IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

IN RE INFORMATION MANAGEMENT SERVICES, INC. DERIVATIVE LITIGATION	)))	Consol. C.A. No. 8168-VCL

OPINION

Date Submitted: August 22, 2013
Date Decided: September 5, 2013

Raymond J. DiCamillo, Scott W. Perkins, RICHARDS, LAYTON & FINGER, P.A., Wilmington, Delaware; J. Christian Word, Katherine A. Schettig, LATHAM & WATKINS LLP, Washington, District of Columbia; *Attorneys for Plaintiffs*.

Peter B. Ladig, Katherine J. Neikirk, MORRIS JAMES LLP, Wilmington, Delaware; J. Stephen McAuliffe, III, MILES & STOCKBRIDGE P.C., Rockville, Maryland; Scott Wilson, MILES & STOCKBRIDGE P.C., Baltimore, Maryland; *Attorneys for Defendants.*

Barry M. Klayman, COZEN O'CONNOR, Wilmington, Delaware; Donald N. Sperling, Jeffrey M. Schwaber, Jamie M. Hertz, STEIN SPERLING BENNETT DE JONG DRISCOLL PC, Rockville, Maryland; *Attorneys for Nominal Defendant, Information Management Services, Inc.*

LASTER, Vice Chancellor.

Trusts that own fifty percent of the common stock of nominal defendant Information Management Services, Inc. ("IMS" or the "Company") allege that two of the Company's three most senior officers mismanaged the Company in breach of their fiduciary duties. The executives consulted with their personal lawyers and advisors about the alleged mismanagement using their work email accounts. IMS gathered the emails but took no position on whether they should be produced. The executives invoked the attorney-client privilege. They did not rely on the work product doctrine. The trusts moved to compel, arguing that the attorney-client privilege does not apply because the Company reserved the right to monitor all email communications on IMS accounts, thereby eliminating any reasonable expectation of confidentiality. The motion is granted.

I. FACTUAL BACKGROUND

The facts for purposes of the motion to compel are drawn from the allegations in the pleadings and the exhibits and affidavits submitted in connection with the briefing on the motion. What follows are not formal factual findings, but rather how the court views the record for purposes of a discovery ruling. At this stage of the case, the court cannot resolve conflicting factual contentions.

A. Information Management Services, Inc.

IMS is a Delaware corporation with its principal place of business in Rockville, Maryland. The Company provides analytical software tools and other products used primarily to evaluate clinical trials for biomedical research.

The Burton family and the Lake family each beneficially own fifty percent of the Company's common stock. The Burton family owns its half through two trusts, the EB

Trust and the IMS Trust. Evelyn Burton is the sole trustee of the EB Trust; Michael Burton is the sole trustee of the IMS Trust. The Lake family owns the other half through the William H. Lake Grantor Trust. Brothers William Lake, Jr. and Andrew Lake are co-trustees of the Lake trust. Their mother, Jean Lake, is a beneficiary of the Lake trust. To differentiate among the individuals, this decision uses their first names.

The Company's board of directors (the "Board") has four members, two from the Burton family and two from the Lake family. The Burton family representatives are Evelyn and Michael. The Lake family representatives are Jean and Andrew.

Effective control over day-to-day management of the Company currently rests with the Lake family. It was not always so. Robert Burton and William Lake, Sr., founded the Company and managed the business together for many years. Robert, now deceased, was Evelyn's husband and Michael's father. William Sr., now retired, is Jean's husband and William and Andrew's father.

William Sr. retired in 2007. Robert passed away in 2010. At the time of Robert's death, William held the positions of President, Secretary, CFO, and Treasurer. Andrew held the position of Executive Vice President. Non-party Janis Beach, who joined the Company in 1974, held the position of COO. Since then, William, Andrew, and Janis have remained the most senior executives at the Company.

B. The Dispute

The Burton trusts allege that in the first quarter of 2011, William permitted IMS to overdraw its revolving line of credit by approximately $80,000, forcing IMS to obtain an emergency increase to meet payroll and other outstanding obligations. William allegedly

did not inform the Board concurrently of this event or the Company's financial position.

In October 2011, Michael joined IMS. Michael perceived problems from inside the Company including lack of growth, a general failure to market the Company's intellectual property, and poor employee morale.

In May 2012, the Burtons scheduled a meeting with William and Andrew to discuss their concerns. William and Andrew cancelled the meeting. In June, IMS informed Michael that his employment would be terminated.

The Burtons next retained Venture Advisors Financial and Strategic Services, LLC ("Venture Advisors") to review the Company's books and records. Venture Advisors also interviewed William, Andrew, and Nancy MacGillivary, a bookkeeper.

In a report issued on July 30, 2012, Venture Advisors criticized senior management on several grounds, including their failure to understand or comply with Generally Accepted Accounting Principles, Federal Acquisition Regulations, and the Fair Labor Standards Act (the "FLSA"). The report identified as issues an absence of professional accounting expertise, a lack of budgeting and financial planning, the use of unconventional compensation practices, and the failure to plan for the Company's "graduation" from Small Business Administration ("SBA") status.

During a special meeting of the Board on August 23, 2012, the directors discussed the Venture Advisors' report and the Burton family's concerns. The Burton representatives proposed to bring in professional managers to serve as the CEO and CFO. The Lake representatives declined, resulting in deadlock. The Board resolved to hire outside counsel to evaluate the Company's compliance with the FLSA. The Burtons

complain that William picked the law firm himself and instructed the firm not to communicate with the Burtons or the Board before presenting its final report.

During a meeting of the Board on September 14, 2012, the Board resolved to hire a consultant to evaluate the SBA issues. The Board deadlocked over the selection of the consultant and the scope of work. In October 2012, the Company retained Rubino & Company, Chartered, a financial services company with a special focus on government contracting, to review the Company's accounting practices and financial reporting.

On November 1, 2012, the Board met again. The Burton representatives proposed terminating William for cause, eliminating the Executive Vice President position held by Andrew, bringing in a CEO from outside the Company, and hiring Robert Dudley of Venture Advisors as CFO. The Lake representatives declined, resulting in deadlock. The Burtons then refused to approve any bonuses for senior management or staff. Over the ensuing weeks, the Burtons modified their position, rejecting only the bonuses for William and Andrew.

