Ehling v. Monmouth-Ocean Hosp. Serv. Corp.

United States District Court for the District of New Jersey

August 20, 2013, Decided; August 20, 2013, Filed

Civ. No. 2:11-cv-03305 (WJM)

Reporter
961 F. Supp. 2d 659 *; 2013 U.S. Dist. LEXIS 117689 **; 36 I.E.R. Cas. (BNA) 749; 2013 WL 4436539

DEBORAH EHLING, Plaintiff, v. MONMOUTH-OCEAN HOSPITAL SERVICE CORP., et al., Defendants.

Prior History: Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 2012 U.S. Dist. LEXIS 74558 (D.N.J., 2012)

Core Terms

user, posts, electronic communication, privacy, disciplinary, friends, Communications, termination, medical leave, electronic, certifications, configured, provides, summary judgment motion, summary judgment, storage, accrue, networking, paperwork, reasons, Counts, retaliation, intrusion, applies, asserts, website, adverse employment action, suspension, accessing, purposes

Case Summary

Overview

HOLDINGS: [1]-A nonprofit hospital service corporation did not violate a former employee's rights under the Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, or the employee's common-law right to privacy, because another employee who had access to the employee's social networking site copied items that were posted on the site and provided those copies to the employee's supervisor; [2]-Evidence the corporation submitted in support of its motion for summary judgment demonstrated that the employee was terminated from her job as a registered nurse and paramedic because she took medical leave and did not return to work, and was sufficient to negate the employee's claims alleging that the hospital violated the FMLA, 29 U.S.C.S. § 2601 et seq., and New Jersey's Conscientious Employee Protection Act, N.J. Stat. Ann. § 34:19-1 et seq., when it terminated her employment.

Outcome

The court granted defendants' motion for summary judgment.

LexisNexis® Headnotes

Civil Procedure > ... > Summary Judgment > Entitlement as Matter of Law > Appropriateness

Civil Procedure > Judgments > Summary Judgment > Evidentiary Considerations

Civil Procedure > ... > Summary Judgment > Entitlement as Matter of Law > Genuine Disputes

Civil Procedure > ... > Summary Judgment > Entitlement as Matter of Law > Materiality of Facts

HN1[] Entitlement as Matter of Law, Appropriateness

Fed. R. Civ. P. 56 provides for summary judgment if the pleadings, the discovery (including, depositions, answers to interrogatories, and admissions on file) and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law. A factual dispute is genuine if a reasonable jury could find for the nonmoving party, and is material if it will affect the outcome of the trial under governing substantive law. A court considers all evidence and inferences drawn therefrom in the light most favorable to the nonmoving party.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

Communications Law > Federal Acts > Electronic Communications Privacy Act

HN2[] Federal Acts, Stored Communications Act

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA), which was intended to afford privacy protection to electronic communications. Pub. L. No. 99-508, 100 Stat. 1848. Title II of the ECPA contains the Federal Stored Communications Act (SCA), 18 U.S.C.S. §§ 2701-2711, which was designed to address access to stored wire and electronic communications and transactional records. The legislative history of the SCA suggests that Congress wanted to protect electronic communications that are configured to be private. Because the SCA was passed in 1986, the statute is best understood by considering its operation and purpose in light of the technology that existed in 1986.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN3[] Federal Acts, Stored Communications Act

The Federal Stored Communications Act (SCA), 18 U.S.C.S. §§ 2701-2711, provides that whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided, or (2) intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents the authorized access to a wire or electronic communication while in electronic storage in such a system shall be liable for damages. 18 U.S.C.S. §§ 2701(a) and 2707. The statute further provides that it shall not be unlawful to access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public. 18 U.S.C.S. § 2511(2)(g)(i). In other words, the SCA covers (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) that are not public.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN4[] Federal Acts, Stored Communications Act

The Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, defines "electronic communication" as any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system. 18 U.S.C.S. § 2510(12).

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN5[] Federal Acts, Stored Communications Act

The Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, defines "electronic communication service" as any service which provides to users thereof the ability to send or receive wire or electronic communications. 18 U.S.C.S. § 2510(15).

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN6[] Federal Acts, Stored Communications Act

The Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, distinguishes between two different types of electronic storage. The first is defined as any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof. 18 U.S.C.S. § 2510(17)(A). The second type of storage is defined as any storage of such communication by an electronic communication service for purposes of backup protection of such communication. 18 U.S.C.S. § 2510(17)(B).

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

Communications Law > Federal Acts > Electronic Communications Privacy Act

HN7[] Federal Acts, Stored Communications Act

The touchstone of the Electronic Communications Privacy Act, Pub. L. No. 99-508, 100 Stat. 1848, is that it protects private information. The language of the statute makes it clear that the statute's purpose is to protect information that the communicator took steps to keep private. 18 U.S.C.S. § 2511(2)(g)(i). Cases interpreting the Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, confirm that information is protectable as long as the communicator actively restricts the public from accessing the information.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN8[] Federal Acts, Stored Communications Act

The Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, does not apply with respect to conduct authorized (1) by a person or entity providing a wire or electronic communications service, or (2) by a user of that service with respect to a communication of or intended for that user. 18 U.S.C.S. § 2701(c). The authorized user exception applies where (1) access to a communication was authorized (2) by a user of that service, (3) with respect to a communication intended for that user. 18 U.S.C.S. § 2701(c)(2). Access is not authorized if the purported authorization was coerced or provided under pressure.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Civil Rights Law > Protection of Rights > Privacy Rights > Electronic Communications

HN9[] Federal Acts, Stored Communications Act

A "user" under the Federal Stored Communications Act, 18 U.S.C.S. §§ 2701-2711, is any person or entity who (A) uses an electronic communications service, and (B) is duly authorized by the provider of such service to engage in such use. 18 U.S.C.S. § 2510(13).

Labor & Employment Law > ... > Family & Medical Leaves > Scope & Definitions > Employee Leave Requirements

Labor & Employment Law > ... > Family & Medical Leaves > Scope & Definitions > Serious Health Conditions

HN10[] Scope & Definitions, Employee Leave Requirements

The Family and Medical Leave Act (FMLA) was enacted for several purposes, one of which was to entitle employees to take reasonable leave for medical reasons. 29 U.S.C.S. § 2601(b)(2). An employee is entitled to take twelve weeks of FMLA leave if that employee has a "serious health condition." 29 U.S.C.S. § 2612(a)(1)(D). An employer may require an employee to submit a certification to support the request for leave, which should include information such as the date on which the condition began, the probable duration of the condition, and the appropriate medical facts. 29

U.S.C.S. § 2613(b). An employer may also require an employee to obtain recertification if the circumstances described by a previous certification have changed significantly. 29 C.F.R. § 825.308; 29 U.S.C.S. § 2613(e). A certification is considered insufficient if the information provided is vague, ambiguous, or nonresponsive. 29 C.F.R. § 825.305.

Labor & Employment Law > ... > Family & Medical Leaves > Scope & Definitions > Employee Leave Requirements

Labor & Employment Law > ... > Retaliation > Statutory Application > Family & Medical Leave Act

Labor & Employment Law > Leaves of Absence > Family & Medical Leaves > Remedies

HN11 **Scope & Definitions, Employee Leave Requirements**

Two distinct causes of action are recognized under the Family and Medical Leave Act (FMLA): (1) an "interference" claim, where a plaintiff alleges that an employer interfered with her right to take FMLA leave; and (2) a "retaliation" claim, where a plaintiff alleges that the employer took an adverse employment action against her in retaliation for taking FMLA leave. 29 U.S.C.S. § 2615(a). To assert an interference claim, an employee only needs to show that he was entitled to benefits under the FMLA and that he was denied them.

Evidence > Burdens of Proof > Allocation

Labor & Employment Law > Leaves of Absence > Family & Medical Leaves > Burdens of Proof

Labor & Employment Law > ... > Retaliation > Statutory Application > Family & Medical Leave Act

Labor & Employment Law > Leaves of Absence > Family & Medical Leaves > Remedies

HN12 **Burdens of Proof, Allocation**

To establish a prima facie retaliation claim under the Family and Medical Leave Act (FMLA), a plaintiff must point to evidence in the record showing that (1) she invoked her right to FMLA-qualifying leave, (2) she suffered an adverse employment decision, and (3) the adverse action was causally related to her invocation of rights. Requiring an employee to clarify information on her FMLA certification is not an adverse employment decision.

Contracts Law > Remedies > Election of Remedies

Labor & Employment Law > Collective Bargaining & Labor Relations > Enforcement of Bargaining Agreements

Labor & Employment Law > ... > Retaliation > Remedies > General Overview

Labor & Employment Law > ... > Retaliation > Statutory Application > Whistleblower Protection Act

HN13 **Remedies, Election of Remedies**

The New Jersey Conscientious Employee Protection Act's (CEPA's) waiver provision provides that the institution of an action in accordance with the CEPA shall be deemed a waiver of the rights and remedies available under any other contract, collective bargaining agreement, State law, rule, or regulation or under the common law. N.J. Stat. Ann. § 34:19-8. Although not every claim under New Jersey's Law Against Discrimination (NJLAD), N.J. Stat. Ann. § 10:5-12, is waived by the assertion of a CEPA claim, retaliation claims under the NJLAD necessarily fall within the CEPA waiver provision.

Evidence > Burdens of Proof > Allocation

Labor & Employment Law > ... > Retaliation > Statutory Application > Whistleblower Protection Act

HN14 **Burdens of Proof, Allocation**

To establish a prima facie case of retaliation under New

Jersey's Conscientious Employee Protection Act, a plaintiff must demonstrate: (1) a reasonable belief that the employer's conduct was violating either a law, rule, regulation, or public policy; (2) the plaintiff performed a "whistle blowing" activity as described in N.J. Stat. Ann. § 34:19-3(a) or (c); (3) an adverse employment action was taken against the plaintiff; and (4) a causal connection existed between the whistle-blowing activity and the adverse employment action.

Labor & Employment
Law > ... > Retaliation > Statutory Application > Whistleblower Protection Act

HN15[] Statutory Application, Whistleblower Protection Act

New Jersey's Conscientious Employee Protection Act defines "retaliatory action" as the discharge, suspension, or demotion of an employee, or other adverse employment action taken against an employee in the terms and conditions of employment. N.J. Stat. Ann. § 34:19-2(e).

Evidence > Burdens of Proof > Allocation

Labor & Employment
Law > ... > Retaliation > Statutory Application > Whistleblower Protection Act

HN16[] Burdens of Proof, Allocation

To prove causation under New Jersey's Conscientious Employee Protection Act, a plaintiff must show that retaliatory discrimination by his or her employer was more likely than not a determinative factor in an adverse employment decision.

Labor & Employment Law > Employee Privacy > Invasion of Privacy

Torts > ... > Invasion of Privacy > Intrusions > Elements

HN17[] Employee Privacy, Invasion of Privacy

A claim for invasion of privacy under New Jersey law will succeed if a plaintiff brings forth evidence showing that (1) there was an intentional intrusion upon the solitude or seclusion of another or his private affairs, and that (2) this intrusion would highly offend a reasonable person. Under the first prong, a defendant must commit an intrusive act. The converse of this principle is that there is no wrong where a defendant did not actually delve into a plaintiff's concerns.

Counsel: **[**1]** For DEBORAH EHLING, Plaintiff: ERNEST HENRY EHLING, LEAD ATTORNEY, FREEHOLD, NJ 07728.

For MONMOUTH-OCEAN HOSPITAL SERVICE CORP, doing business as MONOC, Defendant: M. ELIZABETH DUFFY, LEAD ATTORNEY, DALY, LAMASTRA & CUNNINGHAM, WHITEHOUSE STATION, NJ.

For VINCENT ROBBINS, individually, STACY QUAGLIANA, individually, Defendants: M. ELIZABETH DUFFY, DALY, LAMASTRA & CUNNINGHAM, WHITEHOUSE STATION, NJ.

Judges: WILLIAM J. MARTINI, United States District Judge.

Opinion by: WILLIAM J. MARTINI

Opinion

[*661] OPINION

WILLIAM J. MARTINI, U.S.D.J.:

Plaintiff Deborah Ehling filed this action against Monmouth-Ocean Hospital Service Corp. ("MONOC"), Vincent Robbins, and Stacy Quagliana (collectively "Defendants"). This matter comes before the Court on Defendants' motion for summary judgment under Federal Rule of Civil Procedure 56. There was no oral argument. Fed. R. Civ. P. 78(b). For the reasons set forth below, Defendants' motion for summary judgment is **GRANTED.**

I. BACKGROUND

Plaintiff Deborah Ehling is a registered nurse and paramedic. Defendant MONOC is a non-profit hospital service corporation dedicated to providing emergency medical services to the citizens of the State of New Jersey. Defendant Vincent Robbins is the President and **[**2]** CEO of MONOC. Defendant Stacy Quagliana is

the Executive Director of Administration at MONOC.

Plaintiff was hired by MONOC in 2004 as a registered nurse and paramedic. In July of 2008, Plaintiff took over as President of the Professional Emergency Medical Services Association – New Jersey (the "Union"). As President of the Union, Plaintiff was regularly involved in actions intended to protect MONOC employees. For example, Plaintiff filed complaints with the Environmental Protection Agency ("EPA") and the New Jersey Department of Environmental Protection ("NJDEP"), reporting that MONOC's use of a disinfectant called Zimek was creating health problems for employees. In response, the EPA issued a removal order requiring MONOC to stop using Zimek. Plaintiff **[*662]** also testified in the wage and hour lawsuit of another MONOC employee.

Plaintiff's claims in this case arise out of: (1) an incident involving Plaintiff's Facebook account, and (2) Plaintiff's disciplinary record and medical leave. The Court will summarize the pertinent facts relating to each issue.

A. The Facebook Incident

Facebook is a widely-used social-networking website. The website provides a digital medium that allows users to connect **[**3]** and communicate with each other. Every Facebook user must create a Profile Page, which is a webpage that is intended to convey information about the user. The Profile Page can include the user's contact information; pictures; biographical information, such as the user's birthday, hometown, educational background, work history, family members, and relationship status; and lists of places, musicians, movies, books, businesses, and products that the user likes. A Facebook user can connect with other users by adding them as "Facebook friends." Facebook users can have dozens, hundreds, or even thousands of Facebook friends. In addition to having a Profile Page, each user has a webpage called a News Feed. The News Feed aggregates information that has recently been shared by the user's Facebook friends. By default, Facebook pages are public. However, Facebook has customizable privacy settings that allow users to restrict access to their Facebook content. Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user.

Facebook provides users with several means of communicating with one another. Users can send private messages to one or more users. **[**4]** Users can also communicate by posting information to their Facebook "wall," which is part of each user's Profile Page. A Facebook "wall post" can include written comments, photographs, digital images, videos, and content from other websites. To create a Facebook wall post, users upload data from their computers or mobile devices directly to the Facebook website. Facebook then saves that data onto its computers (called "servers"). New wall posts are typically distributed to a user's Facebook friends using the News Feed feature. Users' most recent wall posts also appear at the top of their Profile Pages. A user's Facebook friends can comment on the wall posts, indicate that they "like" the wall posts, or share the posts with other users. Facebook users typically do not post information to their Facebook walls with the intent to delete it later. Instead, Facebook designed its website so that its servers would save this data indefinitely. As more and more wall posts are added, earlier wall posts move lower and lower down on the user's Profile Page, and are eventually archived on separate pages that are accessible, but not displayed.[1]

During the 2008-2009 timeframe, Plaintiff maintained a Facebook account and had approximately 300 Facebook friends. Plaintiff selected privacy settings for her account that limited access to her Facebook **[*663]** wall to only her Facebook friends. Plaintiff did not add any MONOC managers as Facebook friends. However, Plaintiff added many of her MONOC coworkers as friends, including a paramedic named Tim Ronco. Plaintiff posted on Ronco's Facebook wall, and Ronco had access to Plaintiff's Facebook wall. Unbeknownst to Plaintiff, Ronco was taking screenshots of Plaintiff's Facebook wall and printing them or emailing them to MONOC manager Andrew Caruso. Ronco **[**6]** and Caruso became friends while working together at a previous job, but Ronco never worked in Caruso's division at MONOC. The evidence reflects that Ronco independently came up with the idea to provide Plaintiff's Facebook posts to Caruso. Caruso never asked Ronco for any information about Plaintiff, and

[1] For information about how Facebook works, *see* Mark Allen **[**5]** Chen, *Interactive Contracting in Social Networks,* 97 Cornell L. Rev. 1533, 1542 (2012); James Grimmelmann, *Saving Facebook,* 94 Iowa L. Rev. 1137, 1142-50 (2009); *United States v. Jeffries, No. 3:10-CR-100, 2010 U.S. Dist. LEXIS 125665, 2010 WL 4923335, at *5 n.3 (E.D. Tenn. Oct. 22, 2010)*; *Facebook, Inc. v. Power Ventures, Inc., No. 085780, 2009 U.S. Dist. LEXIS 42367, 2009 WL 1299698, at *1 (N.D. Cal. May 11, 2009)*; *Lane v. Facebook, Inc., No. 08-3845, 2009 U.S. Dist. LEXIS 103668, 2009 WL 3458198, at *1 & n.1 (N.D. Cal. Oct. 23, 2009)*; *Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 n.50 & 51 (C.D. Cal. 2010)*.

never requested that Ronco keep him apprised of Plaintiff's Facebook activity. In fact, Caruso was surprised that Ronco showed him Plaintiff's Facebook posts. Caruso never had the password to Ronco's Facebook account, Plaintiff's Facebook account, or any other employee's Facebook account. Once Caruso received copies of Plaintiff's Facebook posts, he passed them on to Quagliana, MONOC's Executive Director of Administration.

On June 8, 2009, Plaintiff posted the following statement to her Facebook wall:

> An 88 yr old sociopath white supremacist opened fire in the Wash D.C. Holocaust Museum this morning and killed an innocent guard (leaving children). Other guards opened fire. The 88 yr old was shot. He survived. I blame the DC paramedics. I want to say 2 things to the DC medics. 1. WHAT WERE YOU THINKING? and 2. This was your opportunity to really make a difference! WTF!!!! And to the other **[**7]** guards....go to target practice.

After MONOC management was alerted to the post, Plaintiff was temporarily suspended ***with*** pay, and received a memo stating that MONOC management was concerned that Plaintiff's comment reflected a "deliberate disregard for patient safety." In response, Plaintiff filed a complaint with the National Labor Relations Board ("NLRB"). After reviewing the evidence, the NLRB found that MONOC did not violate the National Labor Relations Act. The NLRB also found that there was no privacy violation because the post was sent, unsolicited, to MONOC management.

B. Plaintiff's Disciplinary Record and Medical Leave

MONOC disciplines employees in accordance with a "point" system. According to MONOC's written disciplinary policy, an employee who commits an infraction (such as being late to work) is given one point. Points accumulate if there are further infractions, and points accumulate more quickly if an employee commits the same infraction multiple times. Accumulating a certain number of points results in a disciplinary action. A MONOC employee who accrues seven, eight, or nine points is suspended, and an employee who accrues ten or more points is terminated. An employee **[**8]** can appeal any disciplinary action.

During the seven years that Plaintiff was employed at MONOC, Plaintiff developed an extensive disciplinary record. Plaintiff received six warning notices for lateness, and eleven additional warning notices for violations of MONOC policy, including unauthorized late swipe-outs, excessive call-outs, failing to have sufficient paid time off to cover hours not worked, refusing 9-1-1 calls, and failing to submit the proper documentation for her ambulance shifts. In 2010, after receiving numerous warning notices, Plaintiff began to accrue disciplinary points. Plaintiff steadily **[*664]** continued to accrue disciplinary points throughout 2010 and 2011.

During her employment at MONOC, Plaintiff also took numerous medical leaves. The Family and Medical Leave Act (or "FMLA") entitles employees to take up to twelve weeks of medical leave to recover from serious health conditions. Plaintiff took five continuous FMLA leaves for five different medical conditions, and also took intermittent FMLA leave over the course of approximately two years. Despite taking numerous medical leaves, Plaintiff frequently missed the deadlines for submitting FMLA paperwork, submitted paperwork **[**9]** that was incomplete or inaccurate, or failed to submit paperwork altogether. Nevertheless, MONOC granted Plaintiff all the FMLA leave that she requested, alerted Plaintiff when her paperwork was insufficient, sent her forms two or three times when she missed the deadlines, and even applied FMLA leave retroactively when she failed to make a timely request.

For example, on May 8, 2011, Plaintiff was dispatched to respond to a 9-1-1 call for a critically ill twenty-month old child. Plaintiff refused to do the emergency transport and placed her unit out of service, citing "FMLA reasons." On May 20, 2011, MONOC sent Plaintiff the FMLA paperwork, and asked for clarification on her medical condition. Plaintiff did not respond. Two weeks later, MONOC sent the paperwork to Plaintiff again, and Plaintiff responded by submitting a partially-complete form that did not contain any information from her doctor. MONOC followed up by asking Plaintiff to have a doctor sign the form, but Plaintiff never responded. Shortly thereafter, on June 8, 2011, Plaintiff filed the Complaint in this case.

Throughout this time period, Plaintiff continued to accrue disciplinary points for committing infractions such **[**10]** as arriving late to work. By July 2011, Plaintiff had accrued eight disciplinary points. On July 15, 2011, Plaintiff was issued a two-day suspension. However, MONOC's upper management (including Quagliana) determined that the suspension should be stayed so that Plaintiff could continue working. This meant that all disciplinary action would be put on hold for one year and then removed from Plaintiff's record, provided that Plaintiff did not accrue any more points. On July 17,

2011, just two days after her suspension was stayed, Plaintiff skipped her evening shift to attend a "metaphysical seminar" featuring purported psychic medium James Van Praagh. When asked why she was not coming to work, Plaintiff cited "FMLA" reasons. In the following days, Plaintiff continued to be late to work, and by July 22, 2011, she had accumulated a total of twelve disciplinary points. Plaintiff was then issued a notice of termination. However, MONOC's upper management determined that the termination should be stayed. Thus, neither the suspension nor the termination was ever enforced.

On August 18, 2011, Plaintiff filed a nine-count Amended Complaint in this case. On September 9, 2011, Defendants filed a **[**11]** motion to dismiss.

In October 2011, Plaintiff exhausted her twelve weeks of FMLA leave. Plaintiff told MONOC that she needed additional medical leave at that time, so she was offered a ninety-day personal leave of absence. MONOC sent Plaintiff the leave of absence forms twice, extending the deadline each time, but Plaintiff did not fill out the forms. Eventually, Quagliana filled out the forms herself and then approved them. Plaintiff's leave of absence was set to expire on January 18, 2012. On January 2, 2012, Plaintiff informed MONOC that she would not be returning to work **[*665]** until the end of March 2012. Plaintiff was informed that she could not take additional leave unless she filled out reasonable accommodation forms. MONOC sent Plaintiff the reasonable accommodation forms twice, but Plaintiff never completed them. Because Plaintiff never returned to work and never filled out the reasonable accommodation forms, Plaintiff was terminated on February 7, 2012. Plaintiff did not appeal her termination.

On March 8, 2012, Plaintiff's attorney withdrew from the representation. He was replaced by Plaintiff's brother. On May 30, 2012, this Court entered an Opinion and Order dismissing Count 2 **[**12]** of the Amended Complaint. In July 2012, Plaintiff voluntarily dismissed Counts 8 and 9 of the Amended Complaint. Defendants now move for summary judgment on the remaining counts.

II. LEGAL STANDARD

HN1[↑] *Federal Rule of Civil Procedure 56* provides for summary judgment "if the pleadings, the discovery [including, depositions, answers to interrogatories, and admissions on file] and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." *Fed. R. Civ. P. 56*; *see also Celotex Corp. v. Catrett, 477 U.S. 317, 322-23, 106 S. Ct. 2548, 91 L. Ed. 2d 265 (1986)*; *Turner v. Schering-Plough Corp., 901 F.2d 335, 340 (3d Cir. 1990)*. A factual dispute is genuine if a reasonable jury could find for the non-moving party, and is material if it will affect the outcome of the trial under governing substantive law. *Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986)*. The Court considers all evidence and inferences drawn therefrom in the light most favorable to the non-moving party. *Andreoli v. Gates, 482 F.3d 641, 647 (3d Cir. 2007)*.

