

Rethink How You Communicate with Outside Directors: Certain Communications May Not Be Protected

Authors: Noah Benjamin Kressler

March 09, 2021

A recent decision from the Delaware Court of Chancery is changing how companies communicate confidential information to outside directors. In *In re WeWork Litigation*, C.A. No. 2020-0258-AGB, a discovery dispute arose within litigation commenced by The We Company ("WeWork") against the SoftBank Group ("SBG") after SBG failed to close a tender offer with WeWork. Citing attorney-client privilege, SBG sought to withhold or redact certain email communications sent via the email systems of Sprint Inc. (Sprint), a third party not involved in the litigation, but that was majority-owned by SBG at the time. The emails at issue were sent by Sprint employees who, while also employed by and acting on SBG's behalf as directors, sought and received legal advice from SBG's lawyers concerning WeWork.

The dispute turned on whether or not the Sprint employees had a reasonable expectation of privacy when using their Sprint email accounts for SBG-related purposes such that the transmitted documents constituted protected confidential information. The court employed a four-factor test to answer these questions: (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's emails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

The court found that the first factor weighed against a reasonable expectation of privacy because the Sprint conduct code explicitly stated that employees should not have an expectation of privacy when sending or receiving emails, and that it had a right to review workplace emails at any time. The court determined that the second factor weighed against a reasonable expectation of privacy because SBG failed to provide evidence that Sprint did not monitor the employee's emails at issue and further because Sprint had previously reserved its right to monitor such emails in its conduct code. The third factor weighed against an expectation of privacy because SBG did not demonstrate that the relevant employees took any significant and meaningful steps to prevent Sprint from accessing their SBG-related emails sent from their Sprint email addresses. The court suggested that switching to a different webmail account or encrypting their messages would have constituted appropriate steps to prevent access. Lastly, the court concluded that the employees were aware or should have been aware of Sprint's policy, given their positions within Sprint, and should not have had a reasonable expectation of privacy.

In light of the decision, we are advising companies to scrutinize how they communicate with their board members. If board members are regularly receiving confidential communications at a (non-company) work email address, including where their employer has a right to monitor such emails, it could destroy attorney-client privilege under the four factors discussed above. The *WeWork* decision instructs that in transmitting attorney-client or other confidential communications, it would be prudent to provide company email addresses to outside board members, communicate through director portals, or otherwise encourage outside directors to utilize personal email accounts that are not subject to monitoring from employers or other third parties.

For more information, please contact [Noah Kressler](#), [Lacey Rochester](#), or any member of [Baker Donelson's Corporate Group](#).