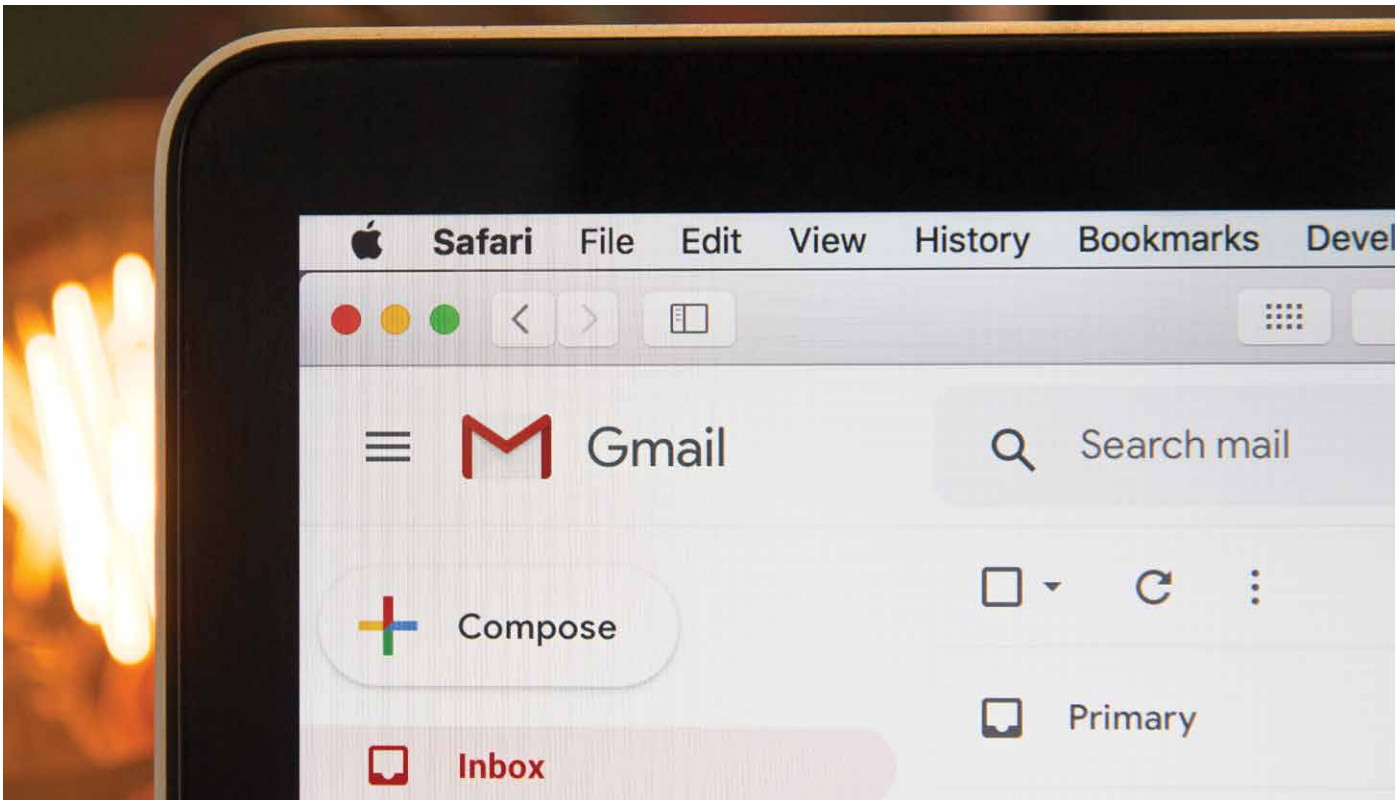

Protecting Email Privilege

Directors' use of external work email leaves the correspondence vulnerable.

BY DOUG RAYMOND

Every business depends on email to communicate with its key constituencies, including directors. However, a recent Delaware Chancery Court decision reminds us of the risks directors run when they rely on email to communicate sensitive matters. The decision provides another reason why directors should think twice before hitting "send" on their next board-related email.