III. DISCUSSION

Only six counts of the Amended Complaint remain:

(1) Count 1: Violation of the **[**13]** Federal Stored Communications Act;
(2) Count 3: Violation of the Family Medical Leave Act;
(3) Counts 4 and 7: Violations of the New Jersey Law Against Discrimination;
(4) Count 5: Violation of the Conscientious Employee Protection Act; and
(5) Count 6: Invasion of Privacy.

Defendants move for summary judgment on each of the remaining counts. The Court will address each count in turn.

A. Count 1: Federal Stored Communications Act

In Count 1, Plaintiff asserts a claim for violation of the Federal Stored Communications Act (or "SCA"), *18 U.S.C. §§ 2701-11*. Plaintiff argues that Defendants violated the SCA by improperly accessing her Facebook wall post about the museum shooting. Plaintiff argues that her Facebook wall posts are covered by the SCA because she selected privacy settings limiting access to her Facebook page to her Facebook friends. Defendants disagree and argue that, even if the SCA applies, the facts in this case fall under one of the SCA's statutory exceptions. For the reasons set forth below, the Court finds that non-public Facebook wall posts are covered by the SCA, and that one of the exceptions to the SCA applies. The Court will address each issue in turn.

i. The SCA Covers **[**14]** Non-Public Facebook Wall Posts

The first issue before the Court is whether the SCA applies to Facebook wall **[*666]** posts. Very few courts have addressed this issue. *See* Catherine Crane, *Social Networking v. the Employment-at-Will Doctrine: A Potential Defense for Employees Fired for Facebooking, Terminated for Twittering, Booted for Blogging, and Sacked for Social Networking,* 89 Wash. U.L. Rev. 639, 668 (2012) ("Very few courts, however, have ruled on whether other unique features found within social networking sites — such as wall posts, status updates, notes, pictures, etc. — could also be protected against employer intrusion under the SCA"). For the reasons set forth below, the Court finds that Facebook wall posts fall within the purview of the SCA.

HN2[] In 1986, Congress passed the Electronic Communications Privacy Act, which was intended to afford privacy protection to electronic communications. *See* Pub.L. No. 99-508, 100 Stat. 1848; Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002). Title II of the Electronic Communications Privacy Act contains the SCA, which was designed to "address[ ] access to stored wire and electronic communications and transactional records." S. Rep. **[**15]** No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557. "The legislative history of the [SCA] suggests that Congress wanted to protect electronic communications that are configured to be private." Konop, 302 F.3d at 875; *see also* S. Rep. No. 99-541, at 35-36, 1986 U.S.C.C.A.N. at 3599 ("This provision [the SCA] addresses the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public."); H.R. Rep. No. 99-647 at 41, 62-63 (1986) (describing the Committee's understanding that the configuration of an electronic communications system would determine whether an electronic communication was accessible to the public).

Because the SCA was passed in 1986, the statute "is best understood by considering its operation and purpose in light of the technology that existed in 1986." William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act,* 98 Geo. L.J. 1195, 1204 (2010). Computer networking was in its infancy in 1986. Id. at 1198. In the mid-1980s, "personal users [had just begun] subscribing to self-contained networks, such as Prodigy, CompuServe, **[**16]** and America Online." *Id.* After connecting to a network via a modem, users could download or send e-mail to other users, access a closed universe of content, and post messages on electronic bulletin board systems ("BBS's"). *Id.* A BBS was "a computer program that simulate[d] an actual bulletin board by allowing computer users who access[ed] a particular computer to post messages" for a community of people. United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990). Notably, the SCA was enacted before the advent of the World Wide Web in 1990 and before the introduction of the web browser in 1994. *Id.* "Despite the rapid evolution of computer and networking technology since the SCA's adoption, its language has remained surprisingly static." Id. at 1196. Thus, the "task of adapting the Act's language to modern technology has fallen largely upon the courts."[2] *Id.*

HN3[] The **[**17]** SCA provides that whoever "(1) intentionally accesses without authorization a facility through which an electronic **[*667]** communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents the authorized access to a wire or electronic communication while in electronic storage in such a system" shall be liable for damages. 18 U.S.C. § 2701(a); 18 U.S.C. § 2707 (providing for civil liability under the statute). The statute further provides that "[i]t shall not be unlawful . . . [to] access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). In other words, the SCA covers: (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) that are not public. Facebook wall posts that are configured to be private meet all four criteria.

First, Facebook wall posts are electronic communications. HN4[] The SCA defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, **[**18]** data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). To create Facebook wall posts, Facebook users transmit writing, images, or other data via the Internet from their computers or mobile devices to Facebook's servers. Mark Allen Chen, *Interactive Contracting in Social Networks,* 97 Cornell L.

---

[2] Most courts, including this one, would prefer that Congress update the statute to take into account the invention of the Internet. As the Ninth Circuit observed, "until Congress brings the laws in line with modern technology, protection of the Internet . . . will remain a confusing and uncertain area of the law." Konop, 302 F.3d at 874.

Rev. 1533, 1542 (2012) ("When Alice uploads the picture to Facebook, she sends a copy of that data over the Internet. Facebook then saves that data onto its computers (called 'servers')."). Thus, Facebook wall posts are electronic communications. *See* Konop, 302 F.3d at 876 (finding similar website postings to be electronic communications under the SCA).

Second, Facebook wall posts are transmitted via an electronic communication service. **HN5**[↑] The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Facebook provides its users with the ability to send and receive electronic communications, including private messages and Facebook wall posts. Accordingly, Facebook **[**19]** is an electronic communication service provider. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 982 (C.D. Cal. 2010) (finding that Facebook and MySpace are electronic communication service providers).

Third, Facebook wall posts are in electronic storage. **HN6**[↑] The SCA distinguishes between two different types of electronic storage. The first is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). The second type of storage is defined as "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). Unlike email, Facebook wall posts are not held somewhere temporarily before they are delivered. Crispin, 717 F. Supp. 2d at 989 ("[I]n in the context of a social-networking site such as Facebook or MySpace, there is no temporary, intermediate step for wall postings or comments."). Rather, the website itself is the final destination for the information. *Id.* (citing Snow v. DIRECTV, Inc., No. 04-515 (RGM), 2005 U.S. Dist. LEXIS 48652, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005)). Thus, Facebook wall posts are **[**20]** not held in temporary, intermediate storage.

However, Facebook does store electronic communications for backup purposes. When Facebook users post information, **[*668]** the information is immediately saved to a Facebook server. When new posts are added, Facebook archives older posts on separate pages that are accessible, but not displayed. Crispin, 717 F. Supp. 2d at 990 n.51 ("As more and more wall postings or comments are added . . . earlier wall postings . . . [are] eventually archived to separate pages."). Because Facebook saves and archives wall posts indefinitely, the Court finds that wall posts are stored for backup purposes. *See* id. at 989 n.50 ("*Theofel, Quon,* and *Konop* implicitly held that although a user may have other purposes for . . . leaving a post on his or her Facebook wall . . . one of multiple purposes may be for backup storage"). Accordingly, Facebook wall posts are in electronic storage.

Fourth, Facebook wall posts that are configured to be private are, by definition, not accessible to the general public. **HN7**[↑] The touchstone of the Electronic Communications Privacy Act is that it protects private information. The language of the statute makes clear that the statute's purpose is **[**21]** to protect information that the communicator took steps to keep private. *See* 18 U.S.C. § 2511(2)(g)(i) (there is no protection for information that is "configured [to be] readily accessible to the general public"); *see also* Konop, 302 F.3d at 875 ("The legislative history of the [Electronic Communications Privacy Act] suggests that Congress wanted to protect electronic communications that are configured to be private"). Cases interpreting the SCA confirm that information is protectable as long as the communicator actively restricts the public from accessing the information. *See* Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding that SCA prevented Viacom from accessing YouTube "videos that [users] have designated as private and chosen to share only with specified recipients"); Crispin, 717 F. Supp. 2d at 991 (finding that SCA protection for Facebook wall posts depends on plaintiff's use of privacy settings); *cf.* Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006) ("an express warning, on an otherwise publicly accessible webpage" is insufficient to give rise to SCA protection).

Facebook allows users to select privacy settings for their Facebook walls. **[**22]** Access can be limited to the user's Facebook friends, to particular groups or individuals, or to just the user. The Court finds that, when users make their Facebook wall posts inaccessible to the general public, the wall posts are "configured to be private" for purposes of the SCA. The Court notes that when it comes to privacy protection, the critical inquiry is whether Facebook users took steps to limit access to the information on their Facebook walls. Privacy protection provided by the SCA does not depend on the number of Facebook friends that a user has. "Indeed, basing a rule on the number of users who can access information would result in arbitrary line-drawing" and would be legally unworkable. Crispin, 717 F. Supp. 2d at 990; *see also* Crane, 89 Wash. U.L. Rev.

at 641 ("The fulcrum in [the privacy] balancing act exists as one, seemingly obvious, factor: privacy settings.").

At least one other court has determined that non-public Facebook wall posts are covered by the SCA, albeit in a slightly different context. In *Crispin,* the District Court for the Central District of California was asked to decide whether a third-party subpoena should be quashed under the SCA. Crispin, 717 F. Supp. 2d at 976. **[**23]** The defendants in *Crispin* subpoenaed information located on the plaintiff's MySpace and Facebook pages, including the plaintiff's Facebook wall posts and MySpace **[*669]** comments. Id. at 968-69. The plaintiff sought to quash the subpoena, arguing that the SCA prohibited Facebook and MySpace from disclosing the information. Id. at 969. To determine whether the SCA applied to these communications, the court analogized a Facebook wall post to technology that existed in 1986: a posting on a BBS. Id. at 980. A BBS could be configured to be public or private. *See* Kaufman v. Nest Seekers, LLC, No. 05-6782, 2006 U.S. Dist. LEXIS 71104, 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006). If a BBS was configured to be private, access to the BBS was restricted to a particular community of users, and the messages posted to the BBS were only viewable by those users. *See* Crispin, 717 F. Supp. 2d at 980-82. The *Crispin* court recognized that there was a long line of cases finding that the SCA was intended to reach private BBS's. Id. at 981(collecting cases). The court then found that there was "no basis for distinguishing between a restrictedaccess BBS and a user's Facebook wall or MySpace comments": both technologies allowed users to **[**24]** post content to a restricted group of people, but not the public at large. Id. at 981. The court therefore concluded that, if the plaintiff's Facebook page was configured to be private, then his wall posts were covered by the SCA. Id. at 991. This Court agrees in all respects with the reasoning of Crispin.

Accordingly, the Court finds that non-public Facebook wall posts are covered by the SCA. Because Plaintiff in this case chose privacy settings that limited access to her Facebook wall to only her Facebook friends, the Court finds that Plaintiff's Facebook wall posts are covered by the SCA.

ii. The SCA's Authorized User Exception Applies in this Case

Having concluded that the SCA applies to the type of communication at issue in this case, the Court next evaluates whether either of the SCA's statutory exceptions apply. **HN8**[↑] The SCA "does not apply with respect to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. §2701(c); *see also* Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2009 U.S. Dist. LEXIS 88702, 2009 WL 3128420, at *2 (D.N.J. Sept. 25, 2009) ("According **[**25]** to the SCA, if access to [a restricted website] was authorized by a user of that service with respect to a communication of or intended for that user, there is no statutory violation") (internal quotations omitted). For the reasons set forth below, the Court finds that the authorized user exception (the second exception) applies in this case.

The authorized user exception applies where (1) access to the communication was "authorized," (2) "by a user of that service," (3) "with respect to a communication . . . intended for that user." 18 U.S.C. § 2701(c)(2). Access is not authorized if the "purported 'authorization' was coerced or provided under pressure." Pietrylo, 2009 U.S. Dist. LEXIS 88702, 2009 WL 3128420, at *3. In this case, all three elements of the authorized user exception are present.

First, access to Plaintiff's Facebook wall post was "authorized." 18 U.S.C. § 2701(c)(2). The undisputed evidence establishes that Ronco voluntarily provided Plaintiff's Facebook posts to MONOC management without any coercion or pressure. Caruso testified at his deposition that Plaintiff's Facebook friend Ronco voluntarily took screenshots of Plaintiff's Facebook page and either emailed those screenshots to Caruso or printed **[**26]** them out for him. Certification of M. Elizabeth Duffy Ex. C 42:20-43:3, 45:11-22, ECF **[*670]** No. 36-1.[3] This information was completely unsolicited. Caruso never asked Ronco for any information about Plaintiff and never requested that Ronco keep him apprised of Plaintiff's Facebook activity; in fact, Caruso was surprised that Ronco showed him Plaintiff's Facebook postings. Ex. C 43:6-8, 44:23-45:1, 52:11-17, 53:4-8, 62:19-21, 87:18-88:1. Caruso never had the password to Ronco's Facebook account, Plainitiff's Facebook account, or any other employee's Facebook account. Ex. C 44:7-9, 88:13-21. Caruso's deposition testimony is supported by additional evidence, including a copy of a May 10, 2009 email from Ronco to Caruso attaching copies of Plaintiff's Facebook posts,

[3] Hereinafter, citations to the Certification of M. Elizabeth Duffy will be referred to using only the Exhibit number.

Quagliana's testimony that she never asked Caruso or anyone else to provide her with a copy of Plaintiff's Facebook page, and Caruso's NLRB affidavit. Ex. H, D 619; Ex. E 47:9-49:6; Ex. H, D 425.

Plaintiff provided no evidence to support her theory that access to her Facebook page was unauthorized. In the Amended Complaint, **[**27]** Plaintiff alleged that Defendants gained access to her Facebook page because a "member of upper management summoned a MONOC employee, who was also one of Ms. Ehling's Facebook friends, into his office" and "coerced, strong-armed, and/or threatened this employee into accessing his Facebook account on the work computer in the supervisor's presence." Am. Compl. ¶ 20. After discovery, it became clear that this was not the case. Instead, the evidence reflected that Ronco voluntarily shared this information with Caruso. Plaintiff now surmises that Ronco must have shared the information for "compensation or privileged treatment or a really good deal." Ex. B 139:5-11. But this theory does not make sense in light of MONOC's management structure. Ronco never worked in a division that Caruso oversaw, and Caruso never had control over Ronco's pay or bonuses, so Caruso was not in a position to offer Ronco any sort of benefit. Ex. C 53:11-19, 86:3-10. Furthermore, Plaintiff's theory is pure speculation. Plaintiff did not depose Ronco because Ronco was "traveling in an RV" and no longer worked for MONOC. Ex. C 62:2-3. And Plaintiff produced no other evidence that Ronco provided information in exchange **[**28]** for compensation (or some other benefit). Thus, the undisputed evidence shows that access to Plaintiff's Facebook wall post was authorized.

Second, access to Plaintiff's Facebook wall post was authorized "by a user of that service." *18 U.S.C. § 2701(c)(2)*. ***HN9***[↑] A "user" is "any person or entity who (A) uses an electronic communications service; and (B) is duly authorized by the provider of such service to engage in such use." *18 U.S.C. § 2510(13)*. It is undisputed that Ronco was a Facebook user: Plaintiff acknowledged that she added Ronco as a Facebook friend and posted on Ronco's Facebook wall. Ex. B 150:17-152:16.

Third, Plaintiff's Facebook wall post was "intended for that user." *18 U.S.C. § 2701(c)(2)*. Based on the privacy settings that Plaintiff selected for her Facebook page, Plaintiff's wall posts were visible to, and intended to be viewed by, Plaintiff's Facebook friends. Am. Compl. ¶ 11. On June 8, 2009, when Plaintiff posted the comment about the museum shooting, Ronco was one of Plaintiff's Facebook friends. Ehling Cert. Ex. A 155:8-21, ECF No. 38. Thus, the post was intended for Ronco.

[*671] In conclusion, access to Plaintiff's Facebook wall post was authorized by a Facebook user with **[**29]** respect to a communication intended for that user. Therefore, the authorized user exception applies and Defendants are not liable under the SCA. Accordingly, the motion for summary judgment on Count 1 is **GRANTED.**

B. Count 3: Family Medical Leave Act

In Count 3, Plaintiff asserts a claim for violation of the Family Medical Leave Act, *29 U.S.C. § 2601*. Defendants move for summary judgment. The Court finds that summary judgment should be granted on Count 3.

HN10[↑] The Family and Medical Leave Act was enacted for several purposes, one of which was to "entitle employees to take reasonable leave for medical reasons." *29 U.S.C. § 2601 (b)(2)*. An employee is entitled to take twelve weeks of FMLA leave if that employee has a "serious health condition." *29 U.S.C. § 2612(a)(1)(D)*. An employer may require an employee to submit a certification to support the request for leave, which should include information such as the date on which the condition began, the probable duration of the condition, and the appropriate medical facts. *29 U.S.C. § 2613 (b)*. An employer may also require an employee to obtain recertification if the "circumstances described by the previous certification have changed significantly." **[**30]** *29 C.F.R. § 825.308*; *29 U.S.C. § 2613 (e)*. A certification is "considered insufficient if . . . the information provided is vague, ambiguous, or non-responsive." *29 C.F.R. § 825.305*.

HN11[↑] Two distinct causes of action are recognized under the FMLA: (1) an "interference" claim, where a plaintiff alleges that an employer interfered with her right to take FMLA leave; and (2) a "retaliation" claim, where a plaintiff alleges that the employer took an adverse employment action against her in retaliation for taking FMLA leave. *Erdman v. Nationwide Ins. Co., 582 F.3d 500, 508 (3d Cir. 2009)*; *29 U.S.C. § 2615 (a)*. Plaintiff asserts both causes of action in this case.

Plaintiff failed to proffer evidence to support her FMLA interference claim. To assert an interference claim, an employee "only needs to show that he was entitled to benefits under the FMLA and that he was denied them." *Sommer v. The Vanguard Grp., 461 F.3d 397, 399 (3d*

Cir. 2006). In this case, the evidence demonstrates that: Plaintiff took five continuous FMLA leaves; Plaintiff took multiple intermittent FMLA leaves; Plaintiff frequently missed the deadlines for filing FMLA certifications, filed certifications with inaccurate information, **[**31]** or failed to file certifications altogether; Defendants nevertheless granted Plaintiff all the FMLA leave that she requested; Defendants alerted Plaintiff when her paperwork was insufficient, sent her forms two or three times when she missed the deadlines, and even applied FMLA leave retroactively when Plaintiff failed to make a timely request; and Plaintiff exhausted her twelve weeks of FMLA leave in October 2011. Ex. B at 65-69, 70, 73-74, 76, 79-81, 99, 100-01, 10608, 122; Exs. G12, G16, G19, G23, G24. In her brief, "plaintiff admits that defendants eventually gave her the FMLA leaves," but she objects to the fact that "she received leave only after MONOC rejected plaintiff's paperwork on several occasions." Opp. Br. at 29, ECF No. 39. Under the FMLA, Defendants clearly had a right to request FMLA certifications and re-certifications from Plaintiff, and to reject the insufficient certifications that she submitted. In fact, given the circumstances, Defendants were extremely accommodating of Plaintiff's many FMLA requests.

[*672] Plaintiff also failed to proffer evidence to support her FMLA retaliation claim. ***HN12***[↑] To establish a *prima facie* retaliation claim, a plaintiff must point to evidence **[**32]** in the record showing that "(1) she invoked her right to FMLA-qualifying leave, (2) she suffered an adverse employment decision, and (3) the adverse action was causally related to her invocation of rights." *Lichtenstein v. Univ. of Pittsburgh Med. Ctr., 691 F.3d 294, 301-02 (3d Cir. 2012)*. In two sentences of her brief, Plaintiff argues that there was retaliation because, "[a]lthough defendants eventually granted Ms. Ehling the FMLA leave she was entitled to, it was only after repeated denials of her . . . FMLA paperwork." Opp. Br. at 29. Requiring Plaintiff to clarify information on her FMLA certification is not an adverse employment decision. And Plaintiff does not point to any other evidence that she suffered an adverse employment decision as a result of taking medical leave.

Accordingly, the motion for summary judgment on Count 3 is **GRANTED.**

C. Counts 4 and 7: New Jersey Law Against Discrimination

In Counts 4 and 7, Plaintiff asserts retaliation claims under the New Jersey Law Against Discrimination ("NJLAD"), *N.J.S.A. 10:5-12*. In Count 4, Plaintiff alleges that Defendants retaliated against her for testifying in her co-worker's wage and hour case. In Count 7, Plaintiff alleges that **[**33]** Defendants retaliated against her for filing this lawsuit. Defendants move for summary judgment on both counts, arguing that Plaintiff waived the right to bring such claims when she filed a claim under the New Jersey Conscientious Employee Protection Act (or "CEPA"), *N.J.S.A. 34:19-1*. The Court agrees.

HN13[↑] CEPA's waiver provision provides that:

> [T]he institution of an action in accordance with this act shall be deemed a waiver of the rights and remedies available under any other contract, collective bargaining agreement, State law, rule or regulation or under the common law.

N.J.S.A. 34:19-8. Although not every NJLAD claim is waived by the assertion of a CEPA claim, "retaliation claims under the LAD necessarily fall within the CEPA waiver provision." *Ivan v. Cnty. of Middlesex, 595 F. Supp. 2d 425, 465-66 (D.N.J. 2009)*; *see also Bowen v. Parking Authority of the City of Camden, No. 00-5765, 2003 U.S. Dist. LEXIS 16305, 2003 WL 22145814, at *24 (D.N.J. Sept. 13, 2003)*; *Sandom v. Travelers Mtg. Servs., Inc., 752 F. Supp. 1240, 1244 (D.N.J. 1990)*. Because both of Plaintiff's NJLAD claims are retaliation claims, they fall within the CEPA waiver provision.

Accordingly, the motion for summary judgment on Counts 4 and 7 is **GRANTED.**

D. **[**34]** Count 5: Conscientious Employee Protection Act

In Count 5, Plaintiff asserts a CEPA claim, arguing that Defendants retaliated against her for reporting the Zimek pesticide issue. Defendants move for summary judgment. The Court finds that summary judgment should be granted on Count 5.

HN14[↑] To establish a *prima facie* case of retaliation under CEPA, a plaintiff must demonstrate: (1) a reasonable belief that the employer's conduct was violating either a law, rule, regulation or public policy; (2) she performed a "whistle blowing" activity as described in *N.J.S.A. 34:19-3(a)* or *(c)*; (3) an adverse employment action was taken against her; and (4) a causal connection existed between the whistle-blowing activity and the adverse employment action. *Dzwonar v. McDevitt, 177 N.J. 451, 462, 828 A.2d 893 (2003)*; *Klein v. Univ. of Med. & Dentistry of New Jersey, 377 N.J. Super. 28, 38, 871 A.2d 681 (App. Div. 2005)*; *Kolb v.*

Burns, 320 N.J. Super. 467, 476, [*673] 727 A.2d 525 (App. Div. 1999). In this case, Plaintiff demonstrated that she had a reasonable belief that MONOC's use of Zimek violated environmental regulations, and that she performed whistle blowing activity by reporting this issue to the EPA and NJDEP. However, Plaintiff failed to demonstrate **[**35]** the last two elements of her CEPA claim.

First, Plaintiff failed to demonstrate that an adverse employment action was taken against her. HN15[] CEPA defines "retaliatory action" as "the discharge, suspension or demotion of an employee, or other adverse employment action taken against an employee in the terms and conditions of employment." N.J.S.A. 34:19-2(e). Plaintiff asserts that, in retaliation for reporting the Zimek issue, Defendants disciplined her for infractions that she did not commit. The record reflects the exact opposite situation: that Defendants chose ***not*** to punish Plaintiff for the numerous infractions that she ***did*** commit. According to MONOC's progressive disciplinary policy, a MONOC employee who accrued eight disciplinary points would be suspended, and an employee with ten or more disciplinary points would be terminated. Ex. H at D8. The record reflects that Plaintiff accrued eight disciplinary points and was issued a notice of suspension, and then accrued a total of twelve disciplinary points and was issued a notice of termination. *See* Ex. H at D5-D10; Ex. I at PERS 230-32, 241, 243, 245, 273, 279, 282, 293, 295, 297, 308. However, in spite of Plaintiff's disciplinary record **[**36]** and MONOC's rigid disciplinary policy, MONOC management decided not to enforce the suspension or the termination, and instead allowed Plaintiff to continue working. Ex. I at PERS 230-32; Ex. L 103:515, 105:2-24. Because the evidence shows that MONOC bent over backwards ***not*** to discipline Plaintiff, Plaintiff cannot demonstrate that an adverse employment action was taken against her.