C. The Litigation

On December 31, 2012, the Burton trusts filed a complaint that charges William with breaching his fiduciary duties as an officer of IMS by mismanaging the Company and Jean and Andrew with breaching their fiduciary duties as directors of IMS by protecting William and enabling him to continue running the Company. In response, on January 28, 2013, the Lake trust filed a complaint of its own that charges Evelyn and Michael with breaching their fiduciary duties by denying bonuses to management, causing the Company to incur liability to reimburse the federal government for amounts

tied to the unpaid bonuses, and publicly disseminating confidential information about the Company. The complaint alleges that Evelyn and Michael have taken these actions in an effort to generate leverage to force a sale of their stock or the Company as a whole. The two actions were consolidated, generating this proceeding.

D. The Motion to Compel

During discovery, IMS advised the plaintiffs that William and Andrew used their work email accounts both before and after the filing of the lawsuit to communicate with their personal attorneys and advisors. The Company collected the emails, and William and Andrew asserted the attorney-client privilege. They did not invoke the work product doctrine. The defendants prepared a privilege log that identified 362 emails and attachments sent between August 2012 and March 2013. The Burton trusts then moved to compel IMS to produce the emails, arguing that the attorney-client privilege did not apply because William and Andrew communicated using work email accounts maintained on the IMS servers.

The IMS Policy Manual notifies employees that IMS has unrestricted access to communications sent using Company computers and that personal use of IMS computers should not be considered private. Section 9.1 of the IMS Policy Manual states: "You should assume files and Internet messages are open to access by IMS staff. After hours you may use IMS computers for personal use, but if you want the files kept private, please save them offline." Motion to Compel Ex. A at 6. Both William and Andrew filed affidavits stating that IMS has never actually engaged in email monitoring.

It is not seriously disputed that William and Andrew knew about the policy. There is also evidence that William understood that his work email account was accessible. In one email, William wrote "I'm switching over to my commercial email, just so I don't leave any more tracks about Mike in my IMS box." Motion to Compel Ex. G. In another email, he told a colleague that he was "sending . . . this via commercial email because it is stated to be confidential." Motion to Compel Ex. H.

II. LEGAL ANALYSIS

Delaware Rule of Evidence 502 establishes the scope of the attorney-client privilege under Delaware law. *See Zirn v. VLI Corp.*, 621 A.2d 773, 781 (Del. 1993) ("The [attorney-client] privilege was recognized at common law but received formal promulgation in Delaware through the adoption of the Delaware Rules of Evidence."). Rule 502(b) states:

> **General rule of privilege.** 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 to a 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.

D.R.E. 502(b). The motion to compel asserts that because William and Andrew used their IMS email accounts, their emails were not "confidential communications." The motion does not otherwise dispute that the requirements for the attorney-client privilege

are met. The opposition does not argue that Andrew should be treated differently because he is a director of the Company.

"The burden of proving that the privilege applies to a particular communication is on the party asserting the privilege." *Moyer v. Moyer*, 602 A.2d 68, 72 (Del. 1992). Rule 502(a)(2) states 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 or those reasonably necessary for the transmission of the communication." D.R.E. 502(a)(2). A party's subjective expectation of confidentiality must be objectively reasonable under the circumstances. *See Upjohn Co. v. United States*, 449 U.S. 383, 389, 395 (1981); Edward J. Imwinkelried, *The New Wigmore: A Treatise on Evidence: Evidentiary Privileges* § 6.8.1 (2013); 1 Paul R. Rice, *Attorney-Client Privilege in the United States* § 6 (2012).

Delaware courts have not addressed whether an employee has a reasonable expectation of privacy in a work email account.[1] In one of the early decisions to consider

[1] A work email account is an employer-provided email account furnished to each employee in which the address usually appears as some version of the individual employee's name followed by "@" followed by some variation on the employer's business name. The account uses the employer's technology infrastructure, typically an enterprise software system that operates on the employer's email server. *See* Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 Touro L. Rev. 647, 654 (2007). A work email account differs from a personal, password-protected, web-based email account, also known as webmail, which the employee may obtain through Google, Hotmail, or other services. *See id.* at 652; *see also* Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 Fordham J. Corp. & Fin. L. 115, 133-34 (2005) (distinguishing between work email and webmail). Courts have generally afforded greater privacy protection to webmail and have reached divergent conclusions when analyzing the attorney-client privilege if the

the issue, the Bankruptcy Court for the Southern District of New York started from the proposition that an employee can have a reasonable expectation of privacy in a work email account. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005). The Bankruptcy Court explained that under United States Supreme Court precedent, an employee can have reasonable expectation of privacy in areas such as the employee's office, desk, and files, but that the "employee's expectation of privacy . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* at 257 (quoting *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987)) (internal quotation marks omitted). "Although e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that lawyers and clients may communicate confidential information through unencrypted e-mail with a reasonable expectation of confidentiality." *Id.* (collecting authorities). In the ordinary course of business, employees who send communications within the

---

employee and personal attorney communicated using webmail. *Compare Long v. Marubeni Am. Corp.*, 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (finding employee could not assert privilege for webmail sent from employer-furnished computer that was set up to automatically store temporary internet files of employee activity, including email images) *with Curto v. Medical World Comm'ns, Inc.*, 2006 WL 1318387, at *8 (E.D.N.Y. May 15, 2006) (finding employee who worked from home had reasonable expectation of privacy in webmail sent using employer-furnished computer that was not connected to employer's network), *and Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 665 (N.J. 2010) (holding that even a company policy authorizing unlimited right to review webmail accessed over company system "would not be enforceable"). *See also Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (finding violations of federal and state law where former employer accessed webmail; distinguishing case from precedents involving work email). This case involves work email, not webmail.

company over the employer's email system can reasonably expect that outsiders will not be able to access the system. *Id.* Consequently, "[a]ssuming a communication is otherwise privileged, the use of the company's e-mail system does not, without more, destroy the privilege." *Id.* at 251.

An employer's policies and procedures regarding work email can alter the employee's reasonable expectation of privacy. Most employers choose to monitor work email accounts, or at least reserve the right to do so, for a host of legitimate business reasons.[2] "In light of the variety of work environments, whether the employee has a reasonable expectation of privacy must be decided on a case-by-case basis." *Asia Global*, 322 B.R. at 257 (citing *Ortega*, 480 U.S. at 718).

To guide the case-by-case analysis, the *Asia Global* court identified four factors:

> (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?

