UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

THOMAS BINGHAM,

Plaintiff,

v. Case No: 8:14-cv-73-T-23JSS

BAYCARE HEALTH SYSTEM,

Defendant.
_____/

ORDER ON MOTION FOR DETERMINATION OF PRIVILEGE

THIS MATTER is before the Court on Defendant's Motion for a Determination That Certain E-Mail Communications Are Not Privileged or Otherwise Protected from Discovery ("Motion"). (Dkt. 94.) Defendant seeks a determination that certain e-mails exchanged between Plaintiff and his attorneys and thereafter forwarded by Plaintiff to his work e-mail account are not protected from discovery by the attorney-client privilege. The Court held a hearing on this matter on June 30, 2016. For the reasons that follow, Defendant's Motion is granted.

BACKGROUND

On January 29, 2016, Defendant served a subpoena on Plaintiff's employer, Holladay Properties Services Midwest, Inc. ("Holladay"), seeking documents related to the allegations in this lawsuit. In response, Holladay produced the responsive documents, which included e-mails and attachments between Plaintiff and his attorneys that Plaintiff forwarded from his personal e-mail account to his work e-mail account at Holladay. (Dkt. 96 at 2.) Upon receiving Holladay's production, Defendant notified Plaintiff of its receipt of the e-mails, and Plaintiff asserted a claim of privilege as to the e-mails. (Dkt. 94.) Defendant now seeks a determination that the e-mails

from Plaintiff's work e-mail account are not confidential and thus not privileged or otherwise protected from discovery.

APPLICABLE STANDARDS

When the court's jurisdiction is premised on a federal question in a civil case, federal law of privilege applies. *Hancock v. Hobbs*, 967 F.2d 462, 467 (11th Cir. 1992); *see* Fed. R. Evid. 501 (providing that federal common law governs a claim of privilege unless the United States Constitution, federal statute, or rules prescribed by the Supreme Court provide otherwise). This lawsuit was brought in federal court based on federal question jurisdiction as an action under the False Claims Act, 31 U.S.C. §§ 3729–3733. (Dkt. 32.) Therefore, federal common law applies in analyzing the attorney-client privilege. The attorney-client privilege protects the disclosures that a client makes to his attorney, in confidence, for the purpose of securing legal advice or assistance. *Cox v. Adm'r U.S. Steel & Carnegie*, 17 F.3d 1386, 1414 (11th Cir. 1994).

To determine if a particular communication is confidential and protected by the attorney-client privilege, the privilege holder must prove that the communication was intended to remain confidential and, under the circumstances, was reasonably expected and understood to be confidential. *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003); *see also United States v. Schaltenbrand*, 930 F.2d 1554, 1562 (11th Cir. 1991) ("The party invoking the attorney-client privilege has the burden of proving that an attorney-client relationship existed and that the particular communications were confidential."). Thus, the relevant inquiry is not whether the individual expected his or her communications to remain confidential but rather whether that expectation was reasonable. *United States v. Bell*, 776 F.2d 965, 971 (11th Cir. 1985).

ANALYSIS

In this case, the e-mails at issue represent communications between Plaintiff and his attorneys that were exchanged on Plaintiff's personal e-mail account.[1] The e-mails contained a link to a cloud storage account where Plaintiff's attorneys had uploaded documents for Plaintiff's review. Plaintiff then forwarded certain e-mails from his personal e-mail account to his work e-mail account so that he could access the links from work. (Dkt. 94 at 2; Dkt. 96 at 2.) The forwarded e-mails contain discussions between Plaintiff and his attorneys, as well as links to documents. (Dkt. 96 at 2.)

Based on the written submissions of the parties and the arguments advanced at the hearing, the parties agree that the e-mails consist of communications between Plaintiff and his attorneys regarding this lawsuit. The parties dispute only whether the e-mails in question are protected by the attorney-client privilege when they were accessed by Plaintiff on his work e-mail account on Holladay's "communications system," which is described in Holladay's policy as "including e-mail and voice mail systems and Intranet/Internet connections." (Dkt. 94-1.) As such, the Court must determine the confidential nature of the e-mails transmitted over Holladay's communications systems.