Second, Plaintiff failed to demonstrate that a causal connection existed between her whistle-blowing activity and any adverse employment action. HN16[] To prove causation, a plaintiff must show that "the retaliatory discrimination was more likely than not a determinative factor in the [adverse employment] decision." Donofry v. Autotote Sys., Inc., 350 N.J. Super. 276, 293, 795 A.2d 260 (App. Div. 2001). The evidence in this case demonstrates that Plaintiff was not terminated for whistle-blowing activity or even for disciplinary reasons; Plaintiff was terminated because she went out on medical leave and never returned to work. Plaintiff exhausted her twelve weeks of FMLA leave and a ninety-day personal leave of absence, and then informed MONOC that she would not be returning to work for several more months. To allow Plaintiff **[**37]** to take additional time off, MONOC sent Plaintiff reasonable accommodation forms twice, but Plaintiff never completed or returned the forms. Because Plaintiff did not return to work or fill out the reasonable accommodation forms, Plaintiff was terminated on February 7, 2012. Plaintiff had the right to appeal her termination, but she chose not to exercise that right. Thus, the facts in the case show that Plaintiff's termination had nothing to do with her whistle-blowing activity.

Accordingly, the motion for summary judgment on Count 5 is **GRANTED.**

E. Count 6: Invasion of Privacy

In Count 6, Plaintiff asserts a claim for common law invasion of privacy. Plaintiff's claim is premised on Defendants' alleged unauthorized "accessing of her private Facebook postings" regarding the museum shooting. Am. Compl. ¶ 78. Defendants argue that they are entitled to summary judgment on the privacy claim because Plaintiff's friend "freely chose to **[*674]** share the information" with Defendants. Mot. Summ. J. at 11. The Court finds that summary judgment should be granted on Count 6.

HN17[] A claim for invasion of privacy under New Jersey law will succeed if a plaintiff brings forth evidence showing that (1) there was an **[**38]** intentional intrusion "upon the solitude or seclusion of another or his private affairs," and that (2) this intrusion would highly offend the reasonable person. Bisbee v. John C. Conover Agency, Inc., 186 N.J. Super. 335, 339, 452 A.2d 689 (App. Div. 1982). Under the first prong, a defendant must commit an intrusive act. *See* Restatement (Second) of Torts § 652B (1977) ("The intrusion itself makes the defendant subject to liability"); O'Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989) (according to the Restatement, an actor must "commit [an] intrusive act" to be liable for invasion of privacy). "The converse of this principle is, however, of course, that there is no wrong where defendant did not actually delve into plaintiff's concerns." Bisbee, 186 N.J. Super at 340. Plaintiff faces a high burden in asserting a cause of action based on intrusion of seclusion. Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 316-17, 990 A.2d 650 (2010).

In this case, Plaintiff failed to show that there was an intentional intrusion by any of the Defendants. In the Amended Complaint, Plaintiff alleged that Defendants gained access to her Facebook page because a "member of upper management summoned a MONOC employee **[**39]** . . . into his office" and "threatened this employee into accessing his Facebook account." Am. Compl. ¶ 20. Now that discovery is complete, it is clear that there is no evidentiary support for these allegations. The evidence does not show that Defendants obtained access to Plaintiff's Facebook page by, say, logging into her account, logging into another employee's account, or asking another employee to log into Facebook. Instead, the evidence shows that Defendants were the passive recipients of information that they did not seek out or ask for. Plaintiff voluntarily gave information to her Facebook friend, and her Facebook friend voluntarily gave that information to someone else. *See* Ex. C 43:6-8, 44:23-45:1, 52:11-17, 53:4-8, 62:19-21, 87:18-88:1; Ex. E 47:9-49:6; Ex. H, D 425, D 619. This may have been a violation of trust, but it was not a violation of privacy.

Accordingly, the motion for summary judgment on Count 6 is **GRANTED.**

IV. CONCLUSION

For the reasons stated above, Defendants' motion for summary judgment is **GRANTED.** An appropriate order follows.

/s/ William J. Martini

WILLIAM J. MARTINI, U.S.D.J.

Date: August 20, 2013

[EDITOR'S NOTE: The following court-provided text does not appear at this cite in F. Supp. 2d.]

[*none] ORDER

THIS MATTER comes before the Court on Defendants' motion **[**40]** for summary judgment under *Federal Rule of Civil Procedure 56*; for the reasons set forth in the accompanying opinion; and for good cause appearing;

IT IS on this 20th day of August 2013, hereby,

ORDERED that Defendants' motion for summary judgment is **GRANTED**.

/s/ William J. Martini

WILLIAM J. MARTINI, U.S.D.J.

End of Document

Holmes v. Petrovich Development Co., LLC

Court of Appeal of California, Third Appellate District

January 13, 2011, Filed

C059133

Reporter
191 Cal. App. 4th 1047 *; 119 Cal. Rptr. 3d 878 **; 2011 Cal. App. LEXIS 33 ***; 111 Fair Empl. Prac. Cas. (BNA) 424

GINA M. HOLMES, Plaintiff and Appellant, v. PETROVICH DEVELOPMENT COMPANY, LLC, et al., Defendants and Respondents.

Prior History: **[***1]** APPEAL from a judgment of the Superior Court of Sacramento County, No. 05AS04356, Shelleyanne W. L. Chang, Judge.

Disposition: Affirmed.

Core Terms

e-mails, pregnancy, communications, privileged, company's, harassment, trial court, attorney-client, conditions, cause of action, defendants', privacy, computers, employees, monitored, forwarded, comments, messages, abusive, summary adjudication, maternity leave, retaliation, hostile, quit, pervasive, handbook, severe, hostile work environment, emotional distress, sexual harassment

Case Summary

Procedural Posture
In plaintiff employee's action against defendant employer, the Superior Court of Sacramento County, California, granted the employer's motion for summary adjudication with respect to claims for hostile work environment sexual harassment, retaliation, and constructive discharge, and a jury returned a verdict for the employer on claims for violation of the right to privacy and intentional infliction of emotional distress. The employee appealed.

Overview

The court of appeal held that summary adjudication was properly granted on the hostile work environment claim under *Gov. Code, § 12940*, based on an absence of evidence that the work environment was objectively offensive. Although coworkers asked about the employee's maternity leave, when she asked them to stop, they complied, and although the employer made some critical comments in e-mail about the stress of being a small business owner who had to accommodate maternity leave, he recognized the employee's legal rights and stated he would honor them. The court also found no merit in the employee's claim of attorney-client privilege. Her e-mails to her lawyer were not protected by privilege because they were not confidential communications within the meaning of *Evid. Code, § 952*, given that the employee used the employer's computer after being expressly advised that such e-mails were not private and were accessible by the employer. This form of communication was akin to consulting her attorney in one of the employer's conference rooms, in a loud voice, with the door open, yet expecting that the conversation overheard by the employer would be privileged.

Outcome
The court affirmed the judgment.

LexisNexis® Headnotes

Civil Procedure > ... > Summary Judgment > Entitlement as Matter of Law > General Overview

Civil Procedure > Appeals > Summary Judgment Review > Standards of Review

HN1[] **Summary Judgment, Entitlement as Matter of Law**

A motion for summary judgment shall be granted if all the papers submitted show that there is no triable issue

as to any material fact and that the moving party is entitled to judgment as a matter of law. Code Civ. Proc., § 437c, subd. (c). Legal questions are considered de novo on appeal. However, the court must presume the judgment is correct, and the appellant bears the burden of demonstrating error.

Labor & Employment
Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

Labor & Employment Law > ... > Sexual Harassment > Scope & Definitions > Sexual Harassment

Labor & Employment
Law > ... > Harassment > Sexual Harassment > Quid Pro Quo

HN2[] Sexual Harassment, Hostile Work Environment

The Fair Employment and Housing Act (FEHA) makes it an unlawful employment practice for an employer, because of sex, to harass an employee. Gov. Code, § 12940, subd. (j)(1). Under FEHA, harassment because of sex includes sexual harassment, gender harassment, and harassment based on pregnancy, childbirth, or related medical conditions. Gov. Code, § 12940, subd. (j)(4)(C). There are two theories upon which sexual harassment may be alleged: quid pro quo harassment, where a term of employment is conditioned upon submission to unwelcome sexual advances; and hostile work environment, where the harassment is sufficiently pervasive so as to alter the conditions of employment and create an abusive work environment.

Labor & Employment
Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN3[] Sexual Harassment, Hostile Work Environment

To prevail on a claim of hostile work environment sexual harassment, an employee must demonstrate that he or she was subjected to sexual advances, conduct, or comments that were (1) unwelcome, (2) because of sex, and (3) sufficiently severe or pervasive to alter the conditions of his or her employment and create an abusive work environment.

Labor & Employment
Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN4[] Sexual Harassment, Hostile Work Environment

Whether an environment is hostile or abusive can be determined only by looking at all the circumstances including the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance. Therefore, to establish liability in a Fair Employment and Housing Act hostile work environment sexual harassment case, a plaintiff employee must show he or she was subjected to sexual advances, conduct, or comments that were severe enough or sufficiently pervasive to alter the conditions of employment and create a hostile or abusive work environment. With respect to the pervasiveness of harassment, courts have held an employee generally cannot recover for harassment that is occasional, isolated, sporadic, or trivial; rather, the employee must show a concerted pattern of harassment of a repeated, routine, or a generalized nature.

Labor & Employment
Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN5[] Sexual Harassment, Hostile Work Environment

To be actionable, a sexually objectionable environment must be both objectively and subjectively offensive, one that a reasonable person would find hostile or abusive, and one that the victim in fact did perceive to be so. That means a plaintiff who subjectively perceives the workplace as hostile or abusive will not prevail under the Fair Employment and Housing Act, if a reasonable person in the plaintiff's position, considering all the circumstances, would not share the same perception. Likewise, a plaintiff who does not perceive the

workplace as hostile or abusive will not prevail, even if it objectively is so.

Labor & Employment Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN6 Sexual Harassment, Hostile Work Environment

The Fair Employment and Housing Act is not a civility code. There is no recovery for hostile work environment sexual harassment that is occasional, isolated, sporadic, or trivial. Rather, a plaintiff must show a concerted pattern of harassment that is repeated, routine, or generalized in nature.

Labor & Employment Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN7 Sexual Harassment, Hostile Work Environment

For purposes of a hostile work environment claim, harassment need not be pervasive if it is sufficiently severe enough to alter the conditions of employment.

Labor & Employment Law > Wrongful Termination > Constructive Discharge > General Overview

HN8 Wrongful Termination, Constructive Discharge

Constructive discharge occurs only when the employer coerces the employee's resignation, either by creating working conditions that are intolerable under an objective standard, or by failing to remedy objectively intolerable working conditions that actually are known to the employer. The conditions prompting resignation must be sufficiently extraordinary and egregious to overcome the normal motivation of a competent, diligent, and reasonable employee to remain on the job. The resignation must be coerced, not merely a rational option chosen by the employee.

Labor & Employment Law > Wrongful Termination > Constructive Discharge > General Overview

Labor & Employment Law > ... > Harassment > Sexual Harassment > Hostile Work Environment

HN9 Wrongful Termination, Constructive Discharge

Where a plaintiff fails to demonstrate the severe or pervasive harassment necessary to support a hostile work environment claim, it will be impossible for her to meet the higher standard of constructive discharge: conditions so intolerable that a reasonable person would leave the job.

Labor & Employment Law > ... > Retaliation > Elements > Adverse Employment Actions

HN10 Elements, Adverse Employment Actions

An adverse employment action, which is a critical component of a retaliation claim, requires a substantial adverse change in the terms and conditions of the plaintiff's employment. A mere offensive utterance or a pattern of social slights by either the employer or coemployees cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment for purposes of the Fair Employment and Housing Act. However, a series of alleged discriminatory acts must be considered collectively rather than individually in determining whether the overall employment action is adverse and, in the end, the determination of whether there was an adverse employment action is made on a case-by-case basis, in light of the objective evidence.

Labor & Employment Law > ... > Retaliation > Elements > Adverse Employment Actions

HN11 Elements, Adverse Employment Actions

Minor or relatively trivial adverse actions or conduct by employers or fellow employees that, from an objective perspective, are reasonably likely to do no more than anger or upset an employee cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment and are not actionable.

Civil Procedure > Appeals > Appellate Briefs

Civil Procedure > Appeals > Reviewability of Lower Court Decisions > Preservation for Review

HN12[] **Appeals, Appellate Briefs**

Points raised for the first time in a reply brief will ordinarily not be considered, because such consideration would deprive the respondent of an opportunity to counter the argument.

Evidence > Privileges > Attorney-Client Privilege > General Overview

HN13[] **Privileges, Attorney-Client Privilege**

See *Evid. Code, § 954*.

Evidence > Privileges > Attorney-Client Privilege > Elements

HN14[] **Attorney-Client Privilege, Elements**

See *Evid. Code, § 952*.

Evidence > Privileges > Attorney-Client Privilege > Scope

HN15[] **Privileges, Attorney-Client Privilege**

See *Evid. Code, § 917*.

Evidence > Privileges > Attorney-Client Privilege > Waiver

HN16[] **Attorney-Client Privilege, Waiver**

See *Evid. Code, § 912, subd. (a)*.

Evidence > Privileges > Attorney-Client Privilege > Scope

HN17[] **Privileges, Attorney-Client Privilege**

Although a communication between persons in an attorney-client relationship does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication, *Evid. Code, § 917, subd. (b)*, this does not mean that an electronic communication is privileged (1) when the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions. A communication under these circumstances is not a confidential communication between client and lawyer within the meaning of *Evid. Code, § 952*, because it is not transmitted by a means that, 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.

Civil Procedure > Appeals > Appellate Briefs

HN18[] **Appeals, Appellate Briefs**

It is an appellant's burden to establish error with reasoned argument and citations to authority. An appellant bears the burden of establishing prejudice by spelling out in his or her brief exactly how an alleged error caused a miscarriage of justice. Appellants may not attempt to rectify their omissions and oversights for the first time in their reply briefs.

Headnotes/Syllabus

Summary

CALIFORNIA OFFICIAL REPORTS SUMMARY

In an employee's action against her former employer, the trial court granted the employer's motion for summary adjudication with respect to causes of action for hostile work environment sexual harassment, retaliation, and constructive discharge, and a jury returned a verdict for the employer on claims for violation of the right to privacy and intentional infliction of emotional distress. (Superior Court of Sacramento County, No. 05AS04356, Shelleyanne W. L. Chang, Judge.)

The Court of Appeal affirmed the judgment, holding that summary adjudication was properly granted on the hostile work environment claim under Gov. Code, § 12940, based on an absence of evidence that the work environment was objectively offensive. During the two months the employee worked for the employer, there was no severe misconduct or pervasive pattern of harassment. Although coworkers asked about the employee's maternity leave, when she asked them to stop, they complied, and although the employer made some critical comments in e-mail about the stress of being a small business owner who had to accommodate a maternity leave, he recognized the employee's legal rights and stated he would honor them. The court also found no merit in the employee's remaining claims of error, all arising from an alleged violation of attorney-client privilege. The employee's e-mails to her lawyer were not protected by attorney-client privilege because they were not confidential communications within the meaning of Evid. Code, § 952, given that the employee used the employer's computer, after being expressly advised that such e-mails were not private and were accessible by the employer. This form of communication was akin to consulting her attorney in one of the employer's conference rooms, in a loud voice, with the door open, yet expecting that the conversation overheard by the employer would be privileged. (Opinion by Scotland, J.,* with Hull, Acting P. J., and Butz, J., concurring.) **[*1048]**

Headnotes

CALIFORNIA OFFICIAL REPORTS HEADNOTES

CA(1)[] **(1)**

Civil Rights § 3.2—Sexual Harassment—Employment.

The California Fair Employment and Housing Act (FEHA) (Gov. Code, § 12900 et seq.) makes it an unlawful employment practice for an employer, because of sex, to harass an employee (Gov. Code, § 12940, subd. (j)(1)). Under FEHA, harassment because of sex includes sexual harassment, gender harassment, and harassment based on pregnancy, childbirth, or related medical conditions (Gov. Code, § 12940, subd. (j)(4)(C)). There are two theories upon which sexual harassment may be alleged: quid pro quo harassment, where a term of employment is conditioned upon submission to unwelcome sexual advances; and hostile work environment, where the harassment is sufficiently pervasive so as to alter the conditions of employment and create an abusive work environment.

CA(2)[] **(2)**

Civil Rights § 3.2—Sexual Harassment—Hostile Work Environment—Elements.

To prevail on a claim of hostile work environment sexual harassment, an employee must demonstrate that he or she was subjected to sexual advances, conduct, or comments that were (1) unwelcome, (2) because of sex, and (3) sufficiently severe or pervasive to alter the conditions of his or her employment and create an abusive work environment. Whether an environment is hostile or abusive can be determined only by looking at all the circumstances including the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance. Therefore, to establish liability in a California Fair Employment and Housing Act (Gov. Code, § 12900 et seq.) hostile work environment sexual harassment case, a plaintiff employee must show he or she was subjected to sexual advances, conduct, or comments that were severe enough or sufficiently pervasive to alter the conditions of employment and create a hostile or abusive work environment. With respect to the pervasiveness of harassment, courts have held an employee generally cannot recover for harassment that is occasional, isolated, sporadic, or trivial; rather, the employee must show a concerted pattern of harassment of a repeated, routine, or a generalized nature.

CA(3)[] **(3)**

Civil Rights § 3.2—Sexual Harassment—Hostile Work

* Retired Presiding Justice of the Court of Appeal, Third Appellate District, assigned by the Chief Justice pursuant to article VI, section 6 of the California Constitution.

Environment—Objective and Subjective Offensiveness.

To be actionable, a sexually objectionable environment must be both objectively and subjectively offensive, one that a reasonable person would find hostile or abusive, and one that the victim in fact did perceive to be so. That means a plaintiff who subjectively perceives the workplace as hostile or abusive **[*1049]** will not prevail under the California Fair Employment and Housing Act (FEHA) (*Gov. Code, § 12900 et seq.*), if a reasonable person in the plaintiff's position, considering all the circumstances, would not share the same perception. Likewise, a plaintiff who does not perceive the workplace as hostile or abusive will not prevail, even if it objectively is so. FEHA is not a civility code. There is no recovery for hostile work environment sexual harassment that is occasional, isolated, sporadic, or trivial. Rather, a plaintiff must show a concerted pattern of harassment that is repeated, routine, or generalized in nature. The harassment need not be pervasive if it is sufficiently severe enough to alter the conditions of employment.

CA(4) **(4)**

Civil Rights § 3.2—Sexual Harassment—Hostile Work Environment—Constructive Discharge.

Constructive discharge occurs only when the employer coerces the employee's resignation, either by creating working conditions that are intolerable under an objective standard, or by failing to remedy objectively intolerable working conditions that actually are known to the employer. The conditions prompting resignation must be sufficiently extraordinary and egregious to overcome the normal motivation of a competent, diligent, and reasonable employee to remain on the job. The resignation must be coerced, not merely a rational option chosen by the employee. Where a plaintiff fails to demonstrate the severe or pervasive harassment necessary to support a hostile work environment claim, it will be impossible for her to meet the higher standard of constructive discharge: conditions so intolerable that a reasonable person would leave the job.

CA(5) **(5)**

Civil Rights § 3—Retaliation.

An adverse employment action, which is a critical component of a retaliation claim, requires a substantial adverse change in the terms and conditions of the plaintiff's employment. A mere offensive utterance or a pattern of social slights by either the employer or coemployees cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment for purposes of the California Fair Employment and Housing Act (*Gov. Code, § 12900 et seq.*). However, a series of alleged discriminatory acts must be considered collectively rather than individually in determining whether the overall employment action is adverse and, in the end, the determination of whether there was an adverse employment action is made on a case-by-case basis, in light of the objective evidence. Minor or relatively trivial adverse actions or conduct by employers or fellow employees that, from an objective perspective, are reasonably likely to do no more than anger or upset an employee cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment and are not actionable.

CA(6) **(6)**

Attorneys at Law § 10—Privilege—Electronic Communication—Confidentiality—Use of Defendant's Equipment.

Although a communication between persons in an attorney-client relationship does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication (*Evid. Code, § 917, subd. (b)*), this does not mean that an electronic communication is privileged when (1) the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions. A communication under these circumstances is not a confidential communication between client and lawyer within the meaning of *Evid. Code, § 952*, because it is not transmitted by a means that, 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.

CA(7) **(7)**

Attorneys at Law § 10—Privilege—Electronic Communication—Confidentiality—Use of Defendant's Equipment—Employer.

In a hostile work environment case, the employee's e-

mails to her lawyer were not protected by attorney-client privilege because they were not confidential communications within the meaning of under *Evid. Code, § 952*. The employee used the employer's computer, after being expressly advised such e-mails were not private and were accessible by the employer, the very person about whom the employee contacted her lawyer. This was akin to consulting her attorney in one of the employer's conference rooms, in a loud voice, with the door open, yet expecting that the conversation overheard by the employer would be privileged.

[*Levy et al., Cal. Torts (2010) ch. 72, § 72.21*; 8 Witkin, Summary of Cal. Law (10th ed. 2005) Constitutional Law, § 926; 2 Witkin, Cal. Evidence (4th ed. 2000) Witnesses, § 85.]

Counsel: Law Offices of Joanna R. Mendoza and Joanna R. Mendoza for Plaintiff and Appellant.

Perkins & Associates and Robin K. Perkins for Defendants and Respondents.

Judges: Opinion by Scotland, J., with Hull, Acting P. J., and Butz, J., concurring.

Opinion by: Scotland **[*1051]**

Opinion

[882]** **SCOTLAND, J.**[*]—Plaintiff Gina M. Holmes appeals from the judgment entered in favor of defendants Petrovich Development Company, LLC, and Paul Petrovich in her lawsuit for sexual harassment, retaliation, wrongful termination, violation of the right to privacy, and intentional infliction of emotional distress. [1] She contends that the trial court erred in granting defendants' motion for summary adjudication with respect to the causes of action for discrimination, retaliation, and wrongful termination, and that the jury's verdict as to the remaining causes of action must be reversed due to evidentiary and instructional errors. We disagree and shall affirm the judgment.

[*] Retired Presiding Justice of the Court of Appeal, Third Appellate District, assigned by the Chief Justice pursuant to *article VI, section 6 of the California Constitution*.

[1] Hereafter, we **[***2]** will refer to Petrovich Development Company, LLC, as the company, to Paul Petrovich as Petrovich, and to them collectively as defendants.

Among other things, we conclude that e-mails sent by Holmes to her attorney regarding possible legal action against defendants did not constitute " 'confidential communication between client and lawyer' " within the meaning of *Evidence Code section 952*. **[**883]** This is so because Holmes 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."

As we will explain, an attorney-client communication "does not lose its privileged character for the sole reason that it is communicated by electronic **[***3]** means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication." (*Evid. Code, § 917, subd. (b)*.) However, the e-mails sent via company computer under the circumstances of this case were akin to 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. By using the company's computer to communicate with her lawyer, knowing the communications violated company computer policy and could be discovered by her employer due to company monitoring of e-mail usage, Holmes did not communicate "in confidence by a means which, so far as the client is aware, **[*1052]** 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." (*Evid. Code, § 952*.) Consequently, the communications were not privileged.

FACTS

Holmes began **[***4]** working for Petrovich as his executive assistant in early June 2004.

The employee handbook, which Holmes admitted reading and signing, contained provisions clearly spelling out the policy concerning use of the company's

technology resources, such as computers and e-mail accounts. The handbook directs employees that the company's technology resources should be used only for company business and that employees are prohibited from sending or receiving personal e-mails. Moreover, the handbook warns that "[e]mployees who use the Company's Technology Resources to create or maintain personal information or messages have no right of privacy with respect to that information or message." The "Internet and Intranet Usage" policy in the handbook specifically states, "E-mail is not private communication, because others may be able to read or access the message. E-mail may best be regarded as a postcard rather than as a sealed letter. …" The handbook spells out further that the company may "inspect all files or messages … at any time for any reason at its discretion" and that it would periodically monitor its technology resources for compliance with the company's policy.