Id. No one factor is dispositive. *Id.* at 258-59. The question of privilege comes down to "whether the [employee's] intent to communicate in confidence was objectively reasonable." *Id.* at 258.

---

[2] *See, e.g.*, *TBG Ins. Servs. Corp. v. Superior Court*, 117 Cal. Rptr. 2d 155, 162 (Cal. Ct. App. 2002) (citing reasons for employer monitoring including legal compliance, legal liability, performance review, productivity measures, and security concerns); Hornung, *supra*, at 120-22 (same); Dion Messer, *To: Client@WorkPlace.com: Privilege at Risk?*, 23 J. Marshall J. Computer & Info. L. 75, 77-79 (2004) (same); Sherman, *supra*, at 657-660 (same).

Numerous courts have applied the *Asia Global* factors or closely similar variants when analyzing the attorney-client privilege.[3] Several of the *Asia Global* factors have been refined through subsequent application. In the current case, the *Asia Global* factors weigh in favor of production.

A. The Corporation's Policies On Work Email And Monitoring

As framed by the *Asia Global* court, the first factor is "does the corporation maintain a policy banning personal or other objectionable use?" 322 B.R. at 257. This factor has been refined to focus on the nature and specificity of the employer's policies regarding email use and monitoring. It 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

---

[3] *See, e.g.*, *Maxtena, Inc. v. Marks*, 2013 WL 1316386, at *5 (D. Md. Mar. 26, 2013); *In re High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *6 (N.D. Cal. Feb. 28, 2013); *United States v. Finazzo*, 2013 WL 619572, at *7 (E.D.N.Y. Feb. 19, 2013); *Goldstein v. Colborne Acquisition Co.*, 873 F. Supp. 2d 932, 937 (N.D. Ill. 2012); *Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1109 (W.D. Wash. 2011); *Hanson v. First Nat'l Bank*, 2011 WL 5201430, at *5 (S.D.W. Va. Oct. 31, 2011); *Kaufman v. SunGard Inv. Sys.*, 2006 WL 1307882, at *4 (D.N.J. May 10, 2006); *In re Royce Homes, LP*, 449 B.R. 709, 737-38 (Bankr. S.D. Tex. 2011), *appeal dismissed*, 466 B.R. 81 (S.D. Tex. 2012). Other courts have applied the *Asia Global* factors when analyzing the marital communications privilege, which also turns on a reasonable expectation of privacy. *See, e.g.*, *In re Reserve Fund Sec. & Deriv. Litig.*, 275 F.R.D. 154, 159-61 (S.D.N.Y. 2011); *In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on April 20, 2010 (Deep Horizon)*, 2011 WL 1193030, at *2 (E.D. La. Mar. 28, 2011); *Sprenger v. Rector & Bd. of Visitors of Va. Tech*, 2008 WL 2465236, at *3 (W.D. Va. June 17, 2008); *United States v. Etkin*, 2008 WL 482281, at *4 (S.D.N.Y. Feb. 20, 2008); *Geer v. Gilman Corp.*, 2007 WL 1423752, at *3 (D. Conn. Feb. 12, 2007).

reserves the right to monitor work email communications.[4] "[A]n outright ban on personal use would likely end the privilege inquiry at the start." *Finazzo*, 2013 WL

---

[4] *See, e.g., Aventa Learning*, 830 F. Supp. 2d at 1108 (finding no reasonable expectation of privacy where "the company reserved the right to access and disclose any file or stored communication[s] [on its systems] at any time"); *Deep Horizon*, 2011 WL 1193030, at *2 (finding that employee could not have reasonable expectation of privacy in work email where "BP's policy announced that [employee's] emails could be monitored and accessed by BP"); *Miller v. Blattner*, 676 F. Supp. 2d 485, 497 (E.D. La. 2009) (holding that when "an employer has a rule prohibiting personal computer use and a published policy that emails on [the employer's] computers were the property of [the employer], an employee cannot reasonably expect privacy in their prohibited communications"); *Pure Power*, 587 F. Supp. 2d at 559-60 ("Courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, where the employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored."); *Sims v. Lakeside School*, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007) ("[W]here an employer indicates that it can inspect laptops that it furnished for use of its employees, the employee does not have a reasonable expectation of privacy over the employer-furnished laptop."); *Long*, 2006 WL 2998671, at *3 (finding employee had no reasonable expectation of privacy when aware of employer's policy which provided that "(a) use of MAC's automated systems for personal purposes was prohibited; (b) MAC employees 'have no right of personal privacy in any matter stored in, created, or sent over the e-mail, voice mail, word processing, and/or internet systems provided' by MAC; and (c) MAC had the right to monitor all data flowing through its automated systems"); *Thygeson v. U.S. Bancorp*, 2004 WL 2066746, at *21 (D. Or. Sept. 15, 2004) ("[W]hen, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."); *Kelleher v. City of Reading*, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (finding employee had no reasonable expectation of privacy in workplace email where the employer's guidelines "explicitly informed employees that there was no such expectation of privacy"); *Garrity v. John Hancock Mut. Life Ins. Co.*, 2002 WL 974676, at *1-2 (D. Mass. May 7, 2002) (finding no reasonable expectation of privacy where company reserved the right to monitor employee use of work email); *Royce Homes*, 449 B.R. at 717, 741 (finding employee had no reasonable expectation of privacy when policy warned that "personal communications may be accessed, viewed, read or retrieved by a company Manager or employee"); *see also Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (Posner, J.) ("But Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so

619572, at *8; *accord Reserve Fund*, 275 F.R.D. at 163 (collecting cases). But a complete ban on personal use is not required.[5] This factor has been held to weigh against production if the employer does not have a clear policy or practice regarding personal use and monitoring.[6]

---

scotches his claim."); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [his employer] notified him that it would be overseeing his internet use."); *Banks v. Mario Indus. of Va., Inc.*, 650 S.E.2d. 687, 695-96 (Va. 2007) (holding that existence of policy advising employee that there was no right of privacy when using employer-furnished computer eliminated reasonable expectation of confidentiality and permitted employer to recover and use employee's letter to attorney that was drafted on employer-furnished computer, then sent through regular mail).