A. Application of Attorney-Client Privilege to Workplace E-Mails

Courts addressing this issue have focused primarily on whether the employer maintains a policy regarding the use of its computer or e-mail systems. Specifically, courts consider the specificity of the policy and the extent to which the policy diminishes an employee's reasonable expectation of privacy in communications transmitted over the employer's systems. However, because the overarching consideration in determining whether a communication is privileged is

[1] At the hearing, Plaintiff stated that there were only a few e-mails produced by Holladay over which the instant dispute arises.

whether the individual had an objectively reasonable expectation that his or her communications were confidential, privilege determinations of this nature are extremely fact-specific and often depend on the particular policy language, if any, adopted by the employer.

Notably, courts have adopted a four-factor test to determine whether a reasonable expectation of privacy exists in the context of e-mail transmitted over and maintained on a company server. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005); *see In re Reserve Fund Sec. & Derivative Litig.*, 275 F.R.D. 154, 159–60 (S.D.N.Y. 2011) (listing cases adopting the four-factor test); *Leor Expl. & Prod. LLC v. Aguiar*, No. 09-60136-CIV, 2009 WL 3097207, at *4 (S.D. Fla. Sept. 23, 2009) (applying the four-factor test). In determining this issue, courts have considered the following four factors: (1) whether the corporation maintains a policy banning personal or other objectionable use; (2) whether the company monitors the use of the employee's computer or e-mail; (3) whether third parties have a right of access to the computer or e-mails; and (4) whether the corporation notifies the employee, or whether the employee was aware, of the use and monitoring policies. *See Asia Global*, 322 B.R. at 257. The four-factor test provides persuasive guidance in evaluating whether an individual's expectation of confidentiality is reasonable in light of the existence of other factors that tend to cast doubt on the reasonableness of that expectation, namely the scope of an employer's policy. *See id*. at 258 ("[T]he question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable.").

The determination of whether a communication is confidential is somewhat similar to the search-and-seizure determination under the Fourth Amendment. *See id.* at 256 (comparing the Fourth Amendment analysis to the attorney-client privilege analysis); *see also* cases cited *infra* note 2. Under the Fourth Amendment analysis, the court considers whether an individual's

expectation of privacy is objectively reasonable. *See O'Connor v. Ortega*, 480 U.S. 709, 715 (1987) (providing that an individual's Fourth Amendment rights are implicated only if the conduct at issue infringes an expectation of privacy "that society is prepared to accept as reasonable"). Similarly, under the attorney-client privilege analysis, the court must consider whether a communication was reasonably expected and understood to be confidential. *Bell*, 776 F.2d at 971. As such, courts addressing the issue of attorney-client privilege refer to Fourth Amendment cases addressing an individual's reasonable expectation of privacy in the context of electronic communications, as the analysis under both standards requires consideration of whether one's expectation of privacy was objectively reasonable.[2] Courts also seek guidance from cases addressing invasion of privacy claims in the context of the workplace, as those cases also consider an individual's reasonable expectation of privacy.[3]

---

[2] For a discussion of an employee's reasonable expectation of privacy in the workplace under the Fourth Amendment, see *O'Connor*, 480 U.S. at 714; *United States v. Ziegler*, 456 F.3d 1138, 1146 (9th Cir. 2006); *Biby v. Bd. of Regents, of Univ. of Neb. at Lincoln*, 419 F.3d 845, 850 (8th Cir. 2005); *United States v. Angevine*, 281 F.3d 1130, 1135 (10th Cir. 2002); *United States v. Slanina*, 283 F.3d 670, 676 (5th Cir. 2002); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002); *Leventhal v. Knapek*, 266 F.3d 64, 73 (2d Cir. 2001); *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000); *United States v. DiTomasso*, 56 F. Supp. 3d 584, 591 (S.D.N.Y. 2014); *United States v. Yudong Zhu*, 23 F. Supp. 3d 234, 238 (S.D.N.Y. 2014); *United States v. Linder*, No. 12 CR 22-1, 2012 WL 3264924, at *8 (N.D. Ill. Aug. 9, 2012); *United States v. Busby*, No. CR 11-00188 SBA, 2011 WL 6303367, at *4 (N.D. Cal. Dec. 16, 2011); *Keck v. Virginia*, No. 3:10-CV-555, 2011 WL 4589997, at *12 (E.D. Va. Sept. 9, 2011); *United States v. Elmquist*, No. 07-00245-01-CR-W-ODS, 2008 WL 3895971, at *10 (W.D. Mo. Aug. 18, 2008) (following the reasoning of *United States v. Thorn*, 375 F.3d 679 (8th Cir. 2004)); *United States v. Mosby*, No. CRIM. A. 3:08-CR-127, 2008 WL 2961316, at *5 (E.D. Va. July 25, 2008); *United States v. Hassoun*, No. 04 60001 CR BROWN, 2007 WL 141151, at *1 (S.D. Fla. Jan. 17, 2007); *Haynes v. Attorney Gen. of Kan.*, No. 03-4209-RDR, 2005 WL 2704956, at *4 (D. Kan. Aug. 26, 2005); *United States v. Scrushy*, No. CR-03-BE-0530-S, 2005 WL 4149004, at *5 (N.D. Ala. Jan. 21, 2005); *United States v. Bailey*, 272 F. Supp. 2d 822, 835 (D. Neb. 2003); *United States v. Sims*, No. CR 00-193 MV, 2001 WL 36498440, at *7 (D. N.M. Apr. 19, 2001); *Wasson v. Sonoma Cty. Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 905 (N.D. Cal. 1997); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1234 (D. Nev. 1996). In this context, the majority of courts have found that employees do not have a reasonable expectation of privacy in their work computers or in e-mails exchanged using a work account, especially when the employer retains a policy or otherwise notifies employees that their equipment or accounts are subject to monitoring.