The handbook also **[***5]** set forth the company's policy regarding harassment and discrimination. It directs an employee who thinks that he or she has been subjected to harassment or discrimination to immediately report it to Petrovich or Cheryl Petrovich, who was the company's secretary and handled some human resources functions. If the complaining party is not comfortable **[**884]** reporting the conduct to them, the report should be made to the company's controller. The policy promises that the complaint will be taken seriously, it will be investigated thoroughly, and there will be no retaliation. The policy also urges the employee, when possible, to confront the person who is engaging in the unwanted conduct and ask the person to stop it.

The next month, July of 2004, Holmes told Petrovich that she was pregnant and that her due date was December 7, 2004. Petrovich recalled that Holmes told him she planned to work up until her due date and then would be out on maternity leave for six weeks.
[*1053]

Holmes did not like it when coworkers asked her questions about maternity leave; she thought such comments were inappropriate. She asked "[t]hat little group of hens" to stop, and they complied. Holmes recalled having about six conversations **[***6]** with Petrovich about her pregnancy, during which they discussed her belly getting big and baby names. She thought "belly-monitoring" comments were inappropriate, but never told Petrovich that he was being offensive.

On Friday morning, August 6, 2004, Petrovich sent Holmes an e-mail discussing various topics, including that they needed to determine how they were going to handle getting a qualified person to help in the office who would be up to speed while Holmes was on maternity leave. He explained that, given his schedule and pace, this would not be a simple task. Thus, they needed to coordinate the transition so neither he nor Holmes would be stressed about it before or after Holmes left on maternity leave. Petrovich stated: "My recollection from the email you sent me when you told me you were pregnant and in our subsequent conversations, you are due around December 7th and will be out six weeks. We are usually swamped between now and the third week of December. The good news is between the third week of December to the second week of January, it slows down a little."

Holmes e-mailed Petrovich a few hours later and advised him that she estimated starting her maternity leave around **[***7]** November 15, and that the time estimate of six weeks might not be accurate as she could be out for the maximum time allowed by the employee handbook and California law, which is four months. She did not expect to be gone for the full four months but thought she should mention it as a possibility. Holmes believed that "Leslie" was "capable of picking up most of the slack" while Holmes was gone, and that the company could hire a "temp just to cover some of the receptionist duties so that Leslie could be more available … ."

A short time later, Petrovich responded, "I need some honesty. How pregnant were you when you interviewed with me and what happened to six weeks? Leslie is not and cannot cover your position, nor can a temp. That is an extreme hardship on me, my business and everybody else in the company. You have rights for sure and I am not going to do anything to violate any laws, but I feel taken advantage of and deceived for sure."

Holmes replied that she thought the subject was better handled in person, "but here it goes anyway. [¶] I find it offensive that you feel I was dishonest or deceitful. I wrote a very detailed email explaining my pregnancy as soon as the tests from **[***8]** my amniocentesis came back that everything was 'normal' with the baby. An amnio cannot be performed until you are nearly 4 months pregnant, hence the delay in knowing the results. I am 39 years old, and **[*1054]** therefore, there was a chance that there could be something 'wrong' or 'abnormal' with the baby. If there had been, I had decided not to carry the baby to **[**885]** term. That is a

very personal choice, and not something that I wanted to have to share with people at work; so in order to avoid that, I waited until I knew that everything was o.k. before telling anyone I was pregnant. [¶] I've also had 2 miscarriages at 3 months into my pregnancy, and could not bear having to share that with co-workers again, as I have in the past. [¶] These are very important and personal decisions that I made. I feel that I have the right to make these decisions, and there is no deceipt [*sic*] or dishonesty involved with this. On a more professional level; there is no requirement in a job interview or application to divulge if you are pregnant or not; in fact, I believe it's considered unethical to even inquire as to such. [¶] At this point, I feel that your words have put us in a bad position where our working **[***9]** relationship is concerned, and I don't know if we can get past it. [¶] As long as we're being straightforward with each other, please just tell me if what you are wanting at this time, is for me to not be here anymore, because that is how it feels. [¶] I need to go home and gather my thoughts."

Because he was concerned that Holmes might be quitting, Petrovich forwarded their e-mail exchange to Cheryl Petrovich; Lisa Montagnino, who handled some human resources functions; in-house counsel Bruce Stewart; and Jennifer Myers, who handled payroll and maintained employee files.

Petrovich also e-mailed Holmes as follows: "All I ever want is for people to be honest with me. The decision is all yours as to whether you stay here. I am NOT asking for your resignation. I do have the right to express my feelings, so I can't help it if you feel offended if the dates and amount of time you told me you would be out on maternity leave no longer apply. I also never asked you about you [being] pregnant in our interview, so you mentioning unethical behavior is out of place. I think you are missing the whole point here. I am trying to keep my business organized and I was working off information you told **[***10]** me. When you disclosed, only upon me asking, that what you told me is incorrect and that you had already decided on a maternity leave date without ever informing me, I [have] the right to question [the] information and not be subject to being quoted California law or my own handbook. You obviously are well versed on all of this which speaks volumes. No, you are not fired. Yes, you are required to be straight with your employer. If you do not wish to remain employed here, I need to know immediately."

On Monday morning, August 9, 2004, Holmes sent an e-mail to Petrovich, who was vacationing in Montana. She explained that she had thought about things a lot over the weekend and felt that what occurred on Friday could have been avoided if they had communicated in person. She enjoyed her **[*1055]** employment and took it as a compliment that Petrovich was worried about filling her shoes in her absence. Holmes stated, "I may only be gone 6 weeks, but I don't want to commit to that, because unforeseen circumstances can happen making my absence continue slightly longer. The max is 4 months, and that is only if there are disability issues; which I don't anticipate in my case, but I wanted to give you the **[***11]** 'outside' number, so you wouldn't be left with any surprises. [¶] I am happy about my pregnancy and happy about my job; I'd like to feel good about continuing to work here, in a positive and supportive environment up until my maternity leave in November, and I would like to return shortly thereafter. [¶] If we are on the same page, please let me know. I will do whatever I can to accommodate you while I'm gone; I can work from home, or come in a few hours a **[**886]** day; I am very flexible and hope that we will be able to work out the bumps along the way."

Petrovich replied that he agreed with Holmes's e-mail and saw things the way that she did. He stated, "I agree we do need to communicate. I need [to] admit I was in shock when you told me you were pregnant so soon after you started work. Right or wrong, I felt entrapped. It's a 'no win' for an employer. Yes, I am happy for you, but it was building in me and I decide[d] to approach it by asking if your plans were still as represented. When everything got moved up, I felt even worse. I know I have no right to feel this way by law or as an employer, but I am human in a tough business where people are constantly trying to take advantage of me. **[***12]** Remember what I said about loyalty in our interview? The person closest to me in the office has been the person in your position. When this happened, it greatly upset me since I was hoping for the very best foundation for us since I have been pleased with your efforts and because it had been a while since I have found someone committed to do what is a tough job. It will take some time for me to 'get over it' but I will and I want you to stay. It will work."

Early the next morning, August 10, 2004, Holmes replied, "Thank you Paul. I understand your feelings, you understand mine; let's move forward in a positive direction, and remember, 'this too shall pass'." She then discussed some business matters, said that everyone was thinking of Petrovich and his family, and stated that "Norman and Oliver say meow and woof!"

At some point after she e-mailed Petrovich, Holmes learned that Petrovich had forwarded their e-mails regarding her pregnancy to Cheryl Petrovich, Bruce Stewart, Lisa Montagnino, and Jennifer Myers. Although she never asked Petrovich not to forward the e-mails to others, and she conceded the e-mails did not contain any language communicating that the information was to be kept **[***13]** private, Holmes was very upset because she "thought that it went without saying" the e-mails should not be disseminated to others.
[*1056]

On August 10, 2004, Holmes saw her doctor for routine obstetric care and complained about being harassed at work regarding her upcoming pregnancy disability leave. According to the doctor, Holmes was "moderately upset" and "somewhat tearful." He advised her that the best course of action would be to discuss the matter directly with her boss about how she feels and remedy the situation. If the harassment continued, then she might benefit from the assistance of a lawyer.

At 3:30 p.m. on the same day that Holmes saw her doctor and had e-mailed Petrovich that they could move forward in a positive direction, Holmes used the company computer to e-mail an attorney, Joanna Mendoza. Holmes asked for a referral to an attorney specializing in labor law, specifically relating to pregnancy discrimination. When Mendoza asked what was going on, Holmes replied that her boss was making it unbearable for her. He said things that were upsetting and hurtful, and had forwarded personal e-mail about her pregnancy to others in the office. Holmes stated, "I know that there are laws that **[***14]** protect pregnant women from being treated differently due to their pregnancy, and now that I am officially working in a hostile environment, I feel I need to find out what rights, if any, and what options I have. I don't want to quit my job; but how do I make the situation better." Holmes explained that her boss had accused her of being dishonest because she underestimated her maternity leave, that he had forwarded a personal e-mail and **[**887]** made it "common reading material for employees," and that he had made her feel like an "outcast." Holmes forwarded to Mendoza a few of Petrovich's e-mails.

At 4:42 p.m. on the same day, Mendoza e-mailed Holmes that she should delete their attorney-client communications from her work computer because her employer might claim a right to access it. Mendoza suggested they needed to talk and, while they could talk on the phone, she "would love an excuse to see [Holmes] and catch up on everything." Mendoza stated they could meet for lunch the next day. Holmes agreed and said she would come to Mendoza's law office, at which time Mendoza could see her "big belly."

On the evening of August 11, 2004, after her lunch with Mendoza, Holmes e-mailed Petrovich saying **[***15]** that Holmes had been upset since his first e-mail on Friday. She had been in tears, her stomach was in knots, and she realized that they would be unable "to put this issue behind us." She stated, "I think you will understand that your feelings about my pregnancy; which you have made more than clear, leave me no alternative but to end my employment here." Holmes advised Petrovich that she had cleared her things from her desk and would not be returning to work. Holmes also e-mailed Jennifer Myers stating that she was quitting and advising her where to send the final paycheck.
[*1057]

In September of 2005, Holmes filed a lawsuit against defendants, asserting causes of action for sexual harassment, retaliation, wrongful termination in violation of public policy, violation of the right to privacy, and intentional infliction of emotional distress. She alleged that the negative comments in Petrovich's e-mails and his dissemination of her e-mails, which contained highly personal information, invaded her privacy, were intended to cause her great emotional distress, and caused her to quit her job to avoid the abusive and hostile work environment created by her employer. According to Holmes, Petrovich **[***16]** disseminated the e-mails to retaliate against her for inconveniencing him with her pregnancy and to cause her to quit. Holmes claimed she was constructively terminated in that continuing her employment with Petrovich "became untenable, as it would have been for any reasonable pregnant woman."

On November 17, 2006, defendants filed a motion for summary judgment or summary adjudication on the ground that, as a matter of law, Holmes could not establish any of her causes of action. Defendants argued Holmes could not establish (1) that there was an objectively or subjectively hostile work environment; (2) that she suffered an adverse employment action in retaliation for her pregnancy; (3) that she suffered an adverse employment action that would cause a reasonable person to quit; (4) that Holmes had a reasonable expectation of privacy in her e-mails; or (5) that Petrovich's conduct was extreme and outrageous.

The trial court granted the motion for summary adjudication as to three of the causes of action. The

court ruled that, although there was evidence that Holmes subjectively perceived her workplace as hostile or abusive, there must also be evidence that the work environment was objectively **[***17]** offensive. "The undisputed brief, isolated, work-related exchanges between her and Mr. Petrovich, and others in the office, could not be objectively found to have been severe enough or sufficiently pervasive to alter the conditions of her employment and create a hostile or abusive work environment based upon her pregnancy." As for Holmes's claims for retaliation and constructive discharge, there was no evidence she experienced an adverse employment action, and no evidence **[**888]** from which a reasonable trier of fact could find that Petrovich "intentionally created or knowingly permitted working conditions that were so intolerable or aggravated at the time of [Holmes's] resignation that a reasonable employer would realize that a reasonable person in [her] position would be compelled to resign."

The trial court denied the motion for summary adjudication as to the causes of action for invasion of privacy and intentional infliction of emotional distress. The court ruled that, despite Holmes's use of e-mail to communicate private information to Petrovich, and despite the company's policy regarding **[*1058]** the nonprivate nature of electronic communications, triable issues of fact remained regarding whether **[***18]** Petrovich's dissemination of the information to other people in the office breached Holmes's right to privacy or whether the disclosure was privileged, and that issues of fact remained concerning whether the disclosure was egregious and outrageous.

The trial of those two causes of action resulted in a defense verdict.

DISCUSSION

I

Holmes contends the trial court erred in granting defendants' motion for summary adjudication on her causes of action for sexual harassment, retaliation, and constructive discharge.

HN1[↑] A motion for summary judgment "shall be granted if all the papers submitted show that there is no triable issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." (*Code Civ. Proc., § 437c, subd. (c)*.) Legal questions are considered de novo on appeal. (*Unisys Corp. v. California Life & Health Ins. Guarantee Assn. (1998) 63 Cal.App.4th 634, 637 [74 Cal. Rptr. 2d 106]*.) However, we must presume the judgment is correct, and the appellant bears the burden of demonstrating error. (*Howard v. Thrifty Drug & Discount Stores (1995) 10 Cal.4th 424, 443 [41 Cal. Rptr. 2d 362, 895 P.2d 469]*.)

Viewing Holmes's specific contentions within the context of the appropriate legal framework, we find no error.

A

First, Holmes **[***19]** contends the trial court erred in granting summary adjudication with respect to her cause of action for sexual harassment.

CA(1)[↑] (1) *HN2*[↑] The California Fair Employment and Housing Act (FEHA) (*Gov. Code, § 12900 et seq.*) makes it an unlawful employment practice for an employer, "because of … sex, … to harass an employee." (*Gov. Code, § 12940, subd. (j)(1)*.) Under FEHA, " 'harassment' because of sex includes sexual harassment, gender harassment, and harassment based on pregnancy, childbirth, or related medical conditions." (*Gov. Code, § 12940, subd. (j)(4)(C)*.)

There are two theories upon which sexual harassment may be alleged: quid pro quo harassment, where a term of employment is conditioned upon **[*1059]** submission to unwelcome sexual advances, and hostile work environment, where the harassment is sufficiently pervasive so as to alter the conditions of employment and create an abusive work environment. (*Mogilefsky v. Superior Court (1993) 20 Cal.App.4th 1409, 1414 [26 Cal. Rptr. 2d 116]*.) Holmes pursued the latter.

CA(2)[↑] (2) *HN3*[↑] To prevail on a claim of hostile work environment sexual harassment, an employee must demonstrate that he or she was subjected to sexual advances, conduct, or comments that were (1) unwelcome, (2) because of sex, and (3) sufficiently severe or pervasive **[***20]** to alter the conditions of his **[**889]** or her employment and create an abusive work environment. (*Lyle v. Warner Brothers Television Productions (2006) 38 Cal.4th 264, 279 [42 Cal. Rptr. 3d 2, 132 P.3d 211]* (hereafter *Lyle*).)

HN4[↑] " ' "[W]hether an environment is 'hostile' or 'abusive' can be determined only by looking at all the circumstances [including] the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance." [Citation.]' [Citation.] Therefore, to establish liability in a FEHA hostile work environment sexual harassment case, a plaintiff

employee must show she was subjected to sexual advances, conduct, or comments that were *severe enough or sufficiently pervasive to alter the conditions of her employment and create a hostile or abusive work environment*." (Lyle, supra, 38 Cal.4th at p. 283, original italics.) "With respect to the pervasiveness of harassment, courts have held an employee generally cannot recover for harassment that is occasional, isolated, sporadic, or trivial; rather, the employee must show a concerted pattern of harassment of a repeated, routine, or a generalized **[***21]** nature." (*Ibid*.)

CA(3)[↑] (3) "HN5[↑] To be actionable, 'a sexually objectionable environment must be both objectively and subjectively offensive, one that a reasonable person would find hostile or abusive, and one that the victim in fact did perceive to be so.' [Citations.] *That means a plaintiff who subjectively perceives the workplace as hostile or abusive will not prevail under the FEHA, if a reasonable person in the plaintiff's position, considering all the circumstances, would not share the same perception*. Likewise, a plaintiff who does not perceive the workplace as hostile or abusive will not prevail, even if it objectively is so." (Lyle, supra, 38 Cal.4th at p. 284, italics added.)

Relying on *Lyle*, the trial court found that, although Holmes subjectively perceived her workplace as hostile, it was not an abusive environment from an objective standpoint as a matter of law. Holmes claims the trial court erred in relying on *Lyle* because the facts in that case are distinguishable. But the trial court did not grant Petrovich's motion based on a factual comparison to ***[*1060]*** *Lyle*; it simply used the standard of review established therein as it was required to do, and as are we, under principles of stare decisis. **[***22]** (Auto Equity Sales, Inc. v. Superior Court (1962) 57 Cal.2d 450, 455 [20 Cal. Rptr. 321, 369 P.2d 937].)

Holmes contends the proper standard in sexual harassment cases is whether a reasonable woman would consider the work environment a hostile one and, hence, the standard in pregnancy discrimination cases should be whether a reasonable pregnant woman would consider her work environment hostile. Thus, Holmes asserts, "Unless there was undisputed evidence that [she] was an *unreasonable* pregnant woman, it is oxymoronic that the lower court found the conduct at issue subjectively offensive but not 'objectively' offensive to a reasonable pregnant woman in [her] position. … Quite frankly, the issue of 'objectively offensive conduct' should have been left to the trier of fact and not been a question of law for the judge to have decided, especially if it was clear that there was subjective offense and highly questionable conduct at issue." (Original italics.)

Holmes's argument is not persuasive. An evaluation of all the circumstances surrounding Holmes's employment discloses an absence of evidence from which a reasonable jury could objectively **[**890]** find that Petrovich created a hostile work environment for a reasonable **[***23]** pregnant woman. During the two months Holmes worked for Petrovich, there was no severe misconduct or pervasive pattern of harassment. Holmes claims that her coworkers treated her differently based upon her pregnancy by asking about her maternity leave, but she admits that, when she asked them to stop, they complied.

Holmes points to the e-mails she exchanged with Petrovich on August 6 and 9, 2004, in which he implied she had deceived him about her pregnancy, stated he was offended that she had changed the period of time she would be absent for maternity leave, and asserted that her pregnancy was an extreme hardship on his business. She also complains that Petrovich unnecessarily forwarded to others her e-mail containing personal information about her age, prior miscarriages, and the possibility she would have terminated her pregnancy if the amniocentesis results had revealed problems with the fetus. Holmes asserts that Petrovich did this to humiliate her. Petrovich said he sent the e-mails to in-house counsel and employees involved in human relations because he thought that Holmes was about to quit.

When viewed in context, the e-mails (set forth at length, *ante*) show nothing more than **[***24]** that Petrovich made some critical comments due to the stress of being a small business owner who must accommodate a pregnant woman's right to maternity leave. He recognized Holmes's legal rights, stated he would honor them, said he was not asking for her resignation, noted he **[*1061]** had been pleased with her work, and simply expressed his feelings as a "human in a tough business where people are constantly trying to take advantage of me." He assured Holmes that "it will work." Rather than giving him a chance to honor his promise, Holmes quit.

It appears Holmes expects FEHA to be a civility code. HN6[↑] It is not. (Lyle, supra, 38 Cal.4th at p. 295.) As we stated above, there is no recovery for harassment that is occasional, isolated, sporadic, or trivial. (Id. at p. 283.) Rather, a plaintiff must show a concerted pattern of harassment that is repeated, routine, or generalized

in nature. (*Mokler v. County of Orange (2007) 157 Cal.App.4th 121, 142 [68 Cal. Rptr. 3d 568]*.) Holmes failed to do so. The isolated incidents to which she points are objectively insufficient.

Holmes relies on three cases for the proposition that harassment need not be pervasive and may be established by only a few instances of conduct over a short **[***25]** period of time. She fails to recognize that ***HN7***[⬆] harassment need not be pervasive *if it is sufficiently severe* enough to alter the conditions of employment. (*Lyle, supra, 38 Cal.4th at p. 283* [the plaintiff must be subjected to conduct or comments severe enough *or* sufficiently pervasive to alter the conditions of her employment and create a hostile work environment].) The cases upon which Holmes relies are not remotely similar to her situation in that they all involve egregious and severe conduct that unquestionably was abusive. In *Hostetler v. Quality Dining, Inc. (7th Cir. 2000) 218 F.3d 798*, the plaintiff's harasser engaged in three incidents over a one-week period of time: (1) he forced his tongue into her mouth, (2) he attempted to kiss her again and to remove her bra, and (3) he told her that he could perform oral sex so effectively he could make her do cartwheels. (*Id. at pp. 802, 807–808*.) In *Erdmann v. Tranquility Inc. (N.D.Cal. 2001) 155 F.Supp.2d 1152*, a homosexual employee's boss insisted that the employee become heterosexual, convert to the employer's **[**891]** Mormon faith, and lead the company's prayer service. (*Id. at pp. 1160–1161*.) And in *Mayfield v. Trevors Store, Inc.* (N.D.Cal., **[***26]** Dec. 6, 2004, No. C-04-1483 MHP) 2004 WL 2806175, the employer not only made comments that made the plaintiff feel stigmatized due to her pregnancy, the employer also wrote negative performance evaluations, assigned the plaintiff large amounts of extra work, and denied her a sick day.

Petrovich did not engage in any similarly egregious conduct, and he provided a nondiscriminatory explanation for his conduct. Because Holmes produced no evidence from which a reasonable jury could infer the existence of a hostile work environment, the trial court correctly granted the motion for summary adjudication on this cause of action.
[*1062]

B

Next, Holmes contends the court erred in granting the motion for summary adjudication on her cause of action for constructive discharge. According to Holmes, she "found the extreme stress associated with being out of work to be preferable to the treatment she was receiving at Petrovich." This claim fares no better than her last.

CA(4)[⬆] (4) "***HN8***[⬆] Constructive discharge occurs only when the employer coerces the employee's resignation, either by creating working conditions that are intolerable under an objective standard, or by failing to remedy objectively intolerable working conditions **[***27]** that actually are known to the employer." (*Mullins v. Rockwell Internat. Corp. (1997) 15 Cal.4th 731, 737 [63 Cal. Rptr. 2d 636, 936 P.2d 1246]*.) The conditions prompting resignation must be "sufficiently extraordinary and egregious to overcome the normal motivation of a competent, diligent, and reasonable employee to remain on the job." (*Turner v. Anheuser-Busch, Inc. (1994) 7 Cal.4th 1238, 1246 [32 Cal. Rptr. 2d 223, 876 P.2d 1022],* disapproved on other grounds in *Romano v. Rockwell Internat., Inc. (1996) 14 Cal.4th 479 [59 Cal. Rptr. 2d 20, 926 P.2d 1114]*.) The resignation must be coerced, not merely a rational option chosen by the employee. (*Turner, at p. 1247*.)

From an objective standpoint, the trial court correctly granted summary adjudication. ***HN9***[⬆] "Where a plaintiff fails to demonstrate the severe or pervasive harassment necessary to support a hostile work environment claim, it will be impossible for her to meet the higher standard of constructive discharge: conditions so intolerable that a reasonable person would leave the job." (*Brooks v. City of San Mateo (9th Cir. 2000) 229 F.3d 917, 930*.) As discussed above, Holmes failed to present sufficient evidence of a hostile work environment. Thus, her wrongful termination claim necessarily fails. (*Jones v. Department of Corrections & Rehabilitation (2007) 152 Cal.App.4th 1367, 1381 [62 Cal. Rptr. 3d 200]* **[***28]** (hereafter *Jones*).)

C

The trial court also granted summary adjudication on Holmes's cause of action for retaliation, ruling there was no evidence of an adverse employment action by Petrovich. We agree.

Holmes argues that she was subjected to negative comments and accusations about her pregnancy, followed by Petrovich's retaliatory conduct when she told him she planned to exercise her leave rights—he retaliated by forwarding her sensitive personal information to others in the office, who had **[*1063]** no reason to know about her prior miscarriages, amniocentesis, and potential termination of her pregnancy.