[5] *See Aventa Learning*, 830 F. Supp. 2d at 1109 (finding no reasonable expectation of privacy where company "discouraged" personal use and advised that its systems "should generally be used only for [company] business"); *Hanson*, 2011 WL 5201430, at *2, *6 (ordering production despite policy that permitted "[i]ncidental and occasional personal use"); *Reserve Fund*, 275 F.R.D. at 161 (finding policy sufficient which stated that "[e]mployees should limit their use of the e-mail resources to official business"); *Deep Horizon*, 2011 WL 1193030, at *2 (finding that employee could not have reasonable expectation of privacy in work email where "BP's policy announced that [employee's] emails could be monitored and accessed by BP"); *Royce Homes*, 449 B.R. at 717, 741 (finding no reasonable expectation of privacy even though policy permitted employees to "conduct limited, reasonable and appropriate personal communications on the company's electronic communication system with the understanding that personal communications may be accessed, viewed, read or retrieved by a company Manager or employee").

[6] *See Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (finding reasonable expectation of privacy when there was no clear policy or practice regarding email monitoring or use; "the anti-theft policy [merely] prohibited 'using' state equipment 'for personal business' without defining further these terms"); *Maxtena*, 2013 WL 1316386, at *5 (finding reasonable expectation of privacy where "[t]here is no evidence here indicating that the [employer] maintained any sort of monitoring or use policy"); *DeGeer v. Gillis*, 2010 WL 3732132, at *9 (N.D. Ill. Sept. 17, 2010) (declining to order production where there was no evidence of a company policy).

The policy manual that IMS provided to all employees contains a section entitled "Computer Privacy." It states: "You should assume files and Internet messages are open to access by IMS staff. After hours you may use IMS computers for personal use, but if you want the files kept private, please save them offline." This policy notified employees that although they could send personal emails using their work accounts, those emails would not be private and could be accessed by IMS. Although this policy is less detailed than some of the policies described in precedent decisions, it sufficiently put IMS employees on notice that their work emails were not private. The first *Asia Global* factor favors production.

B. The Degree To Which The Corporation Acts In Accordance With Its Policies

As framed by the *Asia Global* court, the second factor is "does the company monitor the use of the employee's computer or e-mail?" 322 B.R. at 257. This factor has been refined 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. Although some decisions have held that if an employer reserves the right to monitor work email, then whether it actually does so is irrelevant,[7] the employer's actual conduct with respect to monitoring remains an appropriate factor to consider, particularly if the employer has made specific representations or taken specific actions inconsistent with the

[7] *See, e.g.*, *Chechele v. Ward*, 2012 WL 4481439, at *1-2 (W.D. Okla. Sept. 28, 2012) (disregarding lack of actual monitoring); *Etkin*, 2008 WL 482281, at *4 ("Thus, it is irrelevant that the Government has not established that [the employer] *actually* read [the employee's] email."); *Royce Homes*, 449 B.R. at 739 ("[W]hether [the employer] actually reads an employee's e-mails is irrelevant.").

monitoring policy and the employee can show detrimental reliance.[8] If, however, the employer has clearly and explicitly reserved the right to monitor work email, then the absence of past monitoring or a practice of intermittent or as-needed monitoring comports with the policy and does not undermine it.[9] In that setting, "evidence of actual monitoring would make an expectation of privacy even less reasonable." *Finazzo*, 2013 WL 619572, at *9.

William and Andrew have submitted affidavits saying that IMS never in fact conducted email monitoring. Under its policy, IMS reserves the right to conduct email monitoring. The policy states expressly that employees "should assume files and Internet

---

[8] *See, e.g.*, *High-Tech Employee Antitrust Litig.*, 2013 WL 772668, at *7 ("a company's failure to actually monitor employees' emails or to have an explicit policy of monitoring the emails may suggest to employees that their emails in fact remain confidential"); *United States v. Nagle*, 2010 WL 3896200, at *4 (M.D. Pa. Sept. 30, 2010) (considering degree of actual monitoring); *Haynes v. Office of Attorney Gen.*, 298 F. Supp. 2d 1154, 1161-62 (D. Kan. 2003) (same). *But see, e.g.*, *Finazzo*, 2013 WL 619572, at *10 (declining to give less weight to policy because employee believed company did not monitor email usage as it had not disciplined CEO for violating rules about personal use of email); *Reserve Fund*, 275 F.R.D. at 161-62 (rejecting argument that employer's choice not to enforce policy in certain circumstances rendered policy inapplicable).

[9] *See Finazzo*, 2013 WL 619572, at *9 ("Most courts have concluded such reservation of the right to review destroys any reasonable expectation of privacy, whether or not the employer routinely reviews . . . the e-mails."); *Hanson*, 2011 WL 5201430, at *6 (ordering production where corporation reserved the right to access and monitor email communications, but where there was no evidence of actual monitoring); *Reserve Fund*, 275 F.R.D. at 163-64 (finding no expectation of privacy where employer reserved the right to monitor work emails, but also told employees it would not engage in routine monitoring and would attempt to protect the employee's privacy interests); *Long*, 2006 WL 2998671, at *3 (finding no expectation of privacy in work email where employer reserved the right to monitor); *Holmes v. Petrovich Dev. Co.*, 119 Cal. Rptr. 3d 878, 898 (Cal. Ct. App. 2011) (holding that lack of actual monitoring was "immaterial").

messages are open to access by IMS staff." The fact that IMS has not historically monitored emails does not conflict with its implicit reservation of the right to do so.

Building on the lack of historic monitoring, William and Andrew have contended that because they are the senior officers at IMS, they would decide whether or not IMS would monitor an employee's email. In their view, this gives them a unique expectation of privacy in the IMS system.

Legally, William and Andrew are wrong. "The business and affairs of every corporation organized under this chapter shall be managed by or under the direction of a board of directors . . . ." 8 *Del. C.* § 141(a). The board of directors, not senior management, has the final say on accessing any employee's email. Moreover, because of their statutory obligation to manage the business and affairs of the corporation and the concomitant fiduciary duties they owe to the corporation and its stockholders, individual directors have informational rights that are "essentially unfettered in nature." *Kalisman v. Friedman*, 2013 WL 1668205, at *3 (Del. Ch. Apr. 17, 2013); *accord Schoon v. Troy Corp.*, 2006 WL 1851481, at *1 n.8 (Del. Ch. June 27, 2006); *Intrieri v. Avatex Corp.*, 1998 WL 326608, at *1 (Del. Ch. June 12, 1998); *Belloise v. Health Mgmt., Inc.*, 1996 Del. Ch. LEXIS 127, at *36 (Del. Ch. June 11, 1996) (Allen, C.). If an individual director needed to access an employee's work email for a legitimate purpose, which the law presumes the director to have, then the director could do so. *See* 8 *Del. C.* § 220(d). William's and Andrew's expectations of privacy in their work email are no different from any other employee's.

