Harvard Law School Forum on Corporate Governance

Law Governing Attorney-Client Privilege for Emails Hosted on Noncompany Servers

Posted by Edward B. Micheletti, Lauren N. Rosenello, and Trevor T. Nielsen, Skadden, Arps, Slate, Meagher & Flom LLP, on Wednesday, January 19, 2022

Editor's note: Edward B. Micheletti is partner and Lauren N. Rosenello and Trevor T. Nielsen are associates at Skadden, Arps, Slate, Meagher & Flom LLP. This post is based on their Skadden memorandum, and is part of the Delaware law series; links to other posts in the series are available here.

Delaware Rule of Evidence 502(b) codifies the attorney-client privilege and insulates from discovery "confidential communications made for the purpose of facilitating the rendition of professional legal services to the client." Rule 502(a)(2) further provides that 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." But what happens when such communications are sent using email accounts that can be accessed by third parties that would normally destroy the privilege?

In 2013, the Delaware Court of Chancery adopted a framework for answering this question, and several recent opinions have applied the framework in various contexts to decide if the attorney-client privilege was maintained. This post analyzes the relevant opinions and provides practical guidance to companies aiming to protect the attorney-client privilege.

The rulings suggest that companies should consider requiring directors and employees to use a company-provided email account or some other email account not subject to potential monitoring when communicating with counsel. Where that is not possible, in-house counsel should carefully evaluate the policies of alternative email systems.

Information Management: Four Factors Analyzed

In a 2013 opinion, *In re Information Management Services, Inc. Derivative Litigation*,[1] Vice Chancellor Laster was the first to address the issue in Delaware of whether a party had a reasonable expectation of privacy over communications made using a company email account for personal use. In *Information Management Services*, company executives used their company email accounts to correspond with their personal lawyers.

In evaluating whether the executives could maintain privilege over the emails, the court adopted the four-factor analysis set forth in *In re Asia Global Crossing, Ltd*., a 2005 opinion from the

[1] 81 A.3d 278 (Del. Ch. 2013).

United States Bankruptcy Court for the Southern District of New York[2]: (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 emails? (4) Did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

Applying the *Asia Global* factors, the court in *Information Management Services* found that three of the four factors weighed against a reasonable expectation of privacy and one factor was neutral. The court also held there was no statutory override that would alter the common law analysis, and it therefore ordered the production of the otherwise-privileged emails.

Lynch v. Gonzalez: Statutory Override

Six years later the issue arose again in *Lynch v. Gonzalez*[3] with Vice Chancellor Morgan T. Zurn holding that the emails in question were privileged because of a statutory override of the controlling jurisdiction. The underlying dispute related to whether one of the plaintiffs, an individual, had properly acquired a majority ownership of Belleville Holdings, a Delaware LLC that was a holding company for ownership interests in various Argentine companies.

The defendant, a former co-manager of Belleville, was ousted by the individual plaintiff as manager but remained a minority holder of Belleville, which was also a plaintiff. The defendant controlled email servers that Belleville previously used and which it was attempting to access in order to comply with its discovery obligations. Defendant denied plaintiffs access and searched the email himself, including emails over which plaintiffs claimed attorney-client privilege.

Defendant argued that plaintiffs had no expectation of privacy in emails sent on the server because they knew defendant could access them. While the court found that the *Asia Global* factors suggest the emails were not confidential, plaintiffs proved that Argentine law[4] provided a statutory override and that plaintiffs had rights of privacy in the email.

In re WeWork Litigation: Use of Another Company's Email

The following year, the issue arose again in *In re WeWork Litigation*,[5] when plaintiffs sought to compel defendant SoftBank Group Corp. to produce emails that were sent to or from email accounts hosted by nonparty Sprint, Inc.[6] During the relevant time periods, SoftBank was the majority owner of Sprint and an investor in WeWork, but Sprint was not involved in the WeWork litigation.

---

[2] 322 B.R. 247 (Bankr. S.D.N.Y. 2005).

[3] 2019 WL 6125223 (Del. Ch. 2019).

[4] To determine which law governed the email server, the court looked to the place where the company that has custody of the emails "conducts its business."

[5] 2020 WL 7624636 (Del. Ch. Dec. 22, 2020).

