# STATE OF MICHIGAN

# COURT OF APPEALS

CANDICE R. STAVALE,

Plaintiff-Appellee,

v

DAVID A. STAVALE,

Defendant-Appellant,

FOR PUBLICATION
June 11, 2020
9:15 a.m.

No. 349472
Kent Circuit Court
LC No. 18-010676-DM

Before: K.F. KELLY, P.J., and FORT HOOD and SWARTZLE, JJ.

FORT HOOD, J.

In this interlocutory appeal by leave granted,[1] defendant appeals the trial court's order denying defendant's motion to quash subpoenas on the basis of the requested information being protected by the attorney-client privilege. Defendant contends on appeal that the trial court erred when it concluded that defendant intentionally and voluntarily disclosed privileged information by communicating with his attorney through his employer-provided e-mail address such that he could not avail himself of the attorney-client privilege. We conclude that the trial court erred in its application of the law, and as matter of first impression, articulate in this opinion a framework with which the trial court should reconsider this issue on remand.

This is an action for divorce. The particular issue raised on appeal arose when plaintiff issued subpoenas to defendant's employer requesting e-mails that defendant had sent to his personal attorney through his employer-provided e-mail address. Defendant filed a motion to quash the subpoenas on the basis of the attorney-client privilege, and plaintiff responded that the privilege did not apply because, according to the employer's employee handbook, defendant had no reasonable expectation of privacy when he used the employer-provided e-mail address to communicate with his personal attorney. Although it is not entirely clear from the record whether

[1] *Stavale v Stavale*, unpublished order of the Court of Appeals, entered July 24, 2019 (Docket No. 349472).

the trial court was addressing the appropriate legal question, the court ultimately sided with plaintiff. This appeal followed.

As noted, it is not clear from the record whether the trial court denied the motion to quash on the basis of the attorney-client privilege having never attached to the communications at issue, or on the basis of defendant having waived any use of the privilege after it attached. What is clear is that defendant's argument before the trial court and on appeal is that he did not waive the attorney-client privilege because he did not intentionally and voluntarily disclose his privileged e-mails to his employer. However, the Michigan cases defendant relies upon to explain his application of waiver involve whether disclosure of *already*-privileged information to a third party constituted a waiver of the attorney-client privilege. See *Leibel v General Motors Corp*, 250 Mich App 229, 242; 646 NW2d 179 (2002) (analyzing whether a waiver occurred where otherwise-privileged information became public due to litigation in another court); *Sterling v Keidan*, 162 Mich App 88, 90; 412 NW2d 255 (1987) (examining whether the defendant waived attorney-client privilege when he inadvertently sent an otherwise-privileged document to the plaintiff).

Whether a communication is made in a confidential manner such that the attorney-client privilege can attach is not the same issue as whether an already-privileged communication has been voluntarily disclosed to a third party such that attorney-client privilege is waived. See *Leibel*, 250 Mich App at 238-242 (separately analyzing application of the attorney-client privilege and waiver of the privilege). The distinction is important because, although related, the standard for waiving a privilege that already exists is not the same under Michigan law as the standard for applying the privilege in the first place. See *id*. at 236, 240 (noting that attorney-client privilege attaches only to confidential communications between a client and an attorney, and separately noting the circumstances under which a waiver of the privilege may occur after it has attached). The issue in this case is not one of waiver, or at least not the type of waiver analyzed in *Leibel* and *Sterling*. The issue in this case, fundamentally, is whether defendant had a reasonable expectation of privacy in the use of his employer-provided e-mail such that attorney-client privilege attached to the communication between defendant and his counsel in the first place.