Factually, William and Andrew did not have a different expectation of privacy. As shown by William's communications, he understood that his work email account was not secure. *See* Motion to Compel Ex. G ("I'm switching over to my commercial email, just so I don't leave any more tracks about Mike in my IMS box."); Motion to Compel Ex. H (writing to a colleague in another email, "I'm sending you this via commercial email because it is stated to be confidential.").

Particularly in light of William's emails recognizing that his work account was not confidential, the second *Asia Global* factor could be treated as favoring production. But because IMS never actually engaged in email monitoring, I treat the factor as neutral.

C. Ease Of Third Party Access

As framed by the *Asia Global* court, the third factor is "do third parties have a right of access to the computer or e-mails?" 322 B.R. at 257. In a work email case, this 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. *See Goldstein*, 873 F. Supp. 2d. at 937 (noting that in work email case, the third factor "is somewhat redundant of the first"); *Royce Homes*, 449 B.R. at 740 (noting that "third parties undeniably had access to [the employee's work] e-mails by virtue of their mere placement on [the employer's] server"). The third factor is most helpful when analyzing webmail or other electronic files that the employer has been able to intercept, recover, or otherwise obtain. This factor encompasses consideration of (i) steps the employee took to maintain the privacy of the files, such as password-protection, encryption, or deletion, and (ii) what the employer did to obtain the files, such as whether the employer used

forensic recovery techniques, deployed special monitoring software, or hacked the employee's accounts or files.[10]

This is a straightforward case involving work email. IMS, a third party to the communication, had the right to access William's and Andrew's emails when they communicated using their work accounts. Although William and Andrew took the precautionary step of putting the phrase "subject to the attorney client privilege" in the subject line, they failed to take more significant and meaningful steps to defeat access, such as shifting to a webmail account or encrypting their communications. The third *Asia Global* factor favors production.

D. The Employee's Knowledge Regarding The Company's Policies And Actions

As framed by the *Asia Global* court, the fourth factor is "did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?" 322 B.R. at 257. This factor has persisted relatively unchanged. If the employee lacked knowledge of the email policy and the party seeking production cannot show that the employee was notified of the policy, then this factor favors the existence of a reasonable

[10] *See Finazzo*, 2013 WL 619572, at *10 (explaining that third factor should take into account "what sort of precautions the employee took, or whether obstacles hindered the employer in accessing the privileged communications despite having a policy or practice otherwise allowing the employer to do so"); *Curto*, 2006 WL 1318387, at *1, *8 (noting that employer used forensic consultant to restore portions of emails that employee deleted nearly two years earlier); *Asia Global*, 322 B.R. at 257 n.7 (citing password-protection or encryption as potentially relevant considerations).

expectation of privacy.[11] If the employee had actual or constructive knowledge of the policy, then this factor favors production because any subjective expectation of privacy

[11] *See Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (finding employee had reasonable expectation of privacy in emails sent to attorney using employer-furnished account where employee stated he was unaware of monitoring); *Sprenger*, 2008 WL 2465236, at *4 (finding employee had reasonable expectation of privacy where there was no showing that the employee "[was] notified of the Policy by a log-on banner, flash screen, or employee handbook"); *Mason v. ILS Technologies, LLC*, 2008 WL 731557, at *4 (Feb. 29, 2008) (W.D.N.C. Feb. 29, 2008) (finding employee had reasonable expectation of privacy where it was "hotly disputed whether [employee] was even aware of the policy" and employer could not show that employee had been notified of policy); *Asia Global*, 322 B.R. at 259-61 (finding employee had reasonable expectation of privacy where it was not clear that employees knew of employer policy; company did not appear to have a formal policy regarding use of computers and email); *see also United States v. Slanina*, 283 F.3d 670, 676-77 (5th Cir. 2002) (holding employee had reasonable expectation of privacy where policy did not prevent storage of personal information or inform employees that computer usage would be monitored), *cert. granted, judgment vacated*, 537 U.S. 802 (2002) (vacating and remanding for further consideration in light of *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002)); *Nagle*, 2010 WL 3896200, at *4 (holding that employee had reasonable expectation of privacy in file stored on employer-furnished laptop where employee policy only referred to internet and email); *Haynes*, 298 F. Supp. 2d 1154, 1161-62 (holding that employee had reasonable expectation of privacy (i) where employer had policy stating there would be no reasonable expectation of privacy but employees were given passwords and advised that unauthorized access to other users' email was prohibited and (ii) where employer had never engaged in monitoring).

that the employee may have had is likely unreasonable.[12] Decisions have readily imputed knowledge of an employer's policy to officers and senior employees.[13]

William and Andrew were two of the three most senior officers at IMS, and they do not deny knowing about the Company's policies. As discussed, William's communications demonstrate that he understood his work email was not secure. The fourth *Asia Global* factor favors production.

E. The Potential For A Statutory Override

Three of the four *Asia Global* factors point towards production and one is neutral. The *Asia Global* calculus therefore calls for granting the motion to compel, absent a statutory override that could alter the common law result. *Cf. Protecting the Confidentiality of Unencrypted E-mail*, ABA Formal Op. 99-413 (relying on protections afforded by the Electronic Communications Protection Act of 1986 (the "ECPA") when

---

[12] *See, e.g.*, *Long*, 2006 WL 2998671, at *3 (finding employees had knowledge of work email policy when one employee had helped prepare the employee handbook containing the policy, another was a senior vice president and general manager, and where the employer sent annual reminders about its policy); *Royce Homes*, 449 B.R. at 741 (finding that presence of policy memorialized in employee handbook provided sufficient notice).