[6] Vice Chancellor Zurn also addressed the issue again the next year in *DLO Enterprises, Inc. v. Innovative Chemical Products Group, LLC*, 2020 WL 2844497 (Del. Ch. June 1, 2020), but despite finding that three of the four factors pointed towards production and one was neutral, declined to rule pending supplemental briefing on a potential statutory override.

At the time, SoftBank's COO simultaneously served as chairman of Sprint and WeWork. Additionally, Sprint's CEO — using his Sprint email account — assisted SoftBank's COO with matters related to SoftBank and WeWork. Another Sprint employee was seconded to SoftBank to work as the chief of staff to the SoftBank COO and communicated with the COO using her Sprint email account. SoftBank asserted attorney-client privilege and withheld certain relevant emails that were sent to or from the Sprint email accounts of Sprint's CEO and the Sprint employee who was on secondment to SoftBank.

Applying the *Asia Global* factors as adopted in *Information Management Services*, the court concluded that all four factors weighed in favor of ordering the production of the emails. The court explained that the first factor — does the corporation maintain a policy banning personal or other objectionable use — does not necessarily require an explicit ban on personal use of email. Rather, citing *Information Management Services*, the court explained that the first factor "has been held to weigh in favor of 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."[7]

Because Sprint's policy stated that "[e]mployees should have *no expectation of privacy* in information they send [or] receive" on Sprint's network, and that "Sprint reserves the right to review workplace communications (including … *email* ….)," [8] the court concluded that the first factor weighed in favor of production.

Applying the second factor — does the company monitor the use of the employee's computer or email — the court noted that neither side provided evidence regarding whether Sprint actually monitored its employees' emails, but explained that the absence of any such evidence, combined with the language in Sprint's policy explicitly reserving the right to monitor emails, weighed in favor of production.

For the third factor — do third parties have a right of access to the computer or emails — the court noted that "[i]n a dispute like this concerning use of work email, the third factor 'largely duplicates the first and second factors, because by definition the employer has the technical ability to access the employee's work email account.'"[9] Because there was no compelling evidence that the Sprint employees took "significant and meaningful steps to defeat [Sprint's] access" to the emails,[10] the court concluded that the third factor weighed in favor of production.[11]

Applying the fourth factor — did the corporation notify the employee, or was the employee aware of the use and monitoring policies — the court explained that "[i]f the employee had actual or constructive knowledge of the policy, then this factor favors production because any subjective expectation of privacy that the employee may have had is likely unreasonable."[12] In addition to explaining that knowledge of the policy may be imputed to officers and senior employees, the

---

[7] *Id*. at *2 (citing *In re Info. Mgmt. Servs*., 81 A.3d at 287).
[8] *Id*. at *3.
[9] *Id*. at *4 (citing *In re Info. Mgmt. Servs*., 81 A.3d at 290).
[10] *Id*. (citing *In re Info. Mgmt. Servs*., 81 A.3d at 291).
[11] The court also found it noteworthy that the Sprint employees had access to either a WeWork- or a SoftBank-provided email account that they could have used for the SoftBank-related business as an alternative to their Sprint email accounts.
[12] *Id*. (citing *Info Mgmt. Servs*., 81 A.3d at 291-92).

court noted that the record supported the conclusion that the employees were either aware of the policy or at least were aware of the confidentiality concerns between SoftBank and Sprint. The court therefore concluded that the fourth factor likewise favored production.

Given that all four factors weighed in favor of production, the court held that there was no reasonable expectation of privacy over the emails at issue and ordered their production.[13]

In re Dell Technologies Inc. Class V: A Reasonable Expectation of Privacy

Several months later, the issue arose again in *In re Dell Technologies Inc. Class V Stockholders Litigation*.[14] In *Dell*, the court addressed whether an outside director of Dell had a reasonable expectation of privacy regarding Dell-related emails he sent or received from an email account hosted by his former employer, Accenture LLP. The case highlights again the importance of the language of the email host's privacy policies.

The director was a former CEO of Accenture who had since retired, but he continued to use his Accenture email account. In addition to his service as an outside director for Dell, the director served on the board of several other companies and used the Accenture email account for his communications for all of his board service.