[3] For a discussion of an employee's reasonable expectation of privacy in materials transmitted over an employer's computer system under a claim for invasion of privacy, see *Metzler v. XPO Logistics, Inc.*, No. 4:13-CV-278, 2014 WL 4792984, at *6 (E.D. Tex. Sept. 25, 2014); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 761 (N.D. Ohio 2013); *Mintz v. Mark Bartelstein & Assocs., Inc.*, 885 F. Supp. 2d 987, 997 (C.D. Cal. 2012); *Gauntlett v. Ill. Union Ins. Co.*, No. 5:CV 11-00455-EJD, 2011 WL 5191808, at *9 (N.D. Cal. Nov. 1, 2011); *Yarborough v. King*, No. CA 2:11-2602-MBS-BHH, 2011 WL 5238920, at *5 n.5 (D. S.C. Oct. 3, 2011); *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 633 (C.D. Ill. 2010); *Miller v. Blattner*, 676 F. Supp. 2d 485, 497 (E.D. La. 2009); *Sporer v. UAL Corp.*, No. C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009); *Thygeson v. U.S. Bancorp*, No. CV-03-467-ST, 2004 WL

In applying the four factors discussed above, courts diverge on the issue of whether there must be evidence of actual monitoring or whether a policy reserving the right to monitor employee communications is sufficient to meet the second factor. For example, some courts weigh the act of enforcement more heavily than the existence of a limiting policy. As such, these courts have required some evidence that the employer in fact monitored the employee's communications. *E.g.*, *Flatworld Interactives v. Apple Inc.*, No. C1201956JSWEDL, 2013 WL 11319071, at *1 (N.D. Cal. Dec. 24, 2013); *In re High-Tech Employee Antitrust Litig.*, No. 11-CV-2509-LHK-PSG, 2013 WL 772668, at *7 (N.D. Cal. Feb. 28, 2013); *United States v. Hatfield*, No. 06-CR-0550 (JS), 2009 WL 3806300, at *9 (E.D.N.Y. Nov. 13, 2009); *Brown-Criscuolo v. Wolfe*, 601 F. Supp. 2d 441, 450 (D. Conn. 2009).

Other courts, however, have been satisfied with the finding that the employer's policy provided a right to access and monitor the employee's use, regardless of whether the policy was consistently enforced. These courts have found it sufficient that the employer's policy reserved the right—or permitted the employer—to monitor the employee's communications, without requiring evidence or a showing of actual monitoring. *E.g.*, *L-3 Commc'ns Corp. v. Jaxon Eng'g & Maint., Inc.*, No. 10-CV-02868-MSK-KMT, 2014 WL 183303, at *6 (D. Colo. Jan. 12, 2014); *United States v. Finazzo*, No. 10-CR-457 RRM RML, 2013 WL 619572, at *9 (E.D.N.Y. Feb. 19, 2013); *Chechele v. Ward*, No. CIV-10-1286-M, 2012 WL 4481439, at *2 (W.D. Okla. Sept. 28, 2012); *Dombrowski v. Governor Mifflin Sch. Dist.*, No. CIV.A. 11-1278, 2012 WL 2501017, at *6 (E.D. Pa. June 29, 2012); *Aventa Learning, Inc. v. K12, Inc.*, 830 F. Supp. 2d 1083, 1109 (W.D.