[13] *See, e.g.*, *Goldstein*, 873 F. Supp. 2d at 937 ("That Defendants did not allege they were unaware of the policy is not surprising. They owned the company and were its officers. They likely cannot make that assertion with a straight face."); *Aventa Learning*, 830 F. Supp. 2d at 1107 (holding that senior level manager had constructive knowledge of company's policies because his job was to enforce them when supervising employees); *Long*, 2006 WL 2998671, at *3 (imputing knowledge of policy to senior vice president and general manager); *Royce Homes*, 449 B.R. at 741 (imputing knowledge to "key employee of the [company] . . . [who] surely knew what the [company's] Electronic Communications Policy stated").

opining that attorneys could communicate ethically with their clients using unencrypted email). Delaware, for example, requires that before an employer conducting business in the First State can monitor work email lawfully, the employer must (i) provide notice to employees daily that it engages work email monitoring or (ii) obtain written consent from the monitored employees. 19 *Del. C.* § 705(b). Although the court need not reach the issue, it is possible that if a Delaware employer did not follow either statutory path, then a Delaware employee might have a reasonable expectation of privacy in light of the additional protection provided by the Delaware Code.[14]

The Delaware statute applies only to businesses operating in Delaware, not to Delaware entities who operate elsewhere but choose Delaware as their corporate home. *See Klig v. Deloitte LLP*, 36 A.3d 785, 797-98 (Del. Ch. 2011). In this case, IMS conducts its business in Maryland. IMS is only a Delaware citizen by virtue of having selected Delaware as its state of incorporation and maintaining a registered agent here. The federal government and the State of Maryland are the sovereigns whose law IMS must follow when dealing with its employees' email.

1. The Federal Wiretap Act

Title I of the ECPA amended the Federal Wiretap Act of 1968 by adding the term "electronic communications" to its prohibitions, thereby making it a crime for a person to

[14] Delaware also has adopted state legislation modeled on the Federal Wiretap Act and the Federal Stored Communications Act. *See* 11 *Del. C.* §§ 2401-2412 (Delaware Wiretap Act); 11 *Del. C.* §§ 2421-2427 (Delaware Stored Communications Act). For the reasons discussed below, the Federal Wiretap Act and the Federal Stored Communications Act do not support a reasonable expectation of privacy in work email.

"intentionally intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). Emails are electronic communications for purposes of the Federal Wire Tap Act. *See Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461-62 (5th Cir. 1994); *Healix Infusion Therapy, Inc. v. Helix Health, LLC*, 747 F. Supp. 2d 730, 743 (S.D. Tex. 2010).

The Federal Wiretap Act provides that if a communication was intercepted in violation of the statute, then "no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court . . . of the United States [or] a State." 18 U.S.C. § 2515. On the issue of privilege, Section 2517(4) of the Federal Wiretap Act states that "[n]o *otherwise privileged* wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." *Id.* § 2517(4) (emphasis added).

There are at least four reasons why the Federal Wiretap Act does not affect the privilege analysis for work email. First, the Federal Wiretap Act only applies when a party intercepts a communication. *Conte v. Newsday, Inc.*, 703 F. Supp. 2d 126, 139 (E.D.N.Y. 2010); *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, 2007 WL 4394447, at *4 (E.D. Pa. Dec. 13, 2007). To do so, a party must acquire the communication during transmission. *See, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113-14 (3d Cir. 2003) (collecting cases). Emails that have arrived at their destination, such as the corporate email server, are not within the scope of the Federal Wiretap Act. *Id.* An

employer does not violate the Federal Wiretap Act by accessing stored work emails on its server, as IMS did here.

Second, an intercept requires the use of an "electronic, mechanical or other device." 18 U.S.C. § 2511(1)(b). The Federal Wiretap Act excludes from the definition of "device" the equipment or facility "being used by a provider of wire or electronic communication service in the ordinary course of its business." *Id.* § 2510(5)(a)(ii); *accord Healix Infusion*, 747 F. Supp. 2d at 744 (holding that intercepting requires use of some device other than the email system used to convey the message; "the drive or server on which an e-mail is received does not constitute a device for purposes of the Wiretap Act") (citation omitted); *Conte*, 703 F. Supp. 2d at 140-41 (same); *Crowley v. Cybersource Corp*, 166 F. Supp. 2d 1263, 1268-69 (N.D. Cal. 2001) (same). Because IMS obtained the emails through the ordinary operation of its email system, it did not use a device to intercept them.

Third, a private employer can intercept electronic communications lawfully "where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Consent can be express or implied. *Williams v. Poulos*, 11 F.3d 271, 281 (1st Cir. 1993). The presence of an email monitoring policy in an employee handbook or policy manual is sufficient to support a finding of implied consent to the monitoring of a work email account. *See Shefts v. Petrakis*, 758 F. Supp. 2d 620, 630-31 (C.D. Ill. 2010) (holding company president gave implied consent to corporate monitoring of his email and texts sent using company-furnished device); *Thygeson*, 2004 WL 2066746, at *20 (relying on

"explicit policies set out in [defendant's] Employee Handbook"). The IMS policy on email use was sufficiently specific to establish William and Andrew's implied consent to email monitoring.

Fourth, it is not unlawful for the provider of an email account and the related technical infrastructure to "intercept, disclose, or use" a communication as part of "any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service." 18 U.S.C. § 2511(2)(a)(i). IMS provided William and Andrew with their work email accounts and the underlying technical infrastructure, and IMS therefore had the right to access their email communications as "a necessary incident to" providing the email service and for "the protection of the rights or property" of IMS. Employers monitor email (or reserve the right to do so) in large part to protect their property and to guard against potential liability. *See supra* note 2. IMS could monitor email legitimately for those purposes.

In light of these exceptions, the protections afforded by the Federal Wiretap Act do not give William and Andrew a reasonable expectation of privacy in their work email. The Federal Wiretap Act does not alter the common law privilege analysis.

2. The Federal Stored Communications Act

Title II of the ECPA enacted the Federal Stored Communications Act, which makes it a crime for a person to "intentionally access[] without authorization a facility through which an electronic communication service is provided" or to "intentionally exceed[] an authorization to access that facility" "and thereby obtain[] . . . access to a wire or electronic communication while it is in electronic storage in such system." 18

U.S.C. § 2701(a). By its terms, the Federal Stored Communications Act applies to work email stored on a corporate server. *See Fraser*, 352 F.3d at 115; *Pure Power*, 587 F. Supp. 2d at 555.

The Federal Stored Communications Act's prohibition against access does not apply to conduct authorized "by the person or entity providing a wire or electronic communications service." 18 U.S.C. § 2701(c)(1). This exception has been held to permit an employer to search email stored on a system that the employer administered. *See, e.g.*, *Fraser*, 352 F.3d at 115. IMS administered its email system and qualifies for this exception. The Federal Stored Communications Act does not change the common law privilege analysis either.

