitor, text messages can threaten confidentiality in similar ways, particularly when outside directors use mobile devices (*e.g.*, smartphones or tablets) or phone numbers provided to them by their primary employers. Thus, companies can help prevent privilege waivers by adopting policies formally prohibiting all directors, and especially outside directors, from communicating about confidential board business by text message.

B. Investigatory Steps

1. Know what platforms outside directors use to communicate about board business, including email accounts, phone numbers, and mobile devices—and whether any of those platforms are maintained by non-service-provider entities.

2. For all communication platforms maintained by other companies, like an outside director's primary employer, get to know the use and monitoring policies that apply to those platforms.

Companies can also take steps to learn how and by what means their outside directors communicate about board business. If outside entities (other than service providers such as Google for Gmail) can monitor any of those platforms, then the company should understand whether those outside entities have the right to monitor those platforms and, if so, under what circumstances, to assess potential risk to the company's attorney-client privilege. Companies can protect themselves better by knowing those outside policies, and potential risk factors, *before* a litigant seeks to pierce their privilege. This is especially important given the "dominant" weight that the *Dell* court gave to *Asia Global*'s first factor.[84]

3. Determine outside directors' current or potential future roles with any outside entities that maintain their communication platforms.

Companies can also investigate their outside directors' current and potential future positions with any companies that could or do monitor their means of communication (*e.g.*, email accounts or mobile devices). As the *Dell* court underscored, when Green sent the emails at issue, he had retired from an active position with Accenture, and so his use of his Accenture email were "all personal for him at that point."[85] By contrast, the executives and officers at issue in *WeWork* and *DLO Enterprises* all had active roles with the companies that maintained their communication platforms.[86] So knowing the nature and extent of outside directors' current and potential positions with other entities may help assess potential confidentiality risks.

4. Determine whether any outside entities with a right of access are headquartered in states that protect users' privacy by statute.

Where an entity bases its operations can also affect the assertion of privilege. If that state's laws protect users' privacy, then those laws may create a "statutory override" for the *Asia Global* test by giving textual

---

not provided any compelling evidence that [its custodians] took 'significant and meaningful steps to defeat access' by . . . 'shifting to a webmail account or encrypting their communications.'" (quoting *Info. Mgmt.*, 81 A.3d at 290)).

[84] *Dell Class V*, at 55.

[85] *Id.* at 53.

[86] *See WeWork*, 2020 WL 7624636, at *1; *DLO Enters.*, 2020 WL 2844497, at *1–2.

weight to the reasonableness of users' expectations of privacy.[87] The same is true for entities incorporated in Delaware but base their operations in foreign nations.[88]

In sum, by installing these protections, and investigating how outside directors conduct business with and on behalf of the board of directors, companies can better ensure that the board's communications remain confidential and privileged.

V. Conclusion

Asia Global suggests that companies can assert the attorney-client privilege in the digital boardroom when everyone's expectations of confidentiality are objectively reasonable. Companies and their general counsels should thus take care to ensure that outside directors use appropriately secure and confidential email accounts when communicating with fellow directors and their officers and employees about privileged company matters. If they fail to do so, then communications in the digital boardroom could become discoverable under the *Asia Global* test, depending on the circumstances.

***

If you have any questions about the issues addressed in this memorandum, or if you would like a copy of any of the materials mentioned in it, please do not hesitate to reach out to:

Silpa Maruri
Email: silpamaruri@quinnemanuel.com
Phone: 212-849-7211

George Phillips
Email: georgephillips@quinnemanuel.com
Phone: 212-849-7164

To view more memoranda, please visit www.quinnemanuel.com/the-firm/publications/
To update information or unsubscribe, please email updates@quinnemanuel.com

[87] *See Info. Mgmt.*, 81 A.3d at 292. Although Delaware has such a statute, *see* 19 *Del. C.* § 705(b), it "applies only to businesses operating in Delaware, not to Delaware entities who operate elsewhere but choose Delaware as their corporate home." *Info. Mgmt.*, 81 A.3d at 292 (citing *Klig v. Deloitte LLP*, 36 A.3d 785, 797–98 (Del. Ch. 2011)). The *Information Management* court also looked to federal statutes, and state statutes where the company was headquartered, but held that none provided users with a robust expectation of confidentiality over their emails. *See id.* at 293–96 (discussing the Federal Wiretap Act, 18 U.S.C. §§ 2510–13, the Federal Communications Act, 18 U.S.C. §§ 2701–13, and similar Maryland statutes).

[88] *See Lynch v. Gonzalez*, 2019 WL 6125223, at *6, *10 (Del. Ch. Nov. 18, 2019) (finding that the "statutory override" applied because "under Argentine law, Plaintiffs had a reasonable expectation of privacy in the [ ] emails [at issue]"); *see also DLO Enters.*, 2020 WL 2844497, at *9 (ordering "supplemental briefing on [the] statutory override," which "[t]he parties ha[d] failed to brief").