2066746, at *18 (D. Or. Sept. 15, 2004); *Kelleher v. City of Reading*, No. CIV.A.01-3386, 2002 WL 1067442, at *7 (E.D. Pa. May 29, 2002); *Garrity v. John Hancock Mut. Life Ins. Co.*, No. CIV.A. 00-12143-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002); *Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 100 (E.D. Pa. 1996). The majority of these cases have concluded that an employee has no reasonable expectation of privacy in computer files, e-mails, or electronic data maintained at his or her workplace.

Wash. 2011); *Hanson v. First Nat'l Bank*, No. 5:10–0906, 2011 WL 5201430, at *6 (S.D. W. Va. Oct. 31, 2011); *In re Reserve Fund*, 275 F.R.D. at 164; *In re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, on Apr. 20, 2010*, No. MDL 2179, 2011 WL 1193030, at *3 (E.D. La. Mar. 28, 2011); *Alamar Ranch, LLC v. Cty. of Boise*, No. CV-09-004-S-BLW, 2009 WL 3669741, at *4 (D. Idaho Nov. 2, 2009); *Leor Expl.*, 2009 WL 3097207, at *4; *Smith v. United Salt Corp.*, No. 1:08CV00053, 2009 WL 2929343, at *9 (W.D. Va. Sept. 9, 2009); *United States v. Etkin*, No. 07-CR-913(KMK), 2008 WL 482281, at *4 (S.D.N.Y. Feb. 20, 2008); *Sims v. Lakeside Sch.*, No. C06-1412RSM, 2007 WL 2745367, at *1 (W.D. Wash. Sept. 20, 2007); *Long v. Marubeni Am. Corp.*, No. 05CIV.639 (GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006); *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236 (JLL), 2006 WL 1307882, at *4 (D. N.J. May 10, 2006); *see also United States v. Hamilton*, 778 F. Supp. 2d 651, 655 (E.D. Va. 2011) (focusing on an employer's policy reserving the right to inspect and monitor employee accounts).

Upon review of the applicable caselaw, it appears that the majority of courts have found that an employee has no reasonable expectation of privacy in workplace e-mails when the employer's policy limits personal use or otherwise restricts employees' use of its system and notifies employees of its policy.[4] *See Pure Power*, 587 F. Supp. 2d at 559–60 ("Courts have

[4] The specific facts of this case establish that Holladay maintained a formal policy that limited personal use. As such, in considering the applicable caselaw, cases in which the employer did not maintain a policy regarding electronic communications or did not otherwise ban or limit personal use are distinguishable from the present case. *E.g.*, *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 897, 904 (9th Cir. 2008); *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007); *United States v. Hudson*, No. CRIM.A. 13-20063-01, 2013 WL 4768084, at *9 (D. Kan. Sept. 5, 2013); *Maxtena, Inc. v. Marks*, No. CIV.A. DKC 11-0945, 2013 WL 1316386, at *5 (D. Md. Mar. 26, 2013); *United States v. Nagle*, No. 1:09-CR-384, 2010 WL 3896200, at *4 (M.D. Pa. Sept. 30, 2010); *Convertino v. U.S. Dep't of Justice*, 674 F. Supp. 2d 97, 110 (D. D.C. 2009); *Sprenger v. Rector & Bd. of Visitors of Virginia Tech*, No. CIV.A. 7:07CV502, 2008 WL 2465236, at *4 (W.D. Va. June 17, 2008); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1203 (S.D. Cal. 2008); *see also Orbit One Commc'ns, Inc. v. Numerex Corp.*, 255 F.R.D. 98, 108 n.11 (S.D.N.Y. 2008) (noting the limited right of disclosure in company policy); *Mason v. ILS Techs., LLC*, No. CIVA304CV-139RJC-DCK, 2008 WL 731557, at *4 (W.D.N.C. Feb. 29, 2008) (declining to find waiver of privilege when no evidence established that the employee was aware of the employer's policy and no one alleged that he agreed to abide by it). Similarly, because this case involves the use of a work computer and e-mails sent and retrieved on a work e-mail account, cases addressing an employee's use of a personal computer or use of personal or web-based e-mail accounts are distinguishable. *E.g.*, *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007) (commercial Internet

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."). Further, the majority of courts have relied on the existence of a workplace policy reserving the right to access and monitor employee communications rather than a showing that employee accounts were routinely monitored. Upon consideration, the Court is persuaded by these authorities and agrees under the circumstances presented in this case, that a policy reserving the right to access and monitor employee accounts is sufficient to support a finding that an employee has no reasonable expectation of confidentiality in e-mails transmitted over an employer's e-mail system.