Plaintiffs sought to compel the production of over 900 emails sent to or from the director's Accenture email account, over which the director asserted attorney-client privilege. The court applied the four-factor test from *Asia Global* to hold that the director had a reasonable expectation of privacy regarding the emails.

In addressing the first factor, the court explained that "[t]his factor will favor production when the company has a policy banning personal use or where the company informs users that they have no right to privacy in communications that use that email account."[15] However, the relevant Accenture email policy in place at the time of the communications "acknowledged that personal use was permissible, that Accenture indicated that it would respect personal use except in specific circumstances, and also that Accenture would need to engage, and would engage, in systemwide monitoring to protect the entity and the system."[16]

The court pointed to specific language in the policy that stated that personal use was allowed as long as the use did not "Interfere with on-going work; Adversely affect the problem handling or security of Information; or Create a significant overload on [Accenture's] Technology."[17] The policy also encouraged employees to mark items as "private" or "personal" if they wished to protect the privacy of their communications, but stated that Accenture "maintains the right … to open items that are marked 'private' or 'personal'" in certain circumstances. Those circumstances included "if there is a reasonable suspicion that the communication is really not personal but is, in fact, business related; … if there's a reasonable suspicion that there's been a criminal offense …; if access is needed in connection with a company-related litigation or an internal external

[13] The court did not address whether there was a statutory override.
[14] C.A. No. 2018-0816-JTL (Del. Ch. Sept. 17, 2021) (TRANSCRIPT).
[15] *Id*. at 49.
[16] *Id*. at 50-51.
[17] *Id*. at 51.

investigation; … [and] inadvertent access during the company's general monitoring activities ….”[18]

The court found that the policy “creates a sense in the ready that they have some expectation of privacy in using [Accenture's] system.” The expectation of privacy was heightened in the director's case, the court found, because the director was completely retired from Accenture, and therefore his use of the Accenture email account was entirely personal and noncompany related. The court explained that, in light of the policy, because the director “wasn't interfering with anybody's ongoing work at the company,” “wasn't affecting the company adversely,” “wasn't creating a systemic overload,” and “wasn't engaging in anything that looked like illicit behavior,” the director had a reasonable expectation of privacy over his emails.[19]

The court distinguished this situation from that in *WeWork*, noting that *WeWork* involved a stricter policy and “[t]here were also differences in terms of the involvement in the litigation of the sponsor of the email system.” Unlike the Sprint email accounts at issue in *WeWork*, because the Dell director was retired, Accenture's relationship with him “is more akin to a third-party provider. It isn't all the way analogous to a Google or an AOL or a Hotmail, but … Accenture was providing him with services analogous to that,” the court said.[20] Having found the case distinguishable from *WeWork*, the court concluded that the first factor weighed against production.

The court addressed the three other *Asia Global* factors, and found that each weighed in favor of production. However, the court nonetheless held that the director had a reasonable expectation of privacy, explaining that the first factor “really is the dominant factor in the four-factor analysis.”

Although the court found that the director in this instance could maintain privilege over the emails in question, the court provided practical advice on how best to keep outside directors' communications confidential:

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.[21]

Takeaways

- As the court explicitly advised in *Dell*, one way to maintain privilege and confidentiality over outside director email communications is to require that the director use a company-provided email account or some other email account not subject to third-party monitoring, or communicate through a secure board portal.
- *WeWork* suggests that the same is also true for company employees, whether permanent or temporary. The best practice for a company to ensure that its employees'

[18] *Id*. at 52-53.
[19] *Id.* at 54.
[20] *Id*. 55.
[21] *Id*. at 59.

communications are kept confidential is to require all employees to use a company-provided email or third-party-hosted account where emails are not monitored.

- If it is impracticable for outside directors or employees to use a company-provided email account, in-house counsel should consider reviewing the policy that governs the external email accounts to evaluate whether there are ways to maximize the confidentiality of communications. For example, if the policy requests that users store personal emails in a separate folder, in-house counsel should encourage the outside director or employee to segregate relevant communications.
- Finally, in-house counsel should consider whether there are any statutes in the jurisdictions in which they operate that could impact their own policies regarding email access or those of their outside directors or employees that use noncompany email accounts.