"Whether the attorney-client privilege applies to a communication is a question of law that we review de novo." *Nash Estate v Grand Haven*, 321 Mich App 587, 592; 909 NW2d 862 (2017) (quotation marks and citation omitted). In Michigan, "[t]he attorney-client privilege attaches to communications made by a client to an attorney acting as a legal adviser and made for the purpose of obtaining legal advice." *Id*. at 593 (quotation marks and citation omitted). "The scope of the privilege is narrow: it attaches only to confidential communications by the client to its advisor that are made for the purpose of obtaining legal advice." *Id*. (quotation marks and citation omitted). See also *People v Compeau*, 244 Mich App 595, 597; 625 NW2d 120 (2001) (explaining that attorney-client privilege does not apply unless there is an "element of confidentiality"). The attorney-client privilege is "designed to permit a client to confide in his attorney, knowing that his communications are safe from disclosure." *Nash Estate*, 321 Mich App at 593.

In *Compeau*, there was no element of confidentiality when the defendant spoke to his counsel in the courtroom and a bailiff overheard because the defendant failed to take reasonable precautions to keep the communication confidential, i.e., by quietly whispering or by communicating in writing. *Compeau*, 244 Mich App at 597-598. Recently, in *People v Miller (On Reconsideration)*, unpublished per curiam opinion of the Court of Appeals, issued February 5,

2019 (Docket No. 337460), p 4,[2] we concluded that statements made by a defendant over a jail phone line that the defendant knew to be monitored and recorded were not confidential for the purposes of asserting attorney-client privilege. In both cases, we held that attorney-client privilege did not apply despite the fact that the respective defendants did not necessarily *intend* to disclose their communications to a third party. See *Compeau*, 244 Mich App at 597; *Miller*, unpub op at 4.

With respect to the specific facts of this case, however, no Michigan court has addressed how attorney-client privilege applies in cases in which a party uses an employer-provided means of communication to communicate with a personal attorney, the employer reserves the right to monitor that communication, but either the party is not aware of that monitoring or the employer cannot or does not actually monitor as suggested in its policy. The issue has been addressed, however, by several federal and state courts.[3]

The seminal case in the federal system is *In re Asia Global Crossing, Ltd*, 322 BR 247 (Bankr SD NY, 2005). At issue in that case was "whether an employee's use of [a] company e-mail system to communicate with his personal attorney destroy[ed]" attorney-client privilege. *Id.* at 251. After reviewing Fourth Amendment cases and right-of-privacy cases, the court concluded that four factors should be considered in determining an employee's expectation of privacy in the employer's computer files and e-mail:

> (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.* at 257.]

---

[2] We note that we are not bound by *Miller* pursuant to MCR 7.215(C)(1).

[3] We may look to authority from other jurisdictions for instruction. *Voutsaras Estate v Bender*, 326 Mich App 667, 676; 929 NW2d 809 (2019) ("Although not binding, authority from other jurisdictions may be considered for its persuasive value."). This is particularly true when issues involving attorney-client privilege have been addressed by federal courts:

> "The attorney-client privilege is the oldest of the privileges for confidential communications known to the common law." *Upjohn v United States*, 449 US 383, 389; 101 S Ct 677; 66 L Ed 2d 584 (1981). This Court looks to federal precedent for guidance in determining the scope of the attorney-client privilege when a particular issue has been addressed by a federal court. See, e.g., *Leibel*, 250 Mich App at 236-237; *Reed Diary Farm v Consumers Power Co*, 227 Mich App 614, 619-620; 576 NW2d 709 (1998). [*Nash Estate*, 321 Mich App at 593-594.]

Ultimately, the *Asia Global* court concluded that the company in that case clearly had access to the employee's e-mails contained on the company server, and clearly had a policy banning personal use of the employee e-mail system and providing to employees that communications sent through the corporate e-mail server were "not private or secure." *Id*. at 259. However, the court noted that it was unclear whether employees had ever been notified of the policy or of the monitoring of their e-mails, and thus, the court could not conclude "as a matter of law" that employees lacked a reasonable expectation of privacy when they used their corporate e-mails to communicate with their personal attorney. *Id*. at 261.[4]

*Asia Global* has been "widely adopted" in the federal system as a tool to aid in "the 'reasonable expectation of privacy' determination in the context of e[-]mail transmitted over and maintained on a company server." *In re Reserve Fund Securities & Derivative Litigation*, 275 FRD 154, 159-160 n 2 (SD NY, 2011).[5] Another notable and instructive case comes from a California appellate court.