[892]** This is insufficient to establish an adverse

employment action by Petrovich.

CA(5)[↑] (5) HN10[↑] An " 'adverse employment action,' " which is a critical component of a retaliation claim (*Jones, supra, 152 Cal.App.4th at p. 1380*), requires a "substantial adverse change in the terms and conditions of the plaintiff's employment" (*Akers v. County of San Diego (2002) 95 Cal.App.4th 1441, 1454, 1455 [116 Cal. Rptr. 2d 602]*). "[A] mere offensive utterance or … a pattern of social slights by either the employer or coemployees cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment for purposes of [the **[***29]** FEHA] … ." (*Yanowitz v. L'Oreal USA, Inc. (2005) 36 Cal.4th 1028, 1054 [32 Cal. Rptr. 3d 436, 116 P.3d 1123]* (hereafter *Yanowitz*).) "However, a series of alleged discriminatory acts must be considered collectively rather than individually in determining whether the overall employment action is adverse [citations] and, in the end, the determination of whether there was an adverse employment action is made on a case-by-case basis, in light of the objective evidence." (*Jones, supra, 152 Cal.App.4th at p. 1381*.)

Here, Petrovich did not reduce Holmes's salary, benefits or work hours, and did not terminate her. He assured Holmes that she still had a job and that they would work things out. Holmes chose to quit because Petrovich expressed his concerns about the changes in her pregnancy leave dates and the need to replace her while she was on leave, and because he forwarded an e-mail that she wished to keep private. But she failed to demonstrate there was a triable issue of fact concerning whether he did these things to retaliate against her; she simply concluded that this was his motivation by taking out of context certain comments that he made. Holmes overlooks her own evidence, submitted in opposition to defendants' motion, **[***30]** which demonstrated that Petrovich forwarded the e-mail only to people he believed needed to know that Holmes had changed the anticipated date of her pregnancy leave and that she might be quitting. The fact that he forwarded her entire e-mail, rather than editing it or drafting a new one, does not demonstrate any animus toward her, given there was no clear directive in her e-mail that she did not wish others to see it.

More importantly, "[m]inor HN11[↑] or relatively trivial adverse actions or conduct by employers or fellow employees that, from an objective perspective, are reasonably likely to do no more than anger or upset an employee cannot properly be viewed as materially affecting the terms, conditions, or privileges of employment and are not actionable … ." (*Yanowitz, supra, 36 Cal.4th at p. 1054*.) That is what occurred here. A reasonable person would have talked **[*1064]** to Petrovich, expressed dismay at his actions, given him an opportunity to explain or apologize, and waited to see if conditions changed after the air had cleared. Instead, Holmes chose to quit despite Petrovich's assurances that he wanted her to stay and that things would work out.

For the reasons stated above, the trial court **[***31]** correctly granted defendants' motion for summary adjudication. [2]

[893]** II

Holmes's remaining claims of error all arise from an alleged violation of her attorney-client privilege.

She contends the trial court abused its discretion in (1) denying her motion **[***32]** demanding the return of privileged documents, (2) permitting the introduction of the documents at trial, and (3) giving a limiting instruction that undermined her cause of action for invasion of privacy. She argues that the cumulative prejudicial effect of these errors requires reversal of the judgment.

Her arguments are premised on various statutes governing the attorney-client privilege as follows:

Evidence Code section 954 states in relevant part: HN13[↑] "Subject to Section 912 and except as otherwise provided in this article, the client, whether or not a party, has a privilege to refuse to disclose, and to

---

[2] In her reply brief, Holmes says the court should have denied the motion for summary adjudication in its entirety because it was not timely served. This argument is forfeited because it is raised for the first time in her reply brief without a showing of good cause. (*Garcia v. McCutchen (1997) 16 Cal.4th 469, 482, fn. 10 [66 Cal. Rptr. 2d 319, 940 P.2d 906]*; *Reichardt v. Hoffman (1997) 52 Cal.App.4th 754, 764–765 [60 Cal. Rptr. 2d 770]*.) HN12[↑] "Points raised for the first time in a reply brief will ordinarily not be considered, because such consideration would deprive the respondent of an opportunity to counter the argument." (*American Drug Stores, Inc. v. Stroh (1992) 10 Cal.App.4th 1446, 1453 [13 Cal. Rptr. 2d 432]*; see *Reichardt v. Hoffman, supra, 52 Cal.App.4th at pp. 764–765*.) In any event, in overruling Holmes's objection to the defect in service, the court did not err in ruling Holmes waived the defect by filing an opposition and appearing at the hearing on the motion. (*Carlton v. Quint (2000) 77 Cal.App.4th 690, 696–698 [91 Cal. Rptr. 2d 844]*.)

prevent another from disclosing, a confidential communication between client and lawyer … .” (Further section references are to the Evidence Code unless otherwise specified.)

Section 952 provides that a HN14[↑] “confidential communication between client and lawyer” is “information transmitted between a client and his or her lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons **[*1065]** other than those who are present to further the interest of the client in the consultation or those to whom disclosure **[***33]** is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted … .” (§ 952.)

Section 917 states in relevant part: HN15[↑] “(a) If a privilege is claimed on the ground that the matter sought to be disclosed is a communication made in confidence in the course of the lawyer-client … relationship, the communication is presumed to have been made in confidence and the opponent of the claim of privilege has the burden of proof to establish that the communication was not confidential. [¶] (b) A communication … does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication. …”

Section 912, subdivision (a) provides that the right of any person to claim a lawyer-client privilege HN16[↑] “is waived with respect to a communication protected by the privilege if any holder of the privilege, without coercion, has disclosed a significant part of the communication or has consented to disclosure made by anyone. Consent to disclosure is manifested **[***34]** by any statement or other conduct of the holder of the privilege indicating consent to the disclosure, including failure to claim the privilege in any proceeding in which the holder has the legal standing and opportunity to claim the privilege.”

With this statutory framework in mind, we turn to Holmes's specific contentions.

A

Holmes argues the trial court erred in denying her motion for discovery sanctions, **[**894]** seeking return of the e-mails that she sent her attorney, Joanna Mendoza, using the company's computer. We disagree.

During a deposition, defense counsel questioned Holmes about her e-mail correspondence with her attorney. Mendoza objected on the ground of attorney-client privilege.

Mendoza then wrote to defense counsel, Kevin Iams, demanded the return of the e-mails, and said she would seek a protective order if he refused. Iams replied that Holmes made a knowing waiver of the privilege when she communicated with counsel on the company's e-mail system after being advised that her e-mails were not private. Nevertheless, Iams wrote, “I recognize that this is not an area in which the law is settled. … What I propose as a resolution is a stipulated protective order whereby I and my **[***35]** **[*1066]** clients will agree that we will not use the emails or facsimile copies in any deposition or court proceeding, unless we provide you written notice 45 days in advance. This will allow us further time to meet and confer, obtain a further protective order, or if necessary, to seek the court's intervention.”

Mendoza initially refused the proposed resolution, but then agreed. On May 15, 2006, Iams wrote a confirmation letter stating that Mendoza agreed to delay filing for a protective order pending a review of the “proposed protective order” that Iams would draft, wherein he would agree not to use the documents in any deposition or court proceeding without first giving Mendoza 45 days' written notice. The letter noted, however, that “by entering into the protective order, neither side is waiving any arguments it may have regarding the appropriate use of the [e-mails].” Stating that his schedule that week was hectic, Iams said he would strive to have a draft of the protective order to Mendoza by the end of the week for her review.

Before Iams drafted the stipulated protective order, Attorney Robin Perkins substituted in as defendants' counsel. Thereafter, Perkins used the e-mails in support **[***36]** of defendants' motion for summary judgment.

Holmes demanded that defendants withdraw the e-mail evidence, in accord with their agreement not to use it without prior notice. She submitted a declaration objecting to use of the attorney-client e-mails, claiming they were privileged.

Responding that the parties had never agreed not to utilize the e-mails, and that no protective order had ever been executed, defendants objected to Holmes's declaration that the e-mails were privileged. In defendants' view, the declaration was improper lay opinion, and Holmes had waived the attorney-client

privilege. They pointed out that Holmes's counsel specifically permitted defendants' counsel to ask questions concerning the e-mails, stating: "If the only extent of your questions are going to be about this e-mail exchange, *and you're not going to go into a follow-up meeting that was had or any other communications with her attorney*, and it's not going to be considered a waiver of any of *those communications*, then I have no problem with it." (Italics added.)

The trial court sustained defendants' objections and did not exclude the e-mail evidence.

Thereafter, Holmes sought discovery sanctions for defendants' **[***37]** failure to return the e-mails and for violating the agreement not to use them without affording Holmes prior notice.

Defendants opposed the motion on the grounds that the parties never reached a written stipulation; Holmes never filed a motion to compel, which **[*1067]** meant the court **[**895]** had never ordered Petrovich to return the documents; and the court had already found that the use of the e-mails did not violate the attorney-client privilege.

The court denied the motion for discovery sanctions, finding defendants had not engaged in any discovery abuse. It explained: "With respect to the e-mails that were submitted by defendants with the motion for summary judgment/adjudication, the Court found plaintiff had waived attorney-client privilege … ."

Holmes contests this ruling, asserting "no specific finding of waiver was made" in connection with the motion for summary judgment because defendants' objections to the claim of attorney-client privilege were made on multiple grounds, and the court merely sustained the objections without specifying the basis for its ruling. Thus, she argues, the court erred in relying on a nonexistent finding of waiver to deny the discovery sanctions motion.

Holmes overlooks **[***38]** that Judge Shelleyanne Chang presided over both the motion for summary judgment and/or adjudication and the motion for discovery sanctions. We presume that Judge Chang knew the basis for her own ruling sustaining defendants' objections in the first proceeding. Hence, Judge Chang did not err in relying on her prior determination that Holmes waived the attorney-client privilege. Furthermore, as we shall explain in the next part of the opinion, the e-mails were not privileged.

B

Holmes asserts the court erred in overruling her motion in limine to prevent defendants from introducing the aforementioned e-mails at trial to show Holmes did not suffer severe emotional distress, was only frustrated and annoyed, and filed the action at the urging of her attorney.

The court ruled that Holmes's e-mails using defendants' company computer were not protected by the attorney-client privilege because they were not private.

Holmes argues that the court did not understand the proper application of *section 917*, and thus erred in allowing introduction of the e-mail evidence. According to Holmes, "the California Legislature has already deemed [the fact that a communication was made electronically] to be **[***39]** irrelevant in determining whether a communication is confidential and therefore privileged." However, it is Holmes, not the trial court, who misunderstands the proper application of *section 917*.
[*1068]

CA(6)[↑] (6) *HN17*[↑] Although a communication between persons in an attorney-client relationship "does not lose its privileged character for the sole reason that it is communicated by electronic means or because persons involved in the delivery, facilitation, or storage of electronic communication may have access to the content of the communication" (*§ 917, subd. (b)*), this does not mean that an electronic communication is privileged when (1) the electronic means used belongs to the defendant; (2) the defendant has advised the plaintiff that communications using electronic means are not private, may be monitored, and may be used only for business purposes; and (3) the plaintiff is aware of and agrees to these conditions. A communication under these circumstances is not a " 'confidential communication between client and lawyer' " within the meaning of *section 952* because it is not transmitted "by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present **[***40]** to further the interest of the client in the consultation … ." (*Ibid.*)

[896]** *CA(7)*[↑] (7) When Holmes e-mailed her attorney, she did not use her home computer to which some unknown persons involved in the delivery, facilitation, or storage may have access. Had she done so, that would have been a privileged communication unless Holmes allowed others to have access to her e-mails and disclosed their content. Instead, she used

defendants' computer, after being expressly advised this was a means that was not private and was accessible by Petrovich, the very person about whom Holmes contacted her lawyer and whom Holmes sued. This is akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by Petrovich would be privileged.

Holmes disagrees, but the decisions upon which she relies are of no assistance to her because they involve inapposite factual circumstances, such as *Fourth Amendment* searches and seizures by public or government employers (*Quon v. Arch Wireless Operating Co., Inc. (9th Cir. 2008) 529 F.3d 892* (hereafter *Quon*), revd. *sub nom*. *Ontario v. Quon (2010) 560 U.S. ___, [177 L.Ed.2d 216, 231, 130 S. Ct. 2619]*; **[***41]** *Leventhal v. Knapek (2d Cir. 2001) 266 F.3d 64*; *Convertino v. U.S. Dept. of Justice (D.C. Cir. 2009) 674 F.Supp.2d 97, 110*), or the use of a personal Web-based e-mail account accessed from an employer's computer where the use of such an account was not clearly covered by the company's policy and the e-mails contained a standard hallmark warning that the communications were personal, confidential, attorney-client communications. (*Stengart v. Loving Care Agency, Inc. (2010) 201 N.J. 300 [990 A.2d 650, 659, 663–664]*.)

The present case does not involve similar scenarios. Holmes used her employer's company e-mail account after being warned that it was to be used **[*1069]** only for company business, that e-mails were not private, and that the company would randomly and periodically monitor its technology resources to ensure compliance with the policy. (Cf. *Scott v. Beth Israel Medical Center, Inc. (N.Y.Sub.Ct. 2007) 17 Misc. 3d 934 [847 N.Y.S.2d 436, 441–443]* [despite a statute similar to *§ 917*, an attorney-client privilege did not exist when a company computer was used to send e-mails, and the company's policy prohibited the personal use of e-mails, warned that they were not private, and stated that they could be monitored].) [3]

Holmes emphasizes that she believed her personal e-mail would be private because she utilized a private password to use the company computer and she deleted the e-mails after they were sent. However, her 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. Likewise, simply because she "held onto a copy of the fax," she had no expectation of privacy in documents she sent to **[***43]** her attorney using the company's facsimile machine, a technology resource that, she was told, would **[**897]** be monitored for compliance with company policy not to use it for personal matters.

According to Holmes, even though the company unequivocally informed her that employees who use the company's computers to send personal e-mail have "no right of privacy" in the information sent (because the company would periodically inspect all e-mail to ensure compliance with its policy against personal use of company computers), she nonetheless had a reasonable expectation that her personal e-mail to her attorney would be private because the " 'operational reality' was that there was no access or auditing of employee's computers." (Quoting *Quon, supra, 529 F.3d 892*, revd. *sub nom*. *Ontario v. Quon, supra*, 560 U.S. at p. ___ [177 L.Ed.2d at p. 231].)

In support of this contention, Holmes claims she "knew that her computer was password protected and that no one had asked for or knew her password, and the only person who had the ability to inspect the computers did not ever perform that task." This misrepresents the record in two respects. It is inaccurate to say only one person had the ability to monitor **[***44]** e-mail sent and received on company computers. The company's controller, who had an administrative password giving her access to all e-mail sent by employees **[*1070]** with private passwords, testified that the company's "IT person" as well as company owner Cheryl Petrovich also had such access to e-mail sent and received by company computers. And at no time during her testimony did Holmes claim she knew for a fact that, contrary to its stated policy, the company never actually monitored computer e-mail. She simply said that, to her knowledge, no one did so.

---

[3] *Section 917, subdivision (b)* **[***42]** is derived from the statute at issue in *Scott v. Beth Israel Medical Center, Inc., supra, 847 N.Y.S.2d 436*, New York's *Civil Practice Law and Rules, section 4548*, which states: "No communication privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication." (See Cal. Law Revision Com. com., reprinted at 29B pt. 3A West's Ann. Evid. Code (2009 ed.) foll. § 917, p. 267.)

In any event, Holmes's reliance on *Quon* is misplaced. There, a police sergeant, Jeff Quon, sued his employer, the Ontario Police Department, claiming it violated his *Fourth Amendment* right to be free of unlawful government searches and seizures when it reviewed text messages that he sent on an employer-issued text pager. (*Quon, supra, 529 F.3d at p. 895*.) In holding that Quon had a reasonable expectation of privacy in his text messages due to the operational realities of the workplace, the Ninth Circuit relied in large part on the plurality opinion in *O'Connor v. Ortega (1987) 480 U.S. 709 [94 L.Ed.2d 714, 107 S. Ct. 1492]* (hereafter *O'Connor*). (*Quon, supra, 529 F.3d at pp. 903–904, 907*.)

O'Connor **[***45]** held that the fact an employee works for the government does not negate the employee's *Fourth Amendment* right to be free of unreasonable governmental searches and seizures at work. (*O'Connor, supra, 480 U.S. at pp. 715, 717 [94 L.Ed.2d at pp. 721, 723]*.) But "[t]he operational realities of the workplace … may make *some* employees' expectations of privacy unreasonable … ." (*Id. at p. 717 [94 L.Ed.2d at p. 723]*.) For example, the existence of specific office policies, practices, and procedures may have an effect on public employees' expectations of privacy in their workplace. (*Ibid*.) "Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." (*Id. at p. 718 [94 L.Ed.2d at p. 723]*.)

Relying on *O'Connor*, the Ninth Circuit upheld the district court's determination that Quon had a reasonable expectation of privacy in his text messages because, despite a departmental policy that users of pagers had no right to privacy, the operational reality was that Quon was given an expressly conflicting message to the contrary by his supervisor. (*Quon, supra, **[**898]** 529 F.3d at p. 907*.) **[***46]** In addition to finding Quon had a reasonable expectation of privacy, the Ninth Circuit found the search was unreasonable in violation of the *Fourth Amendment*. (*529 F.3d at pp. 908–909*.)

The United States Supreme Court reversed this decision on the ground the search was not unreasonable. (*Ontario v. Quon, supra*, 560 U.S. at pp. ___–___ [177 L.Ed.2d at pp. 229–231].) Before turning to that issue, it noted that the parties disputed whether Quon had a reasonable expectation of privacy with respect to his pager messages. (*Id*. at p. ___ [177 L.Ed.2d at **[*1071]** p. 226].) Opting not to resolve this issue or whether the *O'Connor* "operational reality" test was applicable, the court observed that it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the *Fourth Amendment* implications of emerging technology before its role in society has become clear." (*Id*. at pp. ___–___ [177 L.Ed.2d at pp. 226–227].) "Even if the Court were certain that the *O'Connor* plurality's approach were the right one, the Court would have difficulty predicting how employees' **[***47]** privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. … And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." (*Id*. at p. ___ [177 L.Ed.2d at p. 227], citation omitted.)

Here, we are not concerned with a potential *Fourth Amendment* violation because Holmes was not a government employee. And, even assuming the "operational reality" test applies, it is of no avail to Holmes because the company explicitly told employees that they did not have a right to privacy in personal e-mail sent by company computers, which e-mail the company could inspect at any time at its discretion, and the company never conveyed a conflicting policy. 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. Just as it is unreasonable to say a person has a legitimate expectation **[***48]** that he or she can exceed with absolute impunity a posted speed limit on a lonely public roadway simply because the roadway is seldom patrolled, it was unreasonable for Holmes to believe that her personal e-mail sent by company computer was private simply because, to her knowledge, the company had never enforced its computer monitoring policy.

In sum, "so far as [Holmes was] aware," within the meaning of *section 952*, the company computer was not a means by which to communicate in confidence any information to her attorney. The company's computer use policy made this clear, and Holmes had no legitimate reason to believe otherwise, regardless of whether the company actually monitored employee e-mail. Thus, when, with knowledge of her employer's computer monitoring policy, Holmes used a company

computer to e-mail her attorney about an employment action against her boss, Petrovich, Holmes in effect knowingly disclosed this information to a third party, the company and thus Petrovich, who certainly was not involved in furthering Holmes's interests in her consultation with her attorney (§ 952) because Petrovich was the party she eventually sued.
[*1072]

[899]** Hence, the trial court correctly ruled that **[***49]** the attorney-client communication was not privileged. (§ 952.)

C

According to Holmes, the trial court erred when it gave the jury a protective admonishment about the attorney-client e-mails.

The court stated: “Jury, normally you may be shocked to see something like this on screen. However, I determined in proceedings prior to trial that this was not privileged information between an attorney and a client because it was communicated through company computers.” When Holmes's attorney began to object, the court responded, “the jury needs to understand that we are not romping wholesale over the attorney/client privilege. And I don't want the jury to be offended by this type of correspondence.”

After an unreported sidebar conference, the court stated: “I think I've made it clear to you [(the jurors)] why you're being permitted to see this kind of unusual correspondence, and the only reason you're able to see it is for the reasons I expressed earlier, namely that it was correspondence on a company computer, but that has nothing whatsoever to do with Miss Holmes' claim of privacy with respect to the pregnancy issues she communicated to Mr. Petrovich and her claims of emotional distress from that. **[***50]** [¶] So don't take my comments as any kind of indication how you should decide the merits of this case based upon this attorney/client communication. It's a very, very different issue. [¶] But I felt you should know why I'm permitting you to see this, because it's a very unusual kind of correspondence between a client and an attorney that normally juries would not see, but you're seeing it for that very limited purpose, but consider it only for the very limited purpose … and don't attach any importance to it on the main claim of Miss Holmes against [Petrovich].?

Holmes argues the above quoted comments undermined her invasion of privacy claim by more or less advising the jury she had no right to privacy in e-mails on a company computer. Not so.

The causes of action for invasion of privacy and intentional infliction of emotional distress were not premised on Petrovich accessing Holmes's attorney-client e-mails, but on his forwarding to her coworkers her private e-mails to him about her pregnancy. She claimed that this dissemination of intimate details concerning her pregnancy violated her right to privacy, that Petrovich's conduct was outrageous, and that it caused Holmes great emotional **[***51]** distress.
[*1073]

The court unambiguously advised the jury that Holmes's e-mails to her attorney were being introduced for a limited purpose, and the court's determination that they were not privileged because they were sent on a company computer had “nothing whatsoever to do with [her] claim of privacy” and her claims of emotional distress. Then, in response to jury questions during deliberations, the court advised the jury that an electronic data transmission may constitute an invasion of privacy if the elements of the tort are established by a preponderance of the evidence, [4] and that policies in an employer handbook could not supersede California law.

[900]** Holmes points to nothing indicating that the court's comments were a misstatement of the evidence or law. Unlike *Lewis v. Bill Robertson & Sons, Inc. (1984) 162 Cal.App.3d 650 [208 Cal. Rptr. 699]*, upon which Holmes relies, the court did not commit misconduct and engage in partisan advocacy by expressing strong opinions on the ultimate issue at trial (*id. at pp. 656–657*), i.e., whether Petrovich invaded her right to privacy by forwarding to Holmes's coworkers the e-mails about her pregnancy. Under the circumstances, she has failed to meet her burden of establishing error. (*Badie v. Bank of America (1998) 67 Cal.App.4th 779, 784–785 [79 Cal. Rptr. 2d 273]* [it ***HN18***[⬆] is the appellants' burden to establish error with reasoned argument and citations to authority].)

---

[4] The court instructed the jury earlier that, to establish her claim for invasion of privacy, Holmes had to prove the following five elements: (1) she had a reasonable expectation of privacy in precluding the dissemination or misuse of sensitive and confidential information under the circumstances; (2) Petrovich invaded her privacy by disseminating or misusing her sensitive or confidential information; (3) the conduct was a serious invasion of her privacy; (4) she was harmed; and (5) Petrovich's conduct was a substantial factor in causing her **[***52]** harm.

Holmes also fails to meet her burden of establishing that the alleged error was prejudicial. (*In re Marriage of McLaughlin (2000) 82 Cal.App.4th 327, 337 [98 Cal. Rptr. 2d 136]* [an appellant bears the burden of establishing prejudice by spelling out in his or her brief exactly how an alleged error caused a miscarriage of justice]; *American Drug Stores, Inc. v. Stroh, supra, 10 Cal.App.4th at p. 1453* [appellants may not attempt to rectify their omissions and oversights for the first time in their **[***53]** reply briefs].) Holmes does not present a coherent argument explaining how the court's statement that her e-mails to her attorney were not privileged undermined her theory that Petrovich egregiously violated her privacy by forwarding e-mails about her difficult and sensitive pregnancy decisions to people she claimed had no legitimate business need to know about the matters discussed therein. Thus, Holmes fails to demonstrate that, but for the court's alleged errors, it is reasonably probable the jury would have returned a more favorable verdict. (*Cassim v. Allstate Ins. Co. (2004) 33 Cal.4th 780, 801–802 [16 Cal. Rptr. 3d 374, 94 P.3d 513]*.)