3. The Maryland Wiretap Act

Maryland has enacted a state version of the Federal Wiretap Act. Md. Code, Cts. & Jud. Proc. §§ 10-401 to 10-414 (the "Maryland Wiretap Act"). Although the Maryland act differs in one significant way from the federal act (Maryland is a dual consent state), the Maryland version ultimately does not alter the common law privilege analysis.

The Maryland Wiretap Act generally parallels the Federal Wiretap Act. Like the federal statute, the Maryland statute makes it unlawful for any person to "[w]illfully intercept, endeavor to intercept, or procure any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." Md. Code, Cts. & Jud. Proc. § 10-402(a). Like the federal act, the Maryland Wiretap Act provides that if a communication was intercepted in violation of the statute, then "no part of the contents of the communication and no evidence derived therefrom may be received in evidence in

any trial, hearing, or other proceeding." *Id.* § 10-405(a). It further provides that "[a]n otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this subtitle, does not lose its privileged character." *Id.* § 10-407(d).

Unlike the federal statute, it is only lawful under Maryland law "for a person to intercept a[n] . . . electronic communication where the person is a party to the communication *and where all of the parties to the communication have given prior consent to the interception*." *Id.* § 10-402(c)(3) (emphasis added). By requiring consent from all parties to the communication, the Maryland Wiretap Act "has imposed stricter requirements for civilian monitoring than has federal law." *Adams v. State*, 406 A.2d 637, 642 (Md. Ct. Spec. App. 1979). The parties' submissions do not suggest that William's or Andrew's personal attorneys and advisors ever consented to IMS obtaining their communications. The dual consent requirement of the Maryland Wiretap Act therefore renders the consent exception inapplicable.

Despite the unavailability of the consent exception, it remained lawful for IMS to possess William's and Andrew's work emails. The Maryland statute, like the federal act, turns on the existence of an "intercept" made with a "device," and the one Maryland decision to address those terms interpreted them narrowly, consistent with federal law. *See Adams*, 406 A.2d at 642. The *Adams* decision indicates that under the Maryland Wiretap Act, an employer accessing work emails stored on its system would be neither using a "device" nor "intercepting" the communications for the same reasons that those concepts would not apply under the Federal Wiretap Act. The Maryland act also contains

an ordinary-course-of-business exception comparable to the Federal Wiretap Act. *See* Md. Code, Cts. & Jud. Proc. § 10-402(c)(1)(i). The Maryland Wiretap Act therefore does not change the outcome of the motion.[15]

4. Maryland Stored Communications Act

Maryland also has enacted a state version of the Federal Stored Communications Act. Md. Code, Cts. & Jud. Proc. §§ 10-4A-01 to 10-4A-08 (the "Maryland Stored Communications Act"). The Maryland act generally parallels the federal act. Like the federal statute, the Maryland statute makes it unlawful for any person to "[i]ntentionally access[] without authorization a facility through which an electronic communication service is provided" or to "[i]ntentionally exceed[] an authorization to access a facility" and thereby "obtain . . . access to a wire or electronic communication while it is in electronic storage" in that system. Md. Code, Cts. & Jud. Proc. § 10-4A-02(a). Like the federal act, the Maryland act applies to work emails stored on a corporate server. *See Upshur v. State*, 56 A.3d 620, 625 (Md. Ct. Spec. App. 2012), *cert. denied*, 62 A.3d 732 (Md. 2013) (observing that the Maryland Stored Communications Act "mirrors its federal counterpart").

---

[15] The Maryland Wiretap Act's prohibition on the use of intercepted communications literally applies only to proceedings in the Maryland courts. *See* Md. Code, Cts. & Jud. Proc. § 10-405(a) (referring to a court "of this State"). Because the existence of other exceptions means that IMS did not violate the Maryland Wiretap Act by obtaining William's and Andrew's email, I need not consider the forum limitation. If IMS had violated the Maryland Wiretap Act, then a strong argument could be made that even a non-Maryland court should respect the Maryland legislature's public policy determination regarding the scope of permissible email monitoring within that state.

The exceptions to the Maryland Stored Communications Act similarly parallel the federal act. They include an exception for conduct authorized "[b]y the person or entity providing a wire or electronic communications service." Md. Code, Cts. & Jud. Proc. § 10-4A-02(c)(1). While no Maryland case has interpreted this exception explicitly, it likely permits an employer to search email stored on a system that the employer administered. *See Upshur*, 56 A.3d at 625 (noting that Maryland act "mirrors its federal counterpart"). IMS administered its email system and would qualify for this exception. Like its federal counterpart, the Maryland Stored Communications Act does not change the privilege analysis for work email.

F. A Cautionary Note

"It is the nature of the judicial process that [the court] decide[s] only the case before [it.]" *Paramount Commc'ns Inc. v. QVC Network Inc.*, 637 A.2d 34, 51 (Del. 1994). This decision has applied the *Asia Global* factors to hold that William and Andrew cannot invoke the attorney-client privilege for communications exchanged with their personal attorneys and advisors using their work email accounts. Although the case has been postured as a consolidated derivative action, it actually involves a dispute between two families, each possessing 50% of the stock and enjoying equal representation on the Board. It is far from clear whether a court would analyze privilege similarly in a more traditional derivative action involving a stockholder plaintiff with a relatively nominal stake and a board comprising individuals without any affiliation with the suing stockholder.

As the *Asia Global* case recognized, the premise that an employer's access to an

employee's work email compromises the attorney-client privilege makes the most sense in litigation between the employer or its successor-in-interest and the employee. *See* 322 B.R. at 256 ("The Insiders used the debtor's e-mail system . . . and the communications apparently concerned actual or potential disputes with the debtor, the owner of the e-mail system."). Those outside the corporation cannot routinely access work email accounts, and laws like the Federal Wiretap Act and the Federal Stored Communications Act have teeth when they try. The 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. Admittedly, courts have applied the *Asia Global* factors and found no reasonable expectation of privacy in suits by outsiders, *see, e.g.*, *Deepwater Horizon*, 2011 WL 1193030 (suits by property owners injured by oil spill), and courts routinely find no reasonable expectation of privacy in actions brought by prosecutors and regulators. It is not clear to me, however, that the analysis translates so easily when the party trying to overcome the privilege is not the corporation or its successor-in-interest.