---

[4] As an aside, we note that *Asia Global* and much of its progeny occasionally use the term "waiver" more tangentially than defendant would seek to in this case. Again, defendant uses the term in order to apply Michigan caselaw that says that defendant needed to take some sort of voluntary and intentional action resulting in the disclosure of already-privileged information to a third party in order to be estopped from asserting attorney-client privilege. While related, the test articulated in *Asia Global* is fundamentally about the initial expected confidentiality of a communication or action. See *Asia Global*, 322 BR at 255-258. The *Asia Global* court might say that a party "waived" privilege by communicating with their attorney in a nonconfidential manner, which is comparable to saying that the party lacked a reasonable expectation of privacy such that attorney-client privilege never attached at all. See *id*. at 260-261. This is not the same as the idea that defendant would put forth: that under Michigan law, when the communication is initially made, if the party did not intend for a third party to overhear, the communication will always necessarily be protected by attorney-client privilege unless waived at a later date. As noted above, that idea is not in keeping with our caselaw. See *Compeau*, 244 Mich App at 597-598 (attorney-client privilege did not attach because the defendant failed to take reasonable precautions to keep his communication confidential, even though he undoubtedly did not intend for his statements to be overheard); *Miller*, unpub op at 4 (attorney-client privilege did not attach because the defendant had reason to know his communications could be monitored, even though he did not intend for the communications to be overheard).

[5] The parties spent a considerable amount of time below discussing *Aventa Learning, Inc v K12, Inc*, 830 F Supp 2d 1083, 1107 (WD Wash, 2011), wherein the United States District Court for the Western District of Washington held that attorney-client privilege did not extend to documents that had been stored on company computers. Defendant contends, somewhat ironically, that *Aventa* is factually distinguishable because it involves whether an action taken subsequent to a communication actually having been made—saving the communication on a company computer—constituted a waiver of privilege. See *id*. at 1106-1108. For plaintiff's purposes, the value of the case is essentially that it is another federal case adopting *Asia Global*'s test for determining the existence of a reasonable expectation of confidentiality when utilizing company-provided

In *Holmes v Petrovich Dev Co, LLC*, 191 Cal App 4th 1047; 119 Cal Rptr 3d 878 (2011), a California appellate court held that attorney-client communications made over the plaintiff's company computer were not privileged.[6] In reaching its conclusion, the court noted that the plaintiff

> used a computer of defendant company to send the e-mails even though (1) she had been told of the company's policy that its computers were to be used only for company business and that employees were prohibited from using them to send or receive personal e-mail, (2) she had been warned that the company would monitor its computers for compliance with this company policy and thus might "inspect all files and messages . . . at any time," and (3) she had been explicitly advised that employees using company computers to create or maintain personal information or messages "have no right of privacy with respect to that information or message." [*Id*. at 1051.]

Notably, it was relevant in *Holmes* that the defendant seeking to prevent the plaintiff from relying on attorney-client privilege was also the employer, and thus "the electronic means used [to communicate] belong[ed] to the defendant" itself. *Id*. at 1068. With that context, the court noted:

> [T]he e-mails sent via company computer under the circumstances of this case were akin to [the plaintiff] consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by him. [*Id*.]

---

computer equipment. Other than being one of many federal examples of the application of the test that came out of *Asia Global*, we do not see the particular import of *Aventa* over any of the other federal cases applying the test.

[6] California Evidentiary Code § 952 defines "confidential communication between client and lawyer" as

> information transmitted between a client and his or her lawyer in the course of that relationship and in confidence by means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted, and includes a legal opinion formed and the advice given by the lawyer in the course of that relationship.