[*1074]

III

In her reply brief, Holmes attempts to raise a new argument challenging the jury's verdict on her cause of action for invasion of privacy. The argument is entitled, "ONE DOES NOT LOSE THEIR [*sic*] CONSTITUTIONAL RIGHT TO PRIVACY SIMPLY BY WALKING THROUGH THE ENTRANCE OF THE WORKPLACE."

She asserts that an employer cannot destroy the constitutional right to privacy via a company handbook without due consideration being paid; that an employee has a reasonable expectation of privacy when an employer's technology policy is not enforced; and that an employer violates an employee's right **[***54]** to privacy when he discloses private information about the employee without a legitimate business reason for doing so.

We decline to address this argument because it is raised for the first time in her reply brief and is thus forfeited. (*Garcia v. McCutchen, supra, 16 Cal.4th at p. 482, fn. 10*; *Reichardt v. Hoffman, supra, 52 Cal.App.4th at pp. 764–765*; *American Drug Stores, Inc. v. Stroh, supra, 10 Cal.App.4th at p. 1453*.)

DISPOSITION

The judgment is affirmed.

Hull, Acting P. J., and Butz, J., concurred.

End of Document

In re Info. Mgmt. Servs., Inc. Derivative Litig.

Court of Chancery of Delaware

August 22, 2013, Submitted; September 5, 2013, Decided

Consol. C.A. No. 8168-VCL

Reporter
81 A.3d 278 *; 2013 Del. Ch. LEXIS 220 **; 2013 WL 5426157

IN RE INFORMATION MANAGEMENT SERVICES, INC. DERIVATIVE LITIGATION

Core Terms

email, monitoring, communications, employees, reasonable expectation of privacy, intercept, privacy, Global, electronic communication, Company's, confidential, attorney-client, no reasonable expectation, accessed, policies, reserved, webmail, files, personal use, Advisors, senior, wire, derivative action, motion to compel, privileged, computers, factors, courts, stored, Internet

Case Summary

Overview
ISSUE: Whether shareholders that alleged two officers mismanaged the corporation were entitled to compel discovery of work emails between the officers and their personal lawyers about the alleged mismanagement. HOLDINGS: [1]-Because the corporation's policy manual notified employees that it had unrestricted access to communications sent using company computers, the officers did not have a reasonable expectation of privacy in the work emails and, accordingly, the content of the emails was not protected by the attorney-client privilege of Del. R. Evid. 502(b); [2]-Under the circumstances of the case, the protections afforded by the federal Wiretap Act of 1968, the federal Electronic Communications Protection Act of 1986, and Maryland's versions of those Acts did not in give employees a reasonable expectation of privacy in their work emails.

Outcome
The motion to compel was granted.

LexisNexis® Headnotes

Evidence > Privileges > Attorney-Client Privilege > Elements

Evidence > Privileges > Attorney-Client Privilege > Scope

HN1[] **Attorney-Client Privilege, Elements**

See Del. R. Evid. 502(b).

Evidence > Burdens of Proof > Allocation

Evidence > Privileges > General Overview

HN2[] **Burdens of Proof, Allocation**

The burden of proving that a privilege applies to a particular communication is on the party asserting the privilege.

Evidence > Privileges > Attorney-Client Privilege > Elements

HN3[] **Attorney-Client Privilege, Elements**

With respect to the attorney-client privilege, Del. R. Evid. 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. A party's

subjective expectation of confidentiality must be objectively reasonable under the circumstances.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN4[] Privacy & Security, Company Communications

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. 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. To guide the case-by-case analysis, the court applies four factors (the Asia Global Crossing test): (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or email, (3) do third parties have a right of access to the computer or emails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies? No one factor is dispositive. The question of privilege comes down to whether the employee's intent to communicate in confidence was objectively reasonable.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN5[] Privacy & Security, Company Communications

In determining whether an employee has a reasonable expectation of privacy in work emails, the first factor of the Asia Global Crossing test is, does the corporation maintain a policy banning personal or other objectionable use? 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 reserves the right to monitor work email communications. An outright ban on personal use would likely end the privilege inquiry at the start. But a complete ban on personal use is not required. 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.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN6[] Privacy & Security, Company Communications

In determining whether an employee has a reasonable expectation of privacy in work emails, the second factor of the Asia Global Crossing test is, does the company monitor the use of the employee's computer or e-mail? 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, 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 monitoring policy and the employee can show detrimental reliance. 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. In that setting, evidence of actual monitoring would make an expectation of privacy even less reasonable.

Business & Corporate Law > ... > Directors & Officers > Management Duties & Liabilities > General Overview

HN7[] Directors & Officers, Management Duties & Liabilities

See Del. Code Ann. tit. 8, § 141(a).

techniques, deployed special monitoring software, or hacked the employee's accounts or files. The 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.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

Business & Corporate Law > ... > Corporate Governance > Directors & Officers > General Overview

HN8[] Privacy & Security, Company Communications

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. If an individual director needs 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. *Del. Code Ann. tit. 8, § 220(d)*. Directors' expectations of privacy in their work email are no different from any other employee's.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN9[] Privacy & Security, Company Communications

In determining whether an employee has a reasonable expectation of privacy in work emails, the third factor of the Asia Global Crossing test is, do third parties have a right of access to the computer or e-mails? 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. 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

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN10[] Privacy & Security, Company Communications

In determining whether an employee has a reasonable expectation of privacy in work emails, as framed by the Asia Global Crossing court, the fourth factor is, did the corporation notify the employee, or was the employee aware, of the use and monitoring policies? 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 expectation of privacy. If the employee had actual or constructive knowledge of the policy, then this factor favors production because any subjective expectation of privacy that the employee may have had is likely unreasonable. Decisions have readily imputed knowledge of an employer's policy to officers and senior employees.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

Communications Law > Federal Acts > Wiretap Acts

Evidence > Privileges > General Overview

Governments > Courts > Common Law

HN11[] Privacy & Security, Company Communications

The protections afforded by the federal Wiretap Act of 1968 do not give employees a reasonable expectation of privacy in their work email. The Act does not alter the

common law privilege analysis with respect to determining whether an employee has a reasonable expectation of privacy in work emails.

Business & Corporate Compliance > ... > Communications Law > Federal Acts > Stored Communications Act

Computer & Internet Law > Privacy & Security > Electronic Communications Privacy Act

Evidence > Privileges > General Overview

Governments > Courts > Common Law

HN12 **Federal Acts, Stored Communications Act**

Tit. II of the Electronic Communications Protection Act of 1986 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.S. § 2701(a). The Act does not change the common law privilege analysis with respect to determining whether an employee has a reasonable expectation of privacy in work emails.

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

Communications Law > Federal Acts > Wiretap Acts

Evidence > Privileges > General Overview

Governments > Courts > Common Law

HN13 **Privacy & Security, Company Communications**

Maryland has enacted a state version of the federal Wiretap Act of 1968. Although the Maryland Wiretap Act, Md. Code, Cts. & Jud. Proc. §§ 10-401 to 10-414, 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 with respect to determining whether an employee has a reasonable expectation of privacy in work emails.

Communications Law > Federal Acts > Wiretap Acts

HN14 **Federal Acts, Wiretap Acts**

Unlike the federal Wiretap Act of 1968, it is only lawful under Maryland law for a person to intercept an 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. Md. Code, Cts. & Jud. Proc. § 10-402(c)(3). By requiring consent from all parties to the communication, the Maryland Wiretap Act, Md. Code, Cts. & Jud. Proc. §§ 10-401 to 10-414, imposes stricter requirements for civilian monitoring than federal law.

Communications Law > Federal Acts > Wiretap Acts

Computer & Internet Law > Privacy & Security > Electronic Communications Privacy Act

HN15 **Federal Acts, Wiretap Acts**

The Maryland Wiretap Act, Md. Code, Cts. & Jud. Proc. §§ 10-401 to 10-414, like the federal Wiretap Act of 1968, turns on the existence of an "intercept" made with a "device," and Maryland caselaw has interpreted these terms narrowly, consistent with federal law. Under the Maryland 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. Md. Code, Cts. & Jud. Proc. § 10-402(c)(1)(i).

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

Business & Corporate Compliance > ... > Communications Law > Federal

Acts > Stored Communications Act

HN16[] Privacy & Security, Company Communications

Maryland has enacted a state version of the federal Stored Communications Act. The Maryland Stored Communications Act, Md. Code, Cts. & Jud. Proc. §§ 10-4A-01 to 10-4A-08, generally parallels the federal Act. Like the federal Act, the Maryland Act makes it unlawful for any person to intentionally access without authorization a facility through which an electronic communication service is provided or to intentionally 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. The exceptions to the Maryland Act similarly parallel the federal Act. They include an exception for conduct authorized by 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.

Counsel: **[**1]** 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.

Judges: LASTER, Vice Chancellor.

Opinion by: LASTER

Opinion

[*282] 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 **[**2]** 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 **[**3]** 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 **[*283]** 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 **[**4]** 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, **[**5]** 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 **[*284]** the Board before presenting its final report.

During a meeting of the Board **[**6]** 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 **[**7]** 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 **[**8]** 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 **[*285]** 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. [9] 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:

> ***HN1***[↑] **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 **[**10]** 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.

HN2[↑] "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)*. ***HN3***[↑] *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, 101 S. Ct. 677, 66 L. Ed. 2d 584 (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 **[**11]** an employee has a reasonable expectation of privacy in a work email account.[1] In one of the early decisions to

[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

[*286] consider 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, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (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 **[**12]** within the 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*.

HN4[] 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 **[*287]** use, (2) does the company monitor the use of the **[**15]** 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*.

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

---

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 **[**13]** and webmail). Courts have generally afforded greater privacy protection to webmail and have reached divergent conclusions when analyzing the attorney-client privilege if the employee and personal attorney communicated using webmail. *Compare Long v. Marubeni Am. Corp., 2006 U.S. Dist. LEXIS 76594, 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 U.S. Dist. LEXIS 29387, 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., 201 N.J. 300, 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 **[**14]** precedents involving work email). This case involves work email, not webmail.

[2] *See, e.g., TBG Ins. Servs. Corp. v. Superior Court, 96 Cal. App. 4th 443, 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).

[3] *See, e.g., Maxtena, Inc. v. Marks, 2013 U.S. Dist. LEXIS 42332, 2013 WL 1316386, at *5 (D. Md. Mar. 26, 2013)*; *In re*

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, ***HN5***[↑] 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 **[**17]** 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 reserves the right to monitor work email communications.[4] "[A]n outright ban on personal

*High-Tech Employee Antitrust Litig., 2013 U.S. Dist. LEXIS 28623, 2013 WL 772668, at *6 (N.D. Cal. Feb. 28, 2013)*; *United States v. Finazzo, 2013 U.S. Dist. LEXIS 22479, 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 U.S. Dist. LEXIS 125935, 2011 WL 5201430, at *5 (S.D.W. Va. Oct. 31, 2011)*; *Kaufman v. SunGard Inv. Sys., 2006 U.S. Dist. LEXIS 28149, 2006 WL 1307882, at *4 (D.N.J. May 10, 2006)*; **[**16]** *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 Secs. & 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 U.S. Dist. LEXIS 37711, 2011 WL 1193030, at *2 (E.D. La. Mar. 28, 2011)*; *Sprenger v. Rector & Bd. of Visitors of Va. Tech, 2008 U.S. Dist. LEXIS 47115, 2008 WL 2465236, at *3 (W.D. Va. June 17, 2008)*; *United States v. Etkin, 2008 U.S. Dist. LEXIS 12834, 2008 WL 482281, at *4 (S.D.N.Y. Feb. 20, 2008)*; *Geer v. Gilman Corp., 2007 U.S. Dist. LEXIS 38852, 2007 WL 1423752, at *3 (D. Conn. Feb. 12, 2007)*.

[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 U.S. Dist. LEXIS 37711, 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 **[**18]** 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 U.S. Dist. LEXIS 69568, 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 U.S. Dist. LEXIS 76594, 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 **[**19]** 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 U.S. Dist. LEXIS 18863, 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 U.S. Dist. LEXIS 9408, 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 U.S. Dist. LEXIS 8343, 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 **[**20]** 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 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., 274 Va. 438, 650*

use would **[*288]** likely end the privilege inquiry at the start." *Finazzo, 2013 U.S. Dist. LEXIS 22479, 2013 WL 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]

[*289] 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, ***HN6***[↑] the second factor is "does the company monitor the use of the employee's computer or e-mail?" *322 B.R. at 257*. **[**23]** 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 monitoring policy and the employee can show detrimental reliance.[8] If, however, the employer has

---

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 U.S. Dist. LEXIS 125935, 2011 WL 5201430, at *2, *6* (ordering production despite **[**21]** 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 U.S. Dist. LEXIS 37711, 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 U.S. Dist. LEXIS 42332, 2013 WL 1316386, at *5* (finding reasonable expectation of privacy **[**22]** where "[t]here is no evidence here indicating that the [employer] maintained any sort of monitoring or use policy"); *DeGeer v. Gillis, 2010 U.S. Dist. LEXIS 97457, 2010 WL 3732132, at *9 (N.D. Ill. Sept. 17, 2010)* (declining to order production where there was no evidence of a company policy).

[7] *See, e.g., Chechele v. Ward, 2012 U.S. Dist. LEXIS 140888, 2012 WL 4481439, at *1-2 (W.D. Okla. Sept. 28, 2012)* (disregarding lack of actual monitoring); *Etkin, 2008 U.S. Dist. LEXIS 12834, 2008 WL 482281, at *4* ("Thus, it is irrelevant that the Government has not established **[**24]** 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.").

[8] *See, e.g., High-Tech Employee Antitrust Litig., 2013 U.S. Dist. LEXIS 28623, 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 U.S. Dist. LEXIS 104711, 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 U.S. Dist. LEXIS 22479, 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

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 **[*290]** expectation of privacy even less reasonable." *Finazzo, 2013 U.S. Dist. LEXIS 22479, 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 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, **[**26]** 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. ***HN7***[] "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)*. ***HN8***[] 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 Del. Ch. LEXIS 100, 2013 WL 1668205, at *3 (Del. Ch. Apr. 17, 2013)*; *accord* *Schoon v. Troy Corp., 2006 Del. Ch. LEXIS 123, 2006 WL 1851481, at *1 n.8 (Del. Ch. June 27, 2006)*; *Intrieri v. Avatex Corp., 1998 Del. Ch. LEXIS 96, 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 **[**27]** 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, ***HN9***[] 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 **[**28]** 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 **[*291]** 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)

---

argument that employer's choice not to enforce policy in certain circumstances rendered policy inapplicable).

[9] *See* *Finazzo, 2013 U.S. Dist. LEXIS 22479, 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 **[**25]** routinely reviews . . . the e-mails."); *Hanson, 2011 U.S. Dist. LEXIS 125935, 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 U.S. Dist. LEXIS 76594, 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., 191 Cal. App. 4th 1047, 119 Cal. Rptr. 3d 878, 898 (Cal. Ct. App. 2011)* (holding that lack of actual monitoring was "immaterial").

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

HN10[↑] 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 **[**30]** 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 expectation of privacy.[11] If the employee had actual or constructive knowledge of the policy, then **[*292]** this factor favors production because any subjective expectation of privacy 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]

---

[10] *See Finazzo, 2013 U.S. Dist. LEXIS 22479, 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 **[**29]** or practice otherwise allowing the employer to do so"); *Curto, 2006 U.S. Dist. LEXIS 29387, 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).

[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 U.S. Dist. LEXIS 47115, 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 U.S. Dist. LEXIS 28905, 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 **[**31]** 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, 123 S. Ct. 69, 154 L. Ed. 2d 3 (2002)*** (vacating and remanding for further consideration in light of *Ashcroft v. Free Speech Coalition, 535 U.S. 234, 122 S. Ct. 1389, 152 L. Ed. 2d 403 (2002)*); *Nagle, 2010 U.S. Dist. LEXIS 104711, 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 **[**32]** was prohibited and (ii) where employer had never engaged in monitoring).

[12] *See, e.g., Long, 2006 U.S. Dist. LEXIS 76594, 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 U.S. Dist. LEXIS 76594, 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]

William **[**33]** 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 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 **[**34]** 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.

[*293] 1. The Federal Wiretap Act

Title I of the ECPA amended the **[**35]** Federal Wiretap Act of 1968 by adding the term "electronic communications" to its prohibitions, thereby making it a crime for a person to "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* **[**36]** 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 U.S. Dist. LEXIS 91644, 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 **[**37]** 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

---

Electronic Communications Policy stated").

[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.

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)* **[**38]** (holding company president gave implied consent to corporate **[*294]** monitoring of his email and texts sent using company-furnished device); *Thygeson, 2004 U.S. Dist. LEXIS 18863, 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 **[**39]** for those purposes.

In light of these exceptions, ***HN11***[] 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

HN12[] 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 **[**40]** 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

HN13[] 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 **[*295]** evidence derived therefrom may be received in evidence in **[**41]** 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)*.

HN14[] 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, 43 Md. App. 528, 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 **[**42]** Andrew's work emails. HN15[] 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

HN16[] 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, 208 Md. App. 383, 56 A.3d 620, 625 (Md. Ct. Spec. App. 2012)*, *cert. denied, 430 Md. 646, 62 A.3d 732 (Md. 2013)* (observing that the Maryland **[*296]** Stored Communications **[**44]** Act "mirrors its federal counterpart").

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 **[**45]** 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.

---

[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 **[**43]** 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.

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 **[**46]** 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 U.S. Dist. LEXIS 37711, 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 **[*297]** against defendants affiliated **[**47]** with the other family. *See* Benerofe v. Cha, 1998 Del. Ch. LEXIS 28, 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 Del. Ch. LEXIS 50, 1997 WL 187316, at *6-8 (Del. Ch. Apr. 7, 1997), *aff'd on other grounds,* 701 A.2d 70 (Del. 1997).[17] These distinctions make it unclear

[16] *See, e.g.,* Rales v. Blasband, 634 A.2d 927, 932 (Del. 1993) ("Because directors are empowered to **[**48]** 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 **[**49]** 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").

[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 Del. Ch. LEXIS 50, 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 **[**50]** 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

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 **[*298]** 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, 91 S. Ct. 1191, 28 L. Ed. 2d 323 (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 waiver) might apply in an appropriate case. *Cf. Saito v. McKesson HBOC, Inc., 2002 Del. Ch. LEXIS 139, 2002 WL 31657622, at *6-7, *11 (Del. Ch. Nov. 13, 2002)* **[**51]** (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 **[**52]** with their personal attorneys and advisors using their work email accounts.

---

a derivative action such that a law firm could represent all defendants without impropriety.

End of Document

Rozell v. Ross-Holst

United States District Court for the Southern District of New York

June 21, 2007, Decided

05 Civ. 2936 (JGK)(JCF)

Reporter
2007 U.S. Dist. LEXIS 46450 *; 2007 WL 7132991

MARY ROZELL, Plaintiff, - against - COURTNEY ROSS-HOLST, an individual, ANDCO, LLC, a corporation, and NEIL PIROZZI, an individual, Defendants.

Subsequent History: Costs and fees proceeding at, Application granted by, in part *Rozell v. Ross-Holst, 2008 U.S. Dist. LEXIS 41609 (S.D.N.Y., May 29, 2008)*

Prior History: *Rozell v. Ross-Holst, 2006 U.S. Dist. LEXIS 2277 (S.D.N.Y., Jan. 20, 2006)*

Core Terms

plaintiff's claim, Defendants', summary judgment, summary judgment motion, sexual harassment, termination, trespass, penal law, e-mail, hostile work environment, quid pro quo, electronic, severe, after-acquired, Deposition, incidents, genuine issue of material fact, private right of action, issue of fact, harassment, files, magistrate judge, compact disk, no evidence, authorization, counterclaim, retaliation, accessed, abusive, privacy

Counsel: **[*1]** OUTTEN & GOLDEN, LLP, Attorneys for Plaintiff, BY: KATHLEEN PERATIS, MARK ROBERT HUMOWIECKI.

LITTLER MENDELSON, P.C., Attorneys for Defendants, BY: A. MICHAEL WEBER.

Judges: Before: HON. JOHN G. KOELTL, District Judge.

Opinion by: JOHN G. KOELTL

Opinion

HON. JOHN G. KOELTL,

District Judge

The plaintiff, Mary Rozell, brings this action against her former employer, Courtney Ross-Holst and Ross' privately-held corporation Andco, LLC, and the chief financial officer (CFO) of Andco, Neil Pirozzi, alleging sexual harassment and retaliation in violation of Title VII of the Civil Rights Act of 1964, the New York State Human Rights Law, and the New York City Human Rights Law, and also alleging claims for computer hacking in violation of federal and state law. The defendant Ross asserts a counterclaim for trespass under New York State law.

Briefly, the plaintiff was employed as a curator for Ross' private art collection, which was managed by the corporate entity Andco. The plaintiff alleges that the CFO of Andco, defendant Pirozzi, subjected her to constant sexual harassment, which -- according to the plaintiff -- culminated at the company Christmas party in December 2003, when, after having leered at her all night, Pirozzi **[*2]** walked the plaintiff home despite her protests and then tried unsuccessfully to kiss her. Several weeks after the incident, the plaintiff complained to Ross about Pirozzi's behavior and allegedly was terminated in retaliation for her complaint about three months later on April 28, 2004.

After the plaintiff's termination, she alleges that Pirozzi hacked into her America Online (AOL) e-mail account and stole sensitive information. Pirozzi allegedly instructed his secretary to call AOL and pretend to be the plaintiff in order to obtain the plaintiff's e-mail password.

Ross' counterclaim for trespass is based on an earlier incident that occurred around January 2003 in which the plaintiff allegedly provided appraisers from Sotheby's auction house with access to art works in Ross' bedroom without Ross' authorization.

Pending before the court are two motions, the

Defendants' motion for summary judgment and the plaintiff's motion for partial summary judgment. Also pending is an objection to a December 21, 2006 discovery ruling of the Magistrate Judge.

The standard of granting summary judgment is well established. Summary judgment may not be granted unless the pleadings, depositions, answers to **[*3]** interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law. *Federal Rule of Civil Procedure 56(c)*; see also *Celotex Corp. v. Catrett, 477 U.S. 317, 322, 106 S. Ct. 2548, 91 L. Ed. 2d 265 (1986)*; *Gallo v. Prudential Residential Service Limited Partnership, 22 F.3d 1219, 1223 (2d Cir. 1994)*. The trial court's task at the summary judgment motion stage of the litigation is carefully limited to discerning whether there are genuine issues of material fact to be tried, not to deciding them. It's duty, in short, is confined at this point to issue-finding; it does not extend to issue-resolution. *Gallo, 22 F.3d at 1224*. The moving party bears the initial burden of informing the district court of the basis for its motion and identifying the matter that it believes demonstrates the absence of a genuine issue of material fact. *Celotex 477 U.S. at 323*. The substantive law governing the case will identify those facts that are material, and only disputes over facts that might affect the outcome of the suit under the governing law will properly preclude the entry of summary judgment. **[*4]** *Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248, 106 S. Ct. 2505, 91 L. Ed. 2d 202 (1986)*.

In determining whether summary judgment is appropriate, a court must resolve all ambiguities and draw all reasonable inferences against the moving party. See *Matsushita Electric Industries Co. v. Zenith Radio Corp., 475 U.S. 574, 587, 106 S. Ct. 1348, 89 L. Ed. 2d 538 (1986)* (citing *United States v. Diebold, Inc., 369 U.S. 654, 655, 82 S. Ct. 993, 8 L. Ed. 2d 176 (1962)*); *Gallo, 22 F.3d at 1223*.

Summary judgment is improper if there is any evidence in the record from any source from which a reasonable inference could be drawn in favor of the nonmoving party. See *Chambers v. T.R.M. Copy Centers Corp., 43 F.3d 29, 37 (2d Cir. 1994)*. If the moving party meets its initial burden of showing a lack of a material issue of fact, the burden shifts to the nonmoving party to come forward with specific facts showing that there is a genuine issue for trial. *Federal Rules of Civil Procedure 56(e)*. The nonmoving party must produce evidence in the record and may not rely simply on conclusory statements or on contentions that the affidavit supporting the motion are not credible. *Ying Jing Gan v. City of New York, 996 F.2d 522, 532 (2d Cir. 1993)*; see also *Scotto v. Almenas, 143 F.3d 105, 114-15 (2d Cir. 1998)*.