As previously discussed, the plaintiffs in this case are trusts affiliated with directors who possess essentially unfettered informational rights. A stockholder with a small stake and no director affiliation would not have similar default rights of access and would be limited to relying on Section 220(a) of the General Corporation Law. *See* 8 *Del. C.* § 220(a). The IMS Board also is split evenly between directors affiliated with the two families, making it virtually inevitable that either family would have stockholder standing to assert the corporation's claims derivatively against defendants affiliated with

the other family. *See Benerofe v. Cha*, 1998 WL 83081, at *3-4 (Del. Ch. Feb. 20, 1998) (demand futile where board is split). In a more typical derivative action not involving a split board, a stockholder plaintiff does not have power to sue in the corporation's name unless and until the corporation chooses not to oppose the stockholder's suit (explicitly or implicitly) or the court determines that the stockholder can sue by denying a motion to dismiss brought pursuant to Rule 23.1.[16] Only then does the stockholder actually gain the power to sue on behalf of the entity. Before that point, Delaware law regards the interests of the corporation as aligned with those of individual defendants. *Scattered Corp. v. Chi. Stock Exch., Inc.*, 1997 WL 187316, at *6-8 (Del. Ch. Apr. 7, 1997), *aff'd on other*

[16] *See, e.g., Rales v. Blasband*, 634 A.2d 927, 932 (Del. 1993) ("Because directors are empowered to manage, or direct the management of, the business and affairs of the corporation, the right of a stockholder to prosecute a derivative suit is limited to situations where the stockholder has demanded that the directors pursue the corporate claim *and* they have wrongfully refused to do so *or* where demand is excused because the directors are incapable of making an impartial decision regarding such litigation.") (emphases added; citation omitted); *Kaplan v. Peat, Marwick, Mitchell & Co.*, 540 A.2d 726, 730 (Del. 1988) ("[P]re-suit demand under Chancery Court Rule 23.1, is an objective burden which must be met in order for the shareholder to have capacity to sue on behalf of the corporation. *The right to bring a derivative action does not come into existence until the plaintiff shareholder has made a demand on the corporation to institute such an action or until the shareholder has demonstrated that demand would be futile.*") (emphasis added); *Zapata Corp. v. Maldonado*, 430 A.2d 779, 784 (Del. 1981) ("[W]here demand is properly excused, the stockholder does possess the ability to initiate the action on his corporation's behalf."). Even then, the corporation can reassert control over the derivative claims through a special litigation committee. *Zapata*, 430 A.2d at 785 (explaining that, "if the board determines that a suit would be detrimental to the company," the board "has the power to choose not to pursue litigation . . . so long as the decision is not wrongful").

grounds, 701 A.2d 70 (Del. 1997).[17] These distinctions make it unclear whether a more typical derivative action plaintiff should be able to obtain otherwise privileged communications sent using a work email account during periods pre-dating the point when the stockholder gains standing to sue.

Moreover, equity historically has imposed other limitations on a stockholder plaintiff's ability to obtain corporate documents in a derivative action, even after the stockholder gains standing to sue on behalf of the corporation. For example, a stockholder seeking to penetrate the corporation's privilege had to show good cause under *Garner v. Wolfinbarger*, 430 F.2d 1093 (5th Cir. 1970), *cert. denied*, 401 U.S. 974 (1971). A stockholder plaintiff does not automatically acquire the unfettered ability to access anything sent or received over the work email system.

Finally, it is possible that the concept of selective waiver (as distinct from partial

---

[17] The Delaware Supreme Court affirmed the Court of Chancery's Rule 23.1 dismissal under an abuse of discretion standard. *Scattered Corp.*, 701 A.2d 70, 73 (Del. 1997), *overruled on other grounds by Brehm v. Eisner*, 746 A.2d 244 (Del. 2000). In *Brehm*, the Delaware Supreme Court overruled seven precedents, including *Scattered*, to the extent those precedents reviewed a Rule 23.1 decision by the Court of Chancery under an abuse of discretion standard or otherwise suggested deferential appellate review. *See Brehm*, 746 A.2d at 253 n.13, 254 (overruling in part on this issue *Scattered*, 1997 WL 187316; *Grimes v. Donald*, 673 A.2d 1207 (Del. 1996); *Heineman v. Datapoint Corp.*, 611 A.2d 950 (Del. 1992); *Levine v. Smith*, 591 A.2d 194 (Del. 1991); *Grobow v. Perot*, 539 A.2d 180 (Del. 1988); *Pogostin v. Rice*, 480 A.2d 619 (Del. 1984); *and Aronson v. Lewis*, 473 A.2d 805 (Del. 1984)). The *Brehm* Court held that going forward appellate review of a Rule 23.1 determination would be *de novo* and plenary. *Brehm*, 746 A.2d at 253-54. Neither the Delaware Supreme Court's ruling on appeal in *Scattered* nor its subsequent modification of the standard of review in *Brehm* altered the Court of Chancery's holding that no conflict of interest existed between the corporation and the individual director defendants at the motion to dismiss stage in a derivative action such that a law firm could represent all defendants without impropriety.

waiver) might apply in an appropriate case. *Cf. Saito v. McKesson HBOC, Inc.*, 2002 WL 31657622, at *6-7, *11 (Del. Ch. Nov. 13, 2002) (holding that selective waiver when documents were provided to the SEC under a confidentiality agreement did not result in global waiver of the work product doctrine; "[c]onfidential disclosure of work product during law enforcement agency investigations relinquishes the work product privilege only as to that agency, not as to the client's other adversaries," thereby "encourag[ing] cooperation with law enforcement agencies without any negative cost to society or to private plaintiffs"). It is also likely, as in *Saito*, that the defendants in a more traditional derivative action would invoke the work product doctrine, which was not argued here.

None of these issues has been presented, and this opinion does not provide any opportunity to hazard a guess about the potential outcome of a case in which they were raised. I mention them only to emphasize that this decision does not purport to announce a rule applicable to all derivative actions, and it should not be interpreted as doing so.

III. CONCLUSION

The motion to compel is granted. Within three days, the defendants shall produce the emails and attachments otherwise protected by the attorney-client privilege that William and Andrew exchanged with their personal attorneys and advisors using their work email accounts.