Defendant contends that the existence of the above code means that *Holmes* cannot be instructive in Michigan because Michigan has no corollary rule. Defendant suggests that the above rule constitutes a narrower explanation of "confidential communication" than provided for by Michigan law, but we note that nothing about the above rule is necessarily inconsistent with Michigan law such that *Holmes* cannot be, at the very least, instructive.

In any event, apart from the employer also being the defendant in the case, the *Holmes* court analyzed nearly identical factors as in *Asia Global*—without reference to the same—for determining the reasonable expectation that the communication at issue would be confidential.

One potential distinction from *Holmes*, however, is that the court seemed to place more emphasis than *Asia Global* on the language of the employer's policy concerning monitoring as opposed to whether the employer actually, regularly enacted that policy. In *Holmes*, the plaintiff argued—as defendant does in this case—that she had a reasonable expectation of privacy in her company e-mail account because she utilized a private password to access her e-mail. *Id*. at 1069. That court concluded, however, that the plaintiff's "belief was unreasonable because she was warned that the company would monitor e-mail to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer." *Id*.

The plaintiff in *Holmes* also argued—similar to the defendant in this case—that although her employer's policy noted that she had no right of privacy in her company e-mail and that the company could "periodically inspect all e-mail to ensure compliance with its policy against personal use of company computers," the plaintiff nonetheless had a reasonable expectation of privacy "because the 'operational reality' was that there was no [actual] access or auditing of employee's computers." *Id*. at 1069-1070. The *Holmes* court noted, however, that there was, in fact, a company controller who had access to all e-mails sent and received by company computers, and "at no time during her testimony did [the plaintiff] claim she knew for a fact that, contrary to its stated policy, the company never actually monitored computer e-mail." *Id*. at 1070. Most importantly, however, the plaintiff could not overcome the fact that "the company explicitly told employees that they did not have a right to privacy in personal e-mail sent by company computers, . . . and the company never conveyed a conflicting policy." *Id*. at 1071. "Absent a company communication to employees explicitly contradicting the company's warning to them that company computers are monitored to make sure employees are not using them to send personal e-mail, it is immaterial that the 'operational reality' is the company does not actually do so." *Id*.

With those cases in mind, including our own caselaw examining circumstances in which an element of confidentiality exists for the purposes of attorney-client privilege, we believe that both *Asia Global* and *Holmes* strike an important balance between an individual's right to privacy, an employer's right to limit that privacy in the workplace under certain circumstances, and the indelible value of the attorney-client privilege to our legal system. We are inclined to follow their lead, with the exception that we prefer the *Holmes* court's emphasis on the employer's policy and the employee's understanding of that policy over whether the employer tended to actually carry out the policy. In determining whether an employee has a reasonable expectation of privacy in an employer-provided e-mail or computer system, it is relevant to consider (1) whether the employer maintains a policy with respect to the use of those systems and what that policy entails, and (2) whether the employee was ever notified or made aware of the employer's policies and practices with respect to computer privacy and monitoring. Obviously, these issues should be decided on a case-by-case basis, and the two-factors above are not exhaustive. For example, whether a company actually monitors employee computers and the employee's knowledge of the same may be relevant

in some cases,[7] but we note that it ordinarily should not overpower considerations of the employer's stated policy and the employee's knowledge of that policy.

In applying the above factors to the case at hand, it is clear that defendant's employer maintained an unambiguous policy regarding defendant's use of his employer-provided e-mail. The employee handbook specifically provided:

> The Company's electronic communication and information systems including, but not limited to, computers, related hardware, software and networks as well as internet systems, telephone, voice mail and email systems are Company property provided to employees and are intended for business use. Any personal use must not interfere with performance or operations and must not violate any Company policy or applicable law. ***Users have no legitimate and/or reasonable expectation of privacy regarding system usage.*** As a result, you should not use the Company's electronic communication systems to discuss or correspond about anything personal, particularly sensitive, confidential, or privileged personal communications to outside parties, as the Company reserves the right to monitor all system usage, including such communications.
>
> The Company may access its electronic communications and information systems and obtain the communications with the systems, including past voice mail and e-mail messages, without notice to users of the system, in the ordinary course of business when the Company deems it appropriate to do so. The Company also has the right to and may inspect or monitor without notice any devise employees use to access electronic communications and information systems, including but not limited to computers, laptops, notebooks, tablet computers, or mobile devices. Further, the Company may review Internet usage. The reasons for which the Company may obtain such access include, but are not limited to: maintaining the system, preventing or investigating allegations of system abuse or misuse, assuring compliance with software copyright laws, complying with legal and regulatory requests for information, protecting proprietary information, and ensuring that operations continue appropriately during an employee's absence.

The policy in this case could not be clearer, and to the extent that defendant was made aware of the same, it is sufficient to extinguish any reasonable expectation of privacy defendant might have had.

When an employee is knowingly subject to the type of policy at issue in this case—a policy that unequivocally states and emphasizes that employees "***have no legitimate and/or reasonable***

[7] Indeed, in this case, defendant filed an e-mail correspondence between defendant's counsel and a representative of defendant's employer, wherein defendant's employer noted that the "Company ha[d] never accessed [defendant's] work e-mail, and it also has never had a need or desire to do so." Defendant's employer further noted that complying with the subpoena would "require [defendant's] password," which the employer did not have.

***expectation of privacy regarding***" usage of their employer-provided e-mail addresses—and unless there is reason to believe that the employee was specifically told to disregard the same or some other extenuating circumstance, employees cannot have a reasonable expectation of privacy in order to assert attorney-client privilege. Use of an employer-provided e-mail to communicate with a personal attorney with knowledge of the above policy is not indicative of having taken reasonable precautions to preserve the confidentiality of the communication. See *Campeau*, 244 Mich App at 597 (attorney-client privilege does not apply when the party seeking to assert the privilege does not take reasonable precautions to preserve the confidentiality of the communications).

What is unclear in this case, however, is the extent to which defendant was notified or otherwise made aware of the policy. There appears to have been no inquiry into that issue. And, a footnote contained in defendant's brief on appeal, at the very least, suggests the possibility that defendant may never have been asked to read or sign the employee manual that puts forth the relevant policy. See *Mintz v Mark Bartelstein & Assoc, Inc*, 885 F Supp 2d 987 (CD Cal, 2012) (distinguishing *Holmes* by indicating that the plaintiff at issue in *Mintz* may "never [have] read the [employment] manual" at issue and had "no recollection of having signed an acknowledgement" of the same). With that in mind, we reverse the trial court's order denying defendant's motion to quash and remand for the trial court to reconsider the issue utilizing the correct legal framework to determine whether defendant had a reasonable expectation of privacy in the use of his employer-provided e-mail.

We note that defendant relies on *Stengart v Loving Care Agency, Inc*, 408 NJ Super 54; 973 A2d 390 (App Div, 2009), *Haynes v Attorney General*, 298 F Supp 2d 1154 (D Kan, 2003), and *United States v Slanina*, 283 F3d 670 (CA 5, 2002), vacated on other grounds 537 US 802; 123 S Ct 69; 153 L Ed 2d 3 (2002), for the contention that he necessarily did have a reasonable expectation of privacy in his employer-provided e-mail. All of the cases are distinguishable and far less instructive than *Asia Global* and *Holmes*.

First, *Slanina* had to do with the defendant's right to privacy in his own computer equipment as well as computer equipment provided by his employer that had "no connection to the [employer's] intra-office network." *Slanina*, 283 F3d at 672. The United States Court of Appeals for the Fifth Circuit concluded that the defendant had a reasonable expectation of privacy in the equipment because it was located in the defendant's locked office and because he had installed passwords to limit access. *Id*. at 676-677. In reaching its conclusion, however, the court explicitly noted "the absence of a policy placing [the defendant] on notice that his computer usage would be monitored." *Id*. at 677. Accordingly, the case is of little import.