The **[*5]** Defendants' move for summary judge the on four claims. (a) the plaintiff's claim of sexual harassment; (b) the plaintiff's claim for retaliation; (c) the plaintiff's claim based on computer hacking; and (d) the plaintiff's request for back pay and front pay.

The plaintiff's claim of sexual harassment is based on two theories, hostile work environment and quid pro quo sexual harassment. The defendants seek summary judgment on both theories.

To establish a prima facie case of hostile work environment under Title VII, a plaintiff must show: (1) discriminatory harassment that was sufficiently severe or pervasive to alter the conditions of the victim's employment and create an abusive working environment, and (2) a specific basis exists for imputing the objectionable conduct to the employer. *Alfano v. Costello 294 F.3d 365, 373 (2d Cir. 2002)*. The plaintiff must show not only that she subjectively perceived the environment to be abusive but also that the environment was objectively hostile and abusive. *Demoret v. Zegarelli, 451 F.3d 140, 149 (2d Cir. 2006)*; *Schiano v. Quality Payroll Systems, 445 F.3d 597, 604 (2d Cir. 2006)*.

The first element requires a showing that the workplace was so severely **[*6]** permeated with discriminatory intimidation, ridicule, and insult that the terms and conditions of her employment were thereby altered. *Alfano, 294 F.3d at 373*. Isolated incidents typically will not create a hostile work environment, unless the incidents are so severe that they alter the terms and conditions of employment. *Demoret, 451 F.3d at 149*. In general, incidents must be more than episodic; they must be sufficiently continuous and concerted in order to be deemed pervasive. *Alfano 294 F.3d at 374*. In analyzing a hostile work environment claim, courts must consider the totality of the circumstances, taking into account such factors as the frequency of the discriminatory conduct; its severity; whether it is physically threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance. *Harris v. Forklift Systems, Inc., 510 U.S. 17, 23, 114 S. Ct. 367, 126 L. Ed. 2d 295 (1993)*.

Although summary judgment is appropriate even in the fact-intensive context of employment discrimination cases, see *Abdu-Brisson v. Delta Air Lines, Inc, 239 F.3d 456 (2d Cir. 2001)*, the Second Circuit Court of Appeals has warned that hostile work environment claims present mixed **[*7]** questions of law and fact that are particularly well-suited for jury determination. *Schiano, 445 F.3d at 605*; see also *Holtz v. Rockefeller & Co., Inc., 258 F.3d 62, 75 (2d Cir. 2001)*; *Gallagher v. Delaney, 139 F.3d 338, 342, 347, 349 (2d Cir. 1998)*.

The Defendants' argue that the incidents about which the plaintiff complains are insufficiently severe to establish the first element of a hostile work environment claim and must be dismissed as a matter of law. At this stage of the litigation, the court disagrees.

The plaintiff has produced evidence that Pirozzi made frequent, unsolicited comments about her body that, as the plaintiff made known to Pirozzi and reported to her staff, made the plaintiff uncomfortable, engaged in suggestive physical contact, insisted on walking the plaintiff to the subway on several occasions and in doing so touched her in an unwanted manner, and visited her isolated office for prolonged periods of time and, while there, discussed intimate details of his personal life and probed the plaintiff with questions about her own personal life.

The most severe alleged incident of harassment occurred at the 2003 company Christmas party. There, according to the plaintiff, **[*8]** Pirozzi leered at the plaintiff throughout the night and repeatedly whispered to her that he was going to walk her home, which made the plaintiff nervous. After the party, Pirozzi insisted on accompanying the plaintiff home despite her telling him that she did not want him to do so. Then, outside her building, Pirozzi allegedly tried to kiss the plaintiff, but the plaintiff deflected the kiss and fled. The next time the plaintiff saw Pirozzi, he allegedly entered the plaintiff's office, squeezed behind her desk, and put his arms around her in a way that made her feel offended and threatened. See affidavit of Mary Rozell, September 28, 2006, paragraphs 40 to 51.

The parties dispute how often these incidents occurred and, of course, dispute the nature and severity of each of these incidents, along with the nature of the Pirozzi's relationship with the plaintiff. Although, viewed in isolation, each of these individual incidents appears only mildly hostile or abusive, the court must consider the totality of the circumstances in the light most favorable to the plaintiff, recognizing that the accumulation of numerous mild harms might, like the slow drip of water in a case of Chinese water **[*9]** torture, eventually cross the threshold from a harmless office crush to the creation of a hostile and abusive work environment. The first element of the plaintiff's hostile work environment claim hinges on a delicate determination of disputed facts, focusing on the frequency and severity of each of these alleged incidents of harm. Applying the relevant standards of this motion for summary judgment to the present record, the issue of whether Pirozzi's conduct was sufficiently severe or pervasive to create both an objectively and subjectively abusive working environment requires a trial.

The second element of the plaintiff's claim of a hostile work environment requires the plaintiff to show that a specific basis exists for imputing the alleged objectionable conduct to the employer. In the case of co-worker harassment, the employer will be liable only if the employer is negligent, either because the employer (1) provided no reasonable avenue of complaint; or (2) knew, or should have known, about the harassment but took no action to stop it. *Richardson v. New York State Department of Correctional Service, 180 F.3d 426, 441 (2d Cir. 1999)*, abrogated on other grounds, *Burlington Northern and Sante Fe Railway Co. v. White, 126 Supreme Court 2405, 165 L. Ed. 2d 345 (2006)*; **[*10]** *Murray v. New York University College of Dentistry, 57 F.3d 243, 249 (2d Cir. 1995)*. In contrast, an employer is presumed absolutely liable for harassment by a plaintiff's supervisor, absent establishing an affirmative defense to rebut that presumption. See *Burlington Industries, Inc. v. Ellerth, 524 U.S. 742, 765, 118 S. Ct. 2257, 141 L. Ed. 2d 633 (1998)*; *Richardson, 180 F.3d at 441*.

There is a genuine issue of material fact as to whether Pirozzi exercised supervisory authority over the plaintiff. The supervisor has the authority to affect the terms and conditions of the victim's employment. *Mack v. Otis Elevator Co., 326 F.3d 116, 126 (2d Cir. 2003)*; *Accord Prince v. Madison Square Garden, 427 F. Supp. 2d 372 (S.D.N.Y. 2006)*. The critical question is whether the authority given by the employer to the employee enabled or materially augmented the ability of the latter to create a hostile work environment. Id.

The plaintiff claims that Pirozzi had the authority to recommend her raises, bonuses and other benefits. The plaintiff raises a genuine issue of material fact with respect to Pirozzi's responsibility for determining raises. The defendants have produced evidence that Pirozzi was not responsible for determining the **[*11]** plaintiff's

raises. However, Pirozzi's testimony suggests that he had at least some influence over the system for determining raises. (See Deposition of Neil Pirozzi, May 2, 2006, at 44-45). Also, the plaintiff's testimony suggests that Pirozzi had an active role in determining riases for the plaintiff and her department. (See Deposition of Mary Rozell, February 1, 2006, at 176 to 80 and 184; Rozell affidavit paragraphs 5 to 6). Moreover, there is a question whether Pirozzi's ability to direct financial matters as CFO and his alleged influence with Ross created any sort of de facto authority sufficient to augment Pirozzi's ability to create a hostile work environment.

Regardless of whether Pirozzi ultimately determined to be a supervisor of the plaintiff, there are triable issues regarding whether Pirozzi's objectionable behavior can be imputed to Andco. There is a genuine issue of fact as to whether a reasonable avenue of complaint was available to the plaintiff to report any alleged sexual harassment. See, for example, *Reed v. A.W. Lawrence & Co., Inc., 95 F.3d 1170, 1181 (2d Cir. 1996)*. The evidence establishes that Andco had no sexual harassment policy, no anti-retaliation policy, **[*12]** and no documented procedure for employees to lodge sexual harassment complaints. The defendants contend that all of the employees knew that they could raise any issues with Ross. However, there is at least an issue of fact as to whether this general knowledge that the defendants impute to the Andco employees was sufficient.

Additionally, the plaintiff claims that Ross' treatment of her complaint was insufficient, alleging that Ross treated her complaint dismissively. The defendants respond that the plaintiff informed Ross that she would handle the issue herself and therefore is estopped from arguing the inadequacy of Andco's complaint procedures. See *Torres v. Pisano, 116 F.3d 625, 639 (2d Cir. 1997)*. The plaintiff, however, responds that she told Ross that she would handle the issue herself only because of Ross' allegedly dismissive attitude at their meeting. Resolving what transpired at this meeting is a question for trial. The defendants' motion for summary judgment on the plaintiff's claim of a hostile work environment is therefore denied.

The plaintiff also alleges actionable discrimination under Title VII on the basis of a quid pro quo sexual harassment. To state a claim under **[*13]** the quid pro quo theory, the plaintiff must show that a tangible employment action resulted from her failure to submit to Pirozzi's sexual advances. See *Schiano, 445 F.3d at 604*. The plaintiff alleges that Pirozzi played a meaningful role in Ross' decision to terminate her after she rejected Pirozzi following the company Christmas party. See, for example, *Bickerstaff v. Vassar College, 196 F.3d 435, 450 to 451 (2d Cir. 1998)*. However, based on the summary judgment record, the plaintiff has failed to produce evidence from which a reasonable finder of fact could conclude that Pirozzi played a meaningful role in the plaintiff's termination. The plaintiff claims that Pirozzi fueled a conflict between the employees in the plaintiff's department and then reported the conflict to Ross, who conducted an independent -- and, according to the plaintiff, inadequate -- investigation of the conflict and terminated the plaintiff. The plaintiff has adduced no evidence that Pirozzi recommended the plaintiff's discharge, and the evidence does not reveal that Pirozzi ever told Ross that the plaintiff was to blame for the conflict. (See Deposition of Courtney Ross, April 25, 2006, at 129 to 30; Deposition **[*14]** of Neil Pirozzi, May 2, 2006, at 221 to 222. Ross decided to discharge the plaintiff. There is no evidence that she was motivated by quid pro quo sexual harassment. There is also no evidence that Pirozzi played any meaningful role in Ross' decision to discharge the plaintiff, and therefore the defendant is entitled to summary judgment on the plaintiff's claim of quid pro quo sexual harassment.

The plaintiff also brings claims under the New York State Human Rights Law and the New York City Human Rights Law. In general the standards under state and city law parallel the standards under Title VII. See *Cruz v. Coach Stores, Inc., 202 F.2d 560, 565* note one (2d Cir. 2000). The plaintiff argues that the standards under the New York City Human Rights Law now diverge from the Title VII a and New York State Human Rights Law standards in that the New York City Human Rights Law is to be construed more liberally. *Ochei v. Coler/Goldwater Memorial Hospital, 450 F. Supp. 2d 275, 282-83 (S.D.N.Y. 2006)*. However, regardless of whether the New York City Human Rights Law is to be more liberally construed, the plaintiff has failed to offer sufficient evidence to establish a claim of quid pro quo sexual **[*15]** harassment. The plaintiff's claim for quid pro quo sexual harassment under the New York State Human Rights Law and the New York City Human Rights Law is also dismissed. On the other hand, because there are triable issues of fact with respect to the plaintiff's claim for a hostile work environment even under Title VII allegedly more stringent standards, there are also triable issues ever fact with respect to the plaintiff's hostile work environment claims under both the New York State Human Rights Law and the

allegedly more liberal New York City Human Rights Law.

In sum, the Defendants' motion for summary judgment on the plaintiff's sexual harassment claim based on a quid pro quo theory is granted. The Defendants' motion for summary judgment on the plaintiff's sexual harass am claim based on a theory of hostile work environment is denied.

The defendants also move for summary judgment on the plaintiff's claim of retaliatory discharge. To establish a prima facie claim for retaliation, the plaintiff must demonstrate that: (1) she engaged in a protected activity; (2) her employer was aware of the activity; (3) the employer took adverse employment action against her; and (4) a causal connection **[*16]** exists between the alleged adverse action and protected activity. *Schiano, 445 F.3d at 609*. The defendants argue that the plaintiff cannot establish that her discharge was causally related to her complaint of sexual harassment.

The plaintiff can establish a causal connection either indirectly by showing a close temporal proximity between the protected activity and the adverse employment action or directly by demonstrating retaliatory animus on the part of the decision maker. See *Gordon v. New York City Board of Education, 232 F.3d 111, 117 (2d Cir. 2000)*. In this case, the plaintiff has produced sufficient evidence to satisfy the causation element of her prima facie case of retaliation based on the temporal proximity -- three months -- between the protected activity and the firing, see, for example, *Hernandez v. Kelwood Co., No. 99 Civ. 10015, 2003 Westlaw 22309326, 20 (S.D.N.Y. October 8, 2003)* involving a five-month gap; *Suggs v. Port Authority of New York & New Jersey, No. 97 Civ. 4026, 1999 U.S. Dist. LEXIS 6319, 1999 Westlaw 269905 at 6 (S.D.N.Y. May 4, 1999)* involving a six-month gap, combined with Ross' shifting explanations for her decision to terminate the plaintiff, which raise serious issues as to **[*17]** Ross' credibility. Similarly, Ross' shifting explanations for her allegedly non-retaliatory basis for terminating the plaintiff's employment is a sufficient basis to create a triable issue of fact as to pretext. For all these reasons, the Defendants' motion for summary judgment on the plaintiff's claim of retaliation is denied.

While the plaintiff's claims of sexual harassment and retaliatory discharge present issues of fact that cannot be resolved on a motion for summary judgment, the claims under Title VII against Ross and Pirozzi in their individual capacities must be dismissed because there is no individual liability under Title VII. See *Tomka v. Seiler Corp., 66 F.3d 1295, 1313 (2d Cir. 1995)*, and abrogated on other grounds by *Burlington Industries, 524 U.S. at 742*; *DeWitt v. Lieberman, 48 F. Supp. 2d 280, 293 (S.D.N.Y. 1999)*. The plaintiff attempts to hold Ross liable individually under Title VII based on a novel veil-piercing theory but offers no authority for applying that doctrine to extend the statutory scope of Title VII. In any event, even assuming the plaintiff's veil-piercing theory was viable, the plaintiff has failed to adduce sufficient facts to establish a prima facie **[*18]** case of veil piercing here. See, for example, *William Pascalacqua Builders, Inc. v. Resnick Developers South, Inc., 933 F.2d 131, 137-39 (2d Cir. 1991)* ; *Shisgal v. Brown, 21 A.D.3d 845, 801 New York Supp. 2d 581, 583-84 (Appellate Division 2005)*; *Thomson-CSF, S.A. v. American Arbitration Association, 64 F.3d 773, 777 to 778 (2d Cir. 1995)*.

There is, for example, no evidence that the corporation was undercapitalized, that corporate formalities were not observed, or that Ross' alleged domination was used to commit a wrong against the plaintiff that resulted in the plaintiff's injury.

The defendants argue that Pirozzi cannot be liable under the New York City Human Rights Law for aiding and abetting because the plaintiff has failed to establish the predicate of employer liability. *DeWitt, 48 F. Supp. 2d at 293*. However, because there are issues of fact that preclude summary judgment on the question of employer liability, Pirozzi is not entitled to summary judgment on the Defendants' argument that he is not liable for aiding and abetting under the New York City Human Rights Law.

The plaintiff brings claims under Title II of the Electronic Communications Privacy Act (ECPA), the Stored Communications Act, *18 U.S.C. Section 2701* **[*19]** and *New York Penal Law Section 156.10* for Pirozzi's allegedly having hacked into the plaintiff's AOL e-mail account. The defendants move for summary judgment on both of these claims.

The ECPA creates civil liability for anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." *18 U.S.C. Sections 2701(a)* and *2707*; see also *Theofel v. Farey-Jones, 359 F.3d 1066, 1072 (9th Cir. 2004)*. Electronic storage is

defined as either "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *18 U.S.C. Sections 2510(17)* and *2711(1)*.

The defendants first argue that the ECPA claim should be dismissed because any information that was accessed through the AOL e-mail account was not "without authorization" as defined in *Section 2701(a)* because Andco owned the AOL e-mail account and because the plaintiff **[*20]** implicitly authorized Andco to access the account. However, there are genuine issues of material fact as to whether Andco was authorized under the ECPA to access the plaintiff's e-mail account, turning on such questions as the nature of the licensing agreement with AOL (the plaintiff initially entered into the account with AOL and there is no evidence that the user name was ever changed), any explicit or implicit authorizations the plaintiff may have granted to Andco by using its computer systems, and the scope and relevance of any Andco computer policies.

The defendants next argue that the ECPA does not apply to e-mails, such as those at issue here, accessed while in post-transmission storage, but rather, only to e-mails being stored temporarily during transmission. The court disagrees that the messages Pirozzi allegedly accessed from the plaintiff's AOL e-mail account were not in electronic storage. The better reading of the statute is that such messages fall within the ECPA's coverage. See *Theofel, 359 F.3d at 1075-77 (Kizinski, J.)*; *Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 924-26 (Western District of Wisconsin 2002)*. But cf. *Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107, 114 (3d Cir. 2004)*; **[*21]** *In re Doubleclick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 511 (S.D.N.Y. 2001)*.

The defendants also argue that the plaintiff waived her rights under the ECPA by using her AOL account for unlawful purposes. The defendants do not clearly articulate the legal theory on which they rely for this argument, although they faintly argue that the plaintiff had no right of privacy in these communications and therefore cannot avail herself of the ECPA's protections. However, the statute provides no exception for Pirozzi's actions based on the plaintiff's allegedly improper use of the account.

Finally, the defendants argue that any violations of the ECPA were not "wilful or intentional," and therefore the court should not impose punitive damages. See *Section 2707(c)*. On the present record, there are issues of fact as to whether Pirozzi's actions were "wilful or intentional." The defendants allege that Pirozzi thought his acts were authorized, and thus his actions were not "wilful or intentional." However, a reasonable jury could conclude that Pirozzi's efforts, which included his assistant fraudulently obtaining the plaintiff's password, were sufficient to warrant the imposition of punitive **[*22]** damages.

The plaintiff has not, however, produced any evidence that Ross had any knowledge of or participation in Pirozzi's efforts to access the plaintiff's e-mail account. Therefore, because there is no evidence that Ross "intentionally" accessed this information, the ECPA claim against Ross is dismissed.

The defendants also move for summary judgment on the plaintiff's claim under the *New York Penal Law Section 156.10*. *Section 156.10* provides in relevant part that "a person is guilty of computer trespass when he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and he or she thereby knowingly gains access to computer material." The defendants correctly argue that there is no implied private right of action under this section of the penal law, which essentially creates an offense against the right of privacy. There is no indication of a legislative intent to create a private right of action under this provision of the penal law and the courts in New York have been reluctant to find private rights of action for violations of the penal law, particularly provisions relating to privacy where the Legislature has **[*23]** recognized only a very limited private right of action. Thus the defendants are entitled to summary judgment dismissing this claim. See *Clark v. Elam Sand & Gravel, Inc., 777 New York Supp. 2d 624, 626, 4 Misc. 3d 294 (Supreme court 2004)*; *Talmor v. Talmor, 185 Misc. 2d 293, 712 N.Y.S. 2d 833, 836 (Supreme Court 2000)*; see also *Sheehy v. Big Flats Community Day, Inc., 73 N.Y.2d 629, 541 N.E.2d 18, 20, 543 N.Y.S.2d 18 (New York 1989)* (discussing the standards for implying a private right of action).

The defendants also move for summary judgment on the plaintiff's claim for back pay and front pay, arguing that the plaintiff is not entitled to this relief because the plaintiff failed to mitigate damages. A discharged employee must use reasonable diligence in finding other suitable employment, which need not be comparable to their previous positions. *Greenway v. Buffalo Hilton*

Hotel, 143 F.3d 47, 53 (2d Cir. 1998) (quoting Ford Motor Co. v. EEOC, 458 U.S. 219, 231-32 n.15, 102 S. Ct. 3057, 73 L. Ed. 2d 721 (1982)). The employer typically bears the burden to demonstrate that the plaintiff failed to mitigate damages. Id. In this case, there are disputed issues of fact as to the plaintiff's mitigation efforts, which cannot be resolved on a motion for summary judgment. Therefore, the Defendants' **[*24]** motion for summary judgment on the plaintiff's claims of back pay and front pay is denied.

In sum, the defendants' motion for summary judgment is denied, except as follows. The Defendants' motion for summary judgment on the plaintiff claim of quid pro quo sexual harassment is granted. The Defendants' motion for summary judgment as to Ross' and Pirozzi's individual liability under Title VII is granted. In addition, the Defendants' motion for summary judgment on the ECPA claim against defendant Ross is granted. The Defendants' motion for summary judgment on the plaintiff's claim under New York Penal Law Section 156.10 is granted.

The plaintiff moves for partial summary judgment on Ross' counterclaims for trespass and the Defendants' after-acquired evidence defense.

After-acquired evidence is evidence of wrongdoing by an employee that would have caused employee's termination, but for the fact that the defendant discovered the wrongdoing only after the employee's termination. Ahing v. Lehman Bros., Inc., No. 94 Civ. 9027 (CSH), 2000 U.S. Dist. LEXIS 5175, 2000 Westlaw 460443, at 11 (S.D.N.Y. April 18, 2000); see also McKennon v. Nashville Banner Publishing Co., 513 U.S. 352, 361-62, 115 S. Ct. 878, 130 L. Ed. 2d 852 (1995).

The plaintiff challenges the **[*25]** Defendants' after-acquired evidence defense, which is based on the plaintiff allegedly having admitted Sotheby's appraisers into Ross' bedroom without authorization. The plaintiff alleges that Ross' deposition testimony makes clear that Ross knew of this conduct prior to the plaintiff's termination, and therefore the incident is not after-acquired evidence. Ross' prior affidavits and the errata sheet to her deposition, however, state that Ross had no knowledge of the plaintiff's conduct prior to the plaintiff's termination. The plaintiff challenges the errata sheet as effectively a sham affidavit that should not be considered. However, even disregarding the errata sheet, Ross' affidavits, which were prepared prior to her deposition, maintain that she did not learn of the incident until after the plaintiff's termination. While Ross' potentially inconsistent testimony raises serious questions as to her credibility, there is still a genuine issue of material fact as to when Ross learned of the incident.

The plaintiff also argues that her conduct did not involve any wrongdoing because there was no Andco policy prohibiting the admission of the Sotheby's art appraisers. In any event, the **[*26]** plaintiff argues, to the extent that there was such a policy, at most her actions constitute a trivial rule violation and not the sort of conduct that would typically support an after-acquired evidence defense. See, for example, Ahing, 2000 U.S. Dist. LEXIS 5175, 2000 Westlaw 460443, at 11. The defendants vigorously contest the plaintiff's claim that she had the authority to admit the Sotheby's art appraisers into Ross' bedroom and contest the claim that the plaintiff's alleged trespass was too trivial or wrongdoing to support an after-acquired evidence defense. At base, these questions present issues of fact that cannot be resolved on a motion for summary judgment. See, for example, Hillman v. Hamilton College, No. 95 Civ. 1442, 1998 U.S. Dist. LEXIS 5064, 1998 Westlaw 166827 at 10 to 11 (Northern District of New York April 9, 1998) (Pooler, J.).

The plaintiff also moves to dismiss Ross' claim of trespass. First, the plaintiff argues that if the after-acquired evidence defense is dismissed, Ross' state law trespass claim, based on the plaintiff's providing the Sotheby's appraisers with access to Ross' bedroom, is not sufficiently related to the plaintiff's federal claims to come within the court's supplemental jurisdiction. However, the **[*27]** court is not dismissing the Defendants' after-acquired evidence defense, and thus the court has supplemental jurisdiction over Ross' state law trespass claim. See 28 U.S.C. Section 1367(a).

The plaintiff next argues that there was no trespass because the plaintiff had the authority to admit the Sotheby's experts to Ross' residence. There are, however, genuine issues of material fact regarding the scope of the plaintiff's authority to admit visitors to Ross' residence that preclude a grant of summary judgment.