B. Holladay's Policy on Electronic Access

Under Holladay's Personnel Handbook, employees have access to the company's communications systems, including the e-mail system, to conduct "legitimate company business." (Dkt. 94-1.) Holladay's policy also allows "de minimus (very limited) personal use," but it provides that Holladay's communications systems may not be used for the operation of personal business or for personal gain. (Dkt. 94-2.) The policy further provides that the "communications systems, including all correspondence, is company property." (Dkt. 94-1.) Specifically, the policy states that "all communications composed, sent, received, or stored on Holladay's communications system are, and remain, the property of Holladay" and "are not the private property of any

---

service provider); *Hoofnagle v. Smyth-Wythe Airport Comm'n*, No. 1:15CV00008, 2016 WL 3014702, at *8 (W.D. Va. May 24, 2016) (personal e-mail account and no policy limiting personal use); *Billups v. Penn State Milton S. Hershey Med. Ctr.*, No. 1-11-CV-01784, 2015 WL 7871029, at *3 n.2 (M.D. Pa. Dec. 3, 2015) (no ban on personal use and limited right to access); *Wellin v. Wellin*, No. 2:13-CV-1831-DCN, 2015 WL 5785709, at *26 (D. S.C. July 31, 2015) (personal e-mail account); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (personal e-mail from a third party e-mail provider); *Sims*, 2007 WL 2745367, at *2 (web-based e-mail); *Geer v. Gilman Corp.*, No. 306 CV 889 JBA, 2007 WL 1423752, at *3 (D. Conn. Feb. 12, 2007) (employee's use of e-mail and computer of her fiancé); *Curto v. Med. World Commc'ns, Inc.*, No. 03CV6327 DRH MLO, 2006 WL 1318387, at *5 (E.D.N.Y. May 15, 2006) (home office); *Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp. 2d 914, 927 (W.D. Wis. 2002) (web-based e-mail account).

employee, even if the employee has used his or her own personal computer, tablet, cell phone or other personal device." (Dkt. 94-2.)

In regard to the monitoring of electronic communications, Holladay's policy provides that Holladay "reserves and intends to exercise the right to monitor, review, audit, intercept, access and disclose all electronic and telephone communications created, received or sent over the company's communication system for any purpose." (Dkt. 94-1.) The policy explicitly warns that it "creates no expectation of privacy concerning such messages" and that the "confidentiality of any message should not be assumed," regardless of password protection. (Dkt. 94-1, 94-2.) Indeed, the policy notes that "the use of passwords for security does not guarantee confidentiality," and "[a]ll e-mail and voicemail passwords for access to information on Holladay's communications system must be disclosed to Holladay." (Dkt. 94-2.)

C. Application of Attorney-Client Privilege to Plaintiff's E-Mails

Upon consideration of the applicable facts and caselaw, the Court finds that the factors weigh in favor of a finding that Plaintiff did not have a reasonable expectation of confidentiality in his workplace e-mails. First, it is clear that Holladay maintained a policy that allowed employees to have "very limited personal use" of Holladay's communications systems and explicitly banned certain personal use. Second, Holladay reserved the right to monitor employees' computer and e-mail. Third, Holladay reserved the right to access, read, and disclose any electronic communication sent or received over its communications systems. And fourth, Holladay made its employees, including Plaintiff, aware of its policy. Indeed, Plaintiff admits awareness of the policy, and Plaintiff certified his acknowledgment of and compliance with the policy. (Dkt. 94-3.) This sufficiently establishes his awareness of the policy, including the provision requiring that all e-mail passwords be disclosed to Holladay.

With regard to Holladay's practice of monitoring employee e-mails, neither party specified whether Holladay regularly monitored its employee's e-mails or electronically stored information. According to Plaintiff, he was "not aware that anyone at Holladay ever actually accessed [his] Holladay account emails, other than for IT Department operational support and/or maintenance," and his understanding was that Holladay rarely monitored employee e-mails. (Dkt. 96, Ex. 1 ¶¶ 7–8.) Likewise, Plaintiff argues that although he was aware of Holladay's policy regarding the potential for monitoring and accessing employees' emails, "[t]he 'operational reality' was that [he] was not aware of Holladay accessing or auditing employee e-mail accounts for purposes unrelated to Holladay's business needs." (Dkt. 96 at 9–10.) Plaintiff therefore admits that he was aware that Holladay did in fact monitor and access employee accounts but only for *certain* purposes. This distinction, however, is insufficient to establish that Plaintiff was unaware of Holladay's policy or that Holladay did not enforce its policy.