Next, in *Haynes*, the plaintiff brought a civil action against the Kansas Attorney General for viewing private information contained on the plaintiff's work computer while he was an employee in the Attorney General's office. *Haynes*, 298 F Supp 2d at 1157. In that case, the plaintiff was specifically told by his employer that "his computer had two files: private and public." *Id*. "He was further told that he could put personal information in the private file and that no one would have access to it." *Id*. With that in mind, even in light of the fact that the plaintiff was shown a screen when he logged onto his computer that informed the plaintiff that he did not have an "expectation of privacy in using th[e] system," the United States District Court in Kansas held that the plaintiff had a reasonable expectation of privacy. First, there is no evidence in this case that defendant was given any such conflicting information. Second, and most importantly, by

focusing on the policy enacted by the Attorney General and the plaintiff's reasonable confusion with respect to that policy, *Haynes* actually supports the framework we are adopting: in determining whether an employee has a reasonable expectation of privacy on an employer's computer system or on an employer-provided e-mail address, courts should look to the privacy policy enacted by the employer as well as the extent to which the employee was notified or made aware of the policy.

Lastly, in *Stengart*, a New Jersey appellate court concluded that e-mails sent from an employee to her attorney through her personal "Yahoo email account," but using an employer-issued laptop, were privileged. *Stengart*, 408 NJ Super at 74. Defendant fails to reconcile the use of a personal, web-based e-mail in *Stengart* with the use of a company provided e-mail address in this case. Moreover, just as in *Haynes*, the reasoning of the New Jersey appellate court is heavily focused on the ambiguity of the company policy at issue. *Id*. at 63-64. The court noted that it was not clear from the policy whether the company reserved the right to intercept communications made from the plaintiff's private, web-based e-mail address, even when using the company-issued laptop. *Id*. at 63-64. The court noted that "although the matter [was] not free from doubt, there [was] much about the language of the policy that would convey to an objective reader that personal emails, such as those in question, do not become company property when sent on a company computer, and little to suggest that an employee would not retain an expectation of privacy in such emails." *Id*. at 65. Forgetting the factual difference between *Stengart* and this case—which is significant—even in *Stengart*, the principal issue with regard to whether the plaintiff had a reasonable expectation of privacy was the company policy at issue and the plaintiff's understanding of that policy. See *id*. at 60-66.

As noted above, the import of the policy at issue in this case is abundantly clear. The policy unambiguously provided that defendant had no expectation of privacy when using his employer-provided e-mail, and that the employer reserved the right to monitor the e-mail without notification to defendant. Thus, the only question is defendant's understanding of that policy at the time the relevant communications were made. Accordingly, on remand, the trial court should give particular focus to whether and to what extent defendant was notified or otherwise made aware of the policy. Again, it should be clear that the issue in this case is whether defendant had a reasonable expectation of privacy in his communication to his attorney. The issue is not whether defendant's communication constituted a voluntary and intentional disclosure of the information to a third party after the fact.[8]

[8] Defendant briefly asserts, as an alternative issue at the end of his reply brief on appeal, that even to the extent the e-mails at issue are not protected by attorney-client privilege, they are work-product that should be excluded on that ground. When this Court granted defendant's application for leave to appeal, we limited the issues to those raised in his application and supporting brief. *Stavale v Stavale*, unpublished order of the Court of Appeals, entered July 24, 2019 (Docket No. 349472). Defendant did not raise this issue in his application, nor did he raise the issue in his supporting brief. He raised the issue in a reply brief. Moreover, even assuming defendant had raised the issue in his application, he failed to adequately raise it below such that there is no record concerning how the e-mails at issue might have implicated the work-product doctrine in order for

Reversed and remanded for proceedings consistent with this opinion. We do not retain jurisdiction.

/s/ Karen M. Fort Hood
/s/ Kirsten Frank Kelly
/s/ Brock A. Swartzle

this Court to even begin to review the issue. Suffice it to say that we decline to address defendant's reliance on the work-product doctrine.