In the *In re WeWork Litigation* case, the court found that individuals who were using their employer's email to communicate about issues related to another business — in this case, WeWork — could not assert the attorney-client privilege over those communications because they had used their employers' email system. The attorney-client privilege protects confidential communications between an attorney and a client for the purpose of obtaining or providing legal advice. The privilege not only protects disclosure of facts that a client communicates to a lawyer in order to receive legal advice but also covers the legal advice the lawyer provides to the client. For this reason, it can be devastating to lose the benefit of the privilege. But privilege is lost when communications are not confidential.

In the *WeWork* case, several individuals employed by Sprint — which had no role in the underlying litigation — had business relationships with WeWork and Softbank. For example, Softbank's COO also served as chairman of the board of both WeWork and Sprint. These individuals sent or received almost 90 emails, using the Sprint email system to communicate with Softbank's lawyers regarding WeWork. The emails related solely to SoftBank and WeWork and did not concern the business or affairs of Sprint or any legal advice rendered for Sprint's benefit.

These communications were later identified by plaintiff's counsel during a lawsuit involving WeWork. Softbank tried to hold back the documents, claiming that they were confidential and were subject to the attorney-client privilege. The Delaware Chancery Court disagreed, finding that the Sprint employees had no "reasonable expectation of privacy" in the emails. The court's decision focused on Sprint's code of conduct, which stated that employees had no expectation of privacy when using Sprint's email system and further permitted Sprint to review employee emails. The individuals involved were presumed to have knowledge of Sprint's policies and so were unable to assert the attorney-client privilege and had to turn over their sensitive emails. (While Softbank owned a majority of the equity in Sprint, the decision did not turn on that relationship. In fact, if Sprint had been a wholly owned subsidiary, the result might have been different, as communications between a parent and its wholly owned subsidiary are generally covered by joint-client privilege, which covers communications between corporate entities with a centralized legal department.)

To avoid a *WeWork* scenario, boards should review the directors' email accounts and make sure that directors using email systems from employers or other entities can demonstrate that their emails are nonetheless confidential. If confidentiality cannot be guaranteed, directors may instead seek to use their personal email, particularly when communicating with counsel or about sensitive matters. But using a personal account can lead to other problems.

In *Schnatter v. Papa John's Int'l, Inc.*, for example, the Delaware Chancery Court permitted access to the personal emails of directors. In that case, the founder of Papa John's International, and also its largest stockholder and a director, made a demand under Section 220 of the Delaware General Corporation Law to inspect the corporation's books and records. The demand was in connection with litigation that followed the board's removal of him as chairman and the termination of several of his agreements with the company. He requested emails and text messages that had been sent from the other directors' personal accounts in order to investigate alleged mismanagement and potential breaches of their fiduciary duties. The *Schnatter* court ultimately required the directors to hand over their personal emails and text messages. The directors involved exposed all of their personal emails — not just those that referenced their board work — to review by a third party, as directors are typically required to turn over a broad set of communications to the company's lawyer (or team of lawyers), who then reviews for potentially relevant documents.

These recent cases stress the importance of pausing before sending a quick board-related email from an external employer or personal email account. Though the demand for quick responses and convenience makes that tempting, directors are better served by using the secure portals and the email system of the company for which they are serving as directors. Any inconvenience in doing so is far outweighed by the growing risks of personal exposure. In certain situations, such as communications with directors on a special committee, a separate but secure email account should be considered instead of a company email account so that these independent committee communications are not on company servers and so are not accessible by management or by directors not on the special committee.

The moral of the story is that directors willing to pause before firing off that email are better able to ensure that their privileged communications stay privileged, and their private conversations stay private. ■

To avoid a WeWork scenario, boards should review the directors' email accounts and make sure that directors using email systems from employers or other entities can demonstrate that their emails are nonetheless confidential.

Doug Raymond *is a partner in the law firm of Faegre Drinker Biddle & Reath LLP (www.faegredrinker.com). He can be reached at Douglas.Raymond@ feagredrinker.com.* ***Deanna Hayes,*** *an associate, assisted in preparation of this column.*