The explicit language in Holladay's policy further undermines Plaintiff's argument, as the policy expressly reserves the right to monitor, access, and disclose all electronic communications received or sent over Holladay's communications systems for *any purpose*. (Dkt. 94-1.) Under the circumstances, it is clear that Plaintiff was aware that Holladay could access and monitor employee e-mails and that Holladay did in fact access and monitor employee accounts for at least some purpose. *See Goldstein v. Colborne Acquisition Co., LLC*, 873 F. Supp. 2d 932, 938 (N.D. Ill. 2012) (finding that the employees' "subjective belief that their communications were confidential was not a reasonable one in light of the company policy in place, and in light of their failure to assert that they were unaware of it").

It is well-settled that the party invoking the attorney-client privilege bears the burden of proving that the particular communications are confidential. *See In re Grand Jury Proceedings in*

Matter of Freeman, 708 F.2d 1571, 1575 (11th Cir. 1983) (stating that the party invoking the privilege has the burden of establishing the confidential nature of the communication). In this case, Plaintiff has asserted that the e-mails are privileged, and therefore he bears the burden of proving the confidentiality of the communications. Plaintiff's subjective belief that Holladay rarely monitored employee e-mails, standing alone, is insufficient to meet his burden. *See Alamar Ranch*, 2009 WL 3669741, at *4 (rejecting the employee's assertion that she was not aware of any company monitoring and finding the assertion unreasonable).

In support of his assertion that his communications were confidential, Plaintiff refers to a provision in Holladay's policy that communications should be treated as confidential and accessed only by the intended recipient. (Dkt. 94-1.) This provision, however, only indicates that employees are to regard e-mail communications of other employees as confidential, specifying that "[e]mployees are not authorized to retrieve or read any communications that are not sent to them." (Dkt. 94-1.) It does not qualify or restrict Holladay's reservation of the right to access and monitor e-mail communications. *See Hanson*, 2011 WL 5201430, at *6 (analyzing a similar provision and finding that it applied to the receipt of communications by other employees, not the employer).

Plaintiff's argument relies primarily on his subjective belief that e-mails he accessed on his workplace account were confidential. However, as noted above, the question is not whether he thought or believed his communications were confidential but rather whether his expectation was reasonable under the circumstances. *See Pensacola Firefighters' Relief Pension Fund Bd. of Trustees v. Merrill Lynch Pierce Fenner & Smith, Inc.*, No. 3:09CV53/MCR/MD, 2011 WL 3512180, at *8 (N.D. Fla. July 7, 2011) (emphasizing that the dispositive question is whether, under the circumstances, the individual reasonably believed that his or her communications were

confidential despite the existence of a workplace policy and despite the individual's subjective belief that the communications were exchanged in confidence).

In light of the explicit provisions in Holladay's policy and Plaintiff's awareness of these provisions, the Court finds that Plaintiff did not have a reasonable expectation that the handful of e-mails he sent or received over Holladay's communications systems were confidential. Specifically, as noted above, the policy expressly limited personal use of Holladay's communications systems, banned the use of the system for the operation of personal business or personal gain, reserved the right to access and monitor employee use for any purpose, warned employees that they had no expectation of privacy in e-mails transmitted over the company system, and required that employees—including Plaintiff—certify compliance with its provisions by signing an acknowledgment form. Plaintiff was well aware of Holladay's policy, including the unequivocal notice that his communications were not to be regarded as confidential, and the risk that his e-mail account would be monitored and accessed. As such, Plaintiff has not met his burden of showing that his communications were reasonably expected and understood to be confidential. Accordingly, it is

ORDERED that Defendant's Motion for a Determination That Certain E-Mail Communications Are Not Privileged or Otherwise Protected from Discovery (Dkt. 94) is **GRANTED**.

DONE and **ORDERED** in Tampa, Florida, on July 20, 2016.

JULIE S. SNEED
UNITED STATES MAGISTRATE JUDGE

Copies furnished to:

Counsel of Record