Ross also asserts a counterclaim for the plaintiff's alleged violation of New York Penal Law Section 140.05, which provides that "a person is guilty trespass when he knowingly enters or remains unlawfully in or upon premises." Ross provides no authority for implying a private right of action under this provision of the penal law. Given the well-established tort of common law

trespass, on which Ross relies, an implied private right of action under this statute would not promote the legislative scheme. See Madden v. Creative Services, Inc., 646 Northeast 2d 780, 784 (New York 1995). Ross' counterclaim under *New York Penal Law Section 140.05* is therefore dismissed.

Therefore, the plaintiff's **[*28]** motion for partial summary judgment is denied, except Ross' counterclaims under *New York Penal Law Section 140.05* is dismissed.

The defendants also object to the magistrate judge's ruling dated September 21, 2006, which denied the Defendants' motion to compel the production of a compact disk allegedly containing files from the plaintiff's work computer. Ross' butler created the compact disk for the plaintiff. He copied the files from the plaintiff's work computer, which the plaintiff claimed to be personal and then, after doing so, deleted those files from the computer. As part of a document request, the defendants sought a copy of the compact disk. The plaintiff, instead, provided the defendants with all of the relevant files from the compact disk. The defendants then sought to compel production of the entire compact disk and the magistrate judge twice denied the request. (Orders of Magistrate Judge Francis, dated September 15, 2006 and September 21, 2006.)

The standard of review for a decision by the magistrate judge on a discovery issue is whether the ruling is clearly erroneous or contrary to law. See *Federal Rule of Civil Procedure 72(a)*; see also *28 U.S.C. Section 636(b)(1)(A)*; **[*29]** *Collens v. City of New York, 222 F.R.D. 249, 251 (S.D.N.Y. 2004)*; *In re Buspirone Patent Litigation, 210 F.R.D. 43, 52 (S.D.N.Y. 2002)*. And an order is clearly erroneous when the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed. *Surles v. Air France, 00 Civ. 5004, 2001 U.S. Dist. LEXIS 15315, 2001 Westlaw 1142231, at 1 (S.D.N.Y. September 27, 2001)*. An order is contary to law when it fails to apply or misapplies relevant statutes, case law or rules of procedure. Id.

The magistrate judge decision in this case fell well within his broad discretion to supervise discovery. The defendants' assertion that the plaintiff's purely personal files are relevant to demonstrate the amount of time the plaintiff spent on personal matters at work is speculative because the plaintiff used the computer--a laptop-outside of work. The magistrate judge was within his discretion to determine that any marginal relevance of the files on the compact disk did not justify their production in light of the burden of production on the plaintiff's privacy interests in the production of the relevant files. Therefore, the defendants objection to the magistrate judge's ruling **[*30]** of September 21, 2006 is overruled.

The court has carefully considered all of the arguments raised by the parties, and to the extent not specifically addressed, the court finds them to be either moot or without merit.

For all of the reasons explained above, the defendants' motion for summary judgment is granted in part and denied in part. The plaintiff's motion for partial summary judgment is granted in part and denied in part. The Defendants' objection to the magistrate judge's ruling is overruled.

So ordered.

Stengart v. Loving Care Agency, Inc.

Supreme Court of New Jersey

December 2, 2009, Argued; March 30, 2010, Decided

A-16 September Term 2009

Reporter
201 N.J. 300 *; 990 A.2d 650 **; 2010 N.J. LEXIS 241 ***; 108 Fair Empl. Prac. Cas. (BNA) 1558; 30 I.E.R. Cas. (BNA) 873; 93 Empl. Prac. Dec. (CCH) P43,853

MARINA STENGART, PLAINTIFF-RESPONDENT, v. LOVING CARE AGENCY, INC., STEVE VELLA, ROBERT CREAMER, LORENA LOCKEY, ROBERT FUSCO, AND LCA HOLDINGS, INC., DEFENDANTS-APPELLANTS.

Prior History: **[***1]** On appeal from the Superior Court, Appellate Division, whose opinion is reported at *408 N.J. Super. 54, 973 A.2d 390 (2009)*.

Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54, 973 A.2d 390, 2009 N.J. Super. LEXIS 143 (App.Div., 2009)

Disposition: The high court modified the judgment of the intermediate appellate court by removing the requirement that the case be remanded to the chancery court. It affirmed the judgment as modified and remanded the matter to the trial court to determine what, if any, sanctions should be imposed on the employer's counsel.

Core Terms

e-mails, attorney-client, communications, company's, laptop, confidential, privileged, messages, privacy, Internet, warning, retrieved, expectation of privacy, personal use, password-protected, monitor, files, trial court, disclosure, employees, hard drive, computers, exchanged, web-based, workplace, contents, forensic, policies, reasonable expectation of privacy, personal account

Case Summary

Procedural Posture

Plaintiff former employee sued defendant employer for discrimination. The trial court held that e-mails between the employee and her attorney on an employer-furnished computer were not privileged and denied the employee's request to disqualify the employer's counsel. The employee appealed; the New Jersey Superior Court, Appellate Division, reversed, finding counsel violated *N.J. R. Prof. Conduct 4.4(b)*. The employer and its counsel appealed.

Overview

The employer provided the employee with a laptop computer, which she used to communicate with her attorney about her working conditions and a possible suit against her employer. She returned the laptop after she resigned. After the employee filed suit, the employer hired a computer expert, who retrieved e-mails between the employee and her attorney from the laptop's hard drive. The employer's counsel read the e-mails and used information culled from them during discovery. The trial court held that as the employee was on notice that all e-mails on her computer were the employer's property, they were not privileged. The intermediate appellate court and high court disagreed. The latter held that, under the circumstances, the employee could have reasonably expected that e-mail communications with her lawyer through her personal, password-protected, web-based e-mail account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them. By reading e-mails that were at least arguably privileged and failing to promptly notify the employee about them, the employer's counsel violated *Rule 4.4(b)*.

Outcome
The high court modified the judgment of the intermediate appellate court by removing the

requirement that the case be remanded to the chancery court. It affirmed the judgment as modified and remanded the matter to the trial court to determine what, if any, sanctions should be imposed on the employer's counsel.

LexisNexis® Headnotes

Evidence > Privileges > Attorney-Client Privilege > Elements

HN1[] Attorney-Client Privilege, Elements

The attorney-client privilege is codified at N.J.S.A. § 2A:84A-20, and it appears in the New Jersey Rules of Evidence as N.J.R.E. 504. Under Rule 504, for a communication to be privileged it must initially be expressed by an individual in his capacity as a client in conjunction with seeking or receiving legal advice from the attorney in his capacity as such, with the expectation that its content remain confidential. § 2A:84A-20(1) and (3).

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Attorney-Client Privilege

Evidence > Privileges > Attorney-Client Privilege > Scope

HN2[] Privacy & Security, Attorney-Client Privilege

E-mail exchanges are covered by the attorney-client privilege like any other form of communication.

Governments > Courts > Judicial Precedent

HN3[] Courts, Judicial Precedent

Under the New Jersey Court Rules, unpublished opinions do not constitute precedent and are not to be cited by any court. R. 1:36-3.

Evidence > Privileges > Attorney-Client Privilege > Scope

HN4[] Privileges, Attorney-Client Privilege

There is a close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence.

Evidence > Privileges > Attorney-Client Privilege > Scope

HN5[] Privileges, Attorney-Client Privilege

A client has the right to prevent disclosures by third persons who learn of her communications with her attorney in a manner not reasonably to be anticipated. N.J.R.E. 504(1)(c)(ii).

Evidence > Privileges > Attorney-Client Privilege > Waiver

HN6[] Attorney-Client Privilege, Waiver

A person waives the attorney-client privilege if she, without coercion and with knowledge of her right or privilege, makes disclosure of any part of the privileged matter or consents to such a disclosure made by anyone. N.J.R.E. 530 (codifying N.J.S.A. § 2A:84A-29).

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Attorney-Client Privilege

Evidence > Privileges > Attorney-Client Privilege > Scope

Labor & Employment Law > Employee Privacy > Invasion of Privacy

Business & Corporate Compliance > ... > Computer & Internet Law > Privacy & Security > Company Communications

HN7[] Privacy & Security, Attorney-Client

Privilege

Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy. But employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the attorney-client privilege, even a clearly written company manual--that is, a policy that bans all personal computer use and provides unambiguous notice that an employer can retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system--would not be enforceable.

Computer & Internet Law > Civil Actions > Invasion of Privacy

Legal Ethics > Professional Conduct > Electronic Communications

Legal Ethics > Professional Conduct > General Overview

HN8[] **Civil Actions, Invasion of Privacy**

N.J. R. Prof. Conduct 4.4(b) provides that a lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender. The term "document" includes e-mail or other electronic modes of transmission subject to being read or put into readable form.

Syllabus

(This syllabus is not part of the opinion of the Court. It has been prepared by the Office of the Clerk for the convenience of the reader. It has been neither reviewed nor approved by the Supreme Court. Please note that, in the interests of brevity, portions of any opinion may not have been summarized).

Stengart v. Loving Care Agency, Inc. **(A-16-09)**

Argued December 2, 2009 -- Decided March 30, 2010

RABNER, C.J., writing for a unanimous Court.

This case presents novel questions about the extent to which an employee can expect privacy and confidentiality in e-mails with her attorney, which she sent and received through her personal, password-protected, web-based e-mail account using an employer-issued computer.

This appeal arises out of an employment discrimination lawsuit that plaintiff Marina Stengart filed against her former employer, defendant Loving Care Agency, Inc. Stengart had been provided a laptop computer to conduct company business. From the laptop, she could send e-mails using her company e-mail account; she could also access the Internet through Loving Care's server. **[***2]** Unbeknownst to Stengart, browser software automatically saved a copy of each web page she viewed on the computer's hard drive in a "cache" folder of temporary Internet files. In December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop. Not long after, Stengart left her employment with Loving Care and returned the laptop. In February 2008, she filed the pending complaint.

In anticipation of discovery, Loving Care hired experts to create a forensic image of the laptop's hard drive, including temporary Internet files. Those files contained the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account. At the bottom of the e-mails sent by Stengart's lawyer, a legend warns readers that the information "is intended only for the personal and confidential use of the designated recipient" of the e-mail, which may be a "privileged and confidential" attorney-client communication.

Attorneys from the law firm (the "Firm") representing Loving Care reviewed the e-mails **[***3]** and used the information in discovery. Stengart's lawyer demanded that the e-mails be identified and returned. The Firm disclosed the e-mails but argued that Stengart had no

reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications (Policy). The Policy states that Loving Care may review, access, and disclose "all matters on the company's media systems and services at any time." It also states that e-mails, Internet communications and computer files are the company's business records and "are not to be considered private or personal" to employees. It goes on to state that "occasional personal use is permitted." The Policy specifically prohibits "certain uses of the e-mail system," such as discriminatory or harassing messages.

Stengart's attorney requested the return of the e-mails and disqualification of the Firm. The trial court denied the application, concluding that in light of the Policy, Stengart waived the attorney-client privilege by sending e-mails on a company computer. The Appellate Division reversed, finding that the e-mails were protected by the attorney-client privilege and that, given the Policy's **[***4]** language, an employee could "retain an expectation of privacy" in personal e-mails sent on a company computer. *Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54, 973 A.2d 390 (App.Div.2009)*. The panel also found that Loving Care's counsel had violated *RPC 4.4(b)* by failing to alert Stengart's attorneys that it possessed the privileged e-mails before reading them. The panel remanded for a hearing to determine whether disqualification of the Firm or some other sanction was appropriate. The Court granted Loving Care's motion for leave to appeal and ordered a stay pending the outcome of this appeal. *200 N.J. 204, 976 A.2d 382 (2009)*.

HELD: Under the circumstances, Stengart could reasonably expect that e-mail communications with her lawyer through her personal, password-protected, web-based e-mail account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them. By reading e-mails that were at least arguably privileged and failing to promptly notify Stengart about them, Loving Care's counsel violated *RPC 4.4(b)*.

1. To determine the reasonableness of Stengart's expectation of privacy, the Court first examines the meaning **[***5]** and scope of the Policy. It does not give express notice to employees that messages exchanged on a personal, password-protected, web-based e-mail account are subject to monitoring if company equipment is used. Although the Policy states that Loving Care may review matters on "the company's media systems and services," those terms are not defined. The prohibition of certain uses of "the e-mail system" appears to refer to company e-mail accounts, not personal accounts. The Policy does not warn employees that the contents of personal, web-based e-mails are stored on a hard drive and can be forensically retrieved and read. It also creates ambiguity by declaring that e-mails "are not to be considered private or personal," while also permitting "occasional personal use" of e-mail. (pp. 12-14)

2. The attorney-client privilege encourages free and full disclosure of information from the client to the attorney. To be protected, a communication must initially be expressed by a client in connection with receiving legal advice, with the expectation that its contents remain confidential. The e-mails between Stengart and her lawyer contain a standard warning that their contents are personal and confidential **[***6]** and may constitute attorney-client communications. The subject matter of those messages appears to relate to Stengart's anticipated lawsuit against Loving Care. (pp. 14-15)

3. In this case, the source of the reasonable-expectation-of-privacy standard is the common law tort of "intrusion on seclusion." Under the *Restatement (Second) of Torts*, a person who "intentionally intrudes" upon the "seclusion of another or his private affairs" is liable for invasion of privacy "if the intrusion would be highly offensive to a reasonable person." Reasonableness has both subjective and objective components. Whether an employee has a reasonable expectation of privacy in a particular work setting must be addressed on a case-by-case basis. (pp. 15-17)

4. No reported New Jersey decision offers direct guidance for this case. A Massachusetts decision, *National Economic Research Associates v. Evans*, is most analogous to the facts here. In *Evans*, an employee used a company laptop to communicate with his attorney through his personal, password-protected Yahoo account. The e-mails were automatically stored in a temporary Internet file on the laptop's hard drive and were later retrieved by a forensic expert. **[***7]** A company manual permitted personal use of e-mail, to "be kept to a minimum," but warned that computer resources were the "property of the Company" and that e-mails were "not confidential" and could be read "during routine checks." The court denied the company's request to use the e-mails. The court reasoned that, while the manual warned that e-mails sent on the network could be read, it did not expressly state that the company would monitor the content of e-mail communications made from an employee's personal e-

mail account when they were viewed on a company-issued computer. Also, the company did not warn employees that the content of such e-mails is stored on the hard drive and capable of being read by the company. The court found that the employee had a reasonable expectation of privacy in e-mails with his attorney. (pp. 17-19)

5. In *In re Asia Global Crossing, Ltd.*, a federal bankruptcy court considered whether a trustee could force the production of e-mails sent by company employees to their personal attorneys on the *company's* e-mail system. The court developed a four-part test to measure an employee's expectation of privacy in his e-mail: (1) does company policy ban personal or **[***8]** other use, (2) does the company monitor the use of the employee's e-mail, (3) do third parties have a right of access to the e-mails, and (4) did the company notify the employee, or was the employee aware, of the use and monitoring policies? Because the evidence was "equivocal" about the existence of a corporate policy banning personal use of e-mail and allowing monitoring, the court could not conclude that the employees' use of the company e-mail system eliminated any applicable attorney-client privilege. In applying the *Asia Global* factors, the fact-specific nature of the inquiry affects the outcome. According to some courts, employees have a lesser expectation of privacy when they communicate with an attorney using a company e-mail account as compared to a personal, web-based account. Some courts have found that the existence of a clear policy banning personal e-mails can diminish the reasonableness of a claim to privacy in e-mail messages with the employee's attorney. (pp. 20-23)

6. Under all of the circumstances, Stengart could reasonably expect that e-mails exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, **[***9]** would remain private. By using a personal e-mail account and not saving the password, Stengart had a subjective expectation of privacy. Her expectation was also objectively reasonable in light of the ambiguous language of the Policy and the attorney-client nature of the communications. (p.23-25)

7. In concluding that the attorney-client privilege protects the e-mails, the Court rejects the claim that the attorney-client privilege either did not attach or was waived. The Policy did not give Stengart, or a reasonable person in her position, cause to anticipate that Loving Care would be watching over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account. Similarly, Stengart did not waive the privilege under *N.J.R.E. 530*. She took reasonable steps to keep the messages confidential and did not know that Loving Care could read communications sent on her Yahoo account. (pp. 25-27)

8. Employers can adopt and enforce lawful policies relating to computer use to protect the assets and productivity of a business, but they have no basis to read the *contents* of personal, privileged, attorney-client communications. A policy that provided unambiguous notice **[***10]** that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system, would not be enforceable. (pp. 28-29)

9. The Firm's review and use of the privileged e-mails violated *RPC 4.4(b)*. That *Rule* provides that a "lawyer who receives a document," which includes an e-mail, and who "has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document" and promptly notify and return the document to the sender. Stengart did not leave the e-mails behind; the Firm retained a forensic expert to retrieve e-mails that were automatically saved on the hard drive. To be clear, the Firm did not maliciously seek out attorney-client documents or rummage through personal files. The record does not suggest any bad faith in the way the Firm interpreted the Policy. Instead, while legitimately attempting to preserve evidence, the Firm erred in not setting aside arguably privileged messages once it realized they were attorney-client communications, and failing to notify its adversary or seek court **[***11]** permission before reading further. (pp. 29-30)

10. The matter is remanded to the trial court to decide whether disqualification of the Firm, screening of attorneys, the imposition of costs, or some other remedy is appropriate. In so doing, the court should evaluate the seriousness of the breach in light of the nature of the e-mails, the manner in which they were reviewed and used, and other considerations noted by the Appellate Division. The court should also weigh the need to maintain the highest standards of the profession against a client's right to freely choose his counsel. (pp. 30-32)

The judgment of the Appellate Division is **AFFIRMED AS MODIFIED** and the matter is **REMANDED** to the trial court to determine what, if any, sanctions should be imposed on counsel for Loving Care.

Counsel: *Peter G. Verniero* argued the cause for appellants (*Sills Cummis & Gross* and *Porzio Bromberg & Newman*, attorneys; *Mr. Verniero* and *James M. Hirschhorn*, of counsel; *Mr. Verniero*, *Mr. Hirschhorn*, *Lynne Anne Anderson*, and *Jerrold J. Wohlgemuth*, on the briefs).

Peter J. Frazza argued the cause for respondent (*Budd Larner*, attorneys; *Mr. Frazza* and *David J. Novack*, of counsel; *Mr. Frazza*, *Donald P. Jacobs*, and *Allen L. Harris*, **[***12]** on the briefs).

Marvin M. Goldstein submitted a brief on behalf of *amicus curiae* Employers Association of New Jersey (*Proskauer Rose*, attorneys; *Mr. Goldstein*, *Mark A. Saloman*, and *John J. Sarno*, of counsel and on the brief).

Jeffrey S. Mandel submitted a brief on behalf of *amicus curiae* Association of Criminal Defense Lawyers of New Jersey (*PinilisHalpern*, attorneys).

Richard E. Yaskin submitted a brief on behalf of *amicus curiae* National Employment Lawyers Association of New Jersey (*Mr. Yaskin and Resnick, Nirenberg & Cash*, attorneys; *Mr. Yaskin* and *Jonathan I. Nirenberg*, on the brief).

Allen A. Etish, President, submitted a brief on behalf of *amicus curiae* New Jersey State Bar Association (*Mr. Etish, Stryker, Tams & Dill, Gibbons, and Scarinci Hollenbeck*, attorneys; *Mr. Etish*, *Douglas S. Brierley*, *Fruqan Mouzon*, and *Thomas Hoff Prol*, on the brief).

Judges: JUSTICES LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA-SOTO, and HOENS join in CHIEF JUSTICE RABNER's opinion.

Opinion by: RABNER

Opinion

[*307] **[**654]** Chief Justice RABNER delivered of the opinion of the Court.

In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those **[***13]** and other forms of technology **[**655]** evolve, the line separating business from personal activities can easily blur.

In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.

This case presents novel questions about the extent to which an employee can expect privacy and confidentiality in personal e-mails with her attorney, which she accessed on a computer belonging to her employer. Marina Stengart used her company-issued laptop to exchange e-mails with her lawyer through her personal, password-protected, web-based e-mail account. She later filed an employment discrimination lawsuit against her employer, Loving Care Agency, Inc. (Loving Care), and others.

In anticipation of discovery, Loving Care hired a computer forensic expert to recover all files stored on the laptop including the e-mails, which had been automatically saved on the hard drive. Loving Care's attorneys reviewed the e-mails and used information culled from them in the course of discovery. In response, Stengart's lawyer demanded that communications **[***14]** between him and Stengart, which he considered privileged, be identified and returned. Opposing counsel disclosed the documents but maintained that the company had the right to review them. Stengart then sought relief in court.

[*308] The trial court ruled that, in light of the company's written policy on electronic communications, Stengart waived the attorney-client privilege by sending e-mails on a company computer. The Appellate Division reversed and found that Loving Care's counsel had violated *RPC 4.4(b)* by reading and using the privileged documents.

We hold that, under the circumstances, Stengart could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege that protected them. By reading e-mails that were at least arguably privileged and failing to notify Stengart promptly about them, Loving Care's counsel breached *RPC 4.4(b)*. We therefore modify and affirm the judgment of the Appellate Division and remand to the trial court to determine what, if any, sanctions should be imposed on counsel for Loving Care.

I.

This appeal arises **[***15]** out of a lawsuit that plaintiff-

respondent Marina Stengart filed against her former employer, defendant-appellant Loving Care, its owner, and certain board members and officers of the company. She alleges, among other things, constructive discharge because of a hostile work environment, retaliation, and harassment based on gender, religion, and national origin, in violation of the New Jersey Law Against Discrimination, *N.J.S.A. 10:5-1 to - 49*. Loving Care denies the allegations and suggests they are an attempt to escape certain restrictive covenants that are the subject of a separate lawsuit.

Loving Care provides home-care nursing and health services. Stengart began working for Loving Care in 1994 and, over time, was promoted to Executive Director of Nursing. The company provided her with a laptop computer to conduct company business. From that laptop, Stengart could send e-mails using her company e-mail address; she could also access the Internet and visit websites through Loving Care's server. Unbeknownst to Stengart, certain browser software in place automatically **[**656]** made a copy **[*309]** of each web page she viewed, which was then saved on the computer's hard drive in a "cache" folder of temporary **[***16]** Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive.

On several days in December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop.

Not long after, Stengart left her employment with Loving Care and returned the laptop. On February 7, 2008, she filed the pending complaint.

In an effort to preserve electronic evidence for discovery, in or around April 2008, Loving Care hired experts to create a forensic image of the laptop's hard drive. Among the items retrieved were temporary Internet files containing the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account. [1] Stengart's lawyers represented at oral argument that one e-mail was simply a communication he sent to her, to which she did not respond.

A legend appears at the bottom of the e-mails that Stengart's lawyer sent. It warns readers that

> THE INFORMATION CONTAINED IN THIS EMAIL COMMUNICATION IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENT NAMED ABOVE. This message may be an Attorney-Client communication, and as such is privileged and confidential. If the reader of [2] this message is not the intended recipient, you are hereby notified that **[*310]** you have received this communication in error, and that your review, dissemination, distribution, or copying of the message is strictly prohibited. If you have received this transmission in error, please destroy this transmission and notify us immediately by telephone and/or reply email.

At least two attorneys from the law firm representing Loving Care, Sills Cummis (the "Firm"), reviewed the e-mail communications between Stengart and her attorney. The Firm did not advise opposing counsel about the e-mails until months later. In its October 21, 2008 reply to Stengart's first set of interrogatories, the Firm stated that it had obtained certain information from "e-mail correspondence"--between Stengart and her lawyer--from Stengart's "office computer on December 12, 2007 at 2:25 p.m." In response, Stengart's **[**657]** attorney sent a letter demanding that the Firm identify and return all "attorney-client privileged communications" in its possession. The Firm identified and disclosed the e-mails but asserted **[***19]** that Stengart had no reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications.

---

[1] The record does not specify how many of the e-mails were sent or received during work hours. Loving Care asserts that the e-mails in question were exchanged during work hours through the company's **[***17]** server. However, counsel for Stengart represented at oral argument that four of the e-mails were transmitted or accessed during non-work hours--three on a weekend and one on a holiday. It is unclear, and ultimately not relevant, whether Stengart was at the office when she sent or reviewed them.

[2] In the forensically retrieved version of the e-mails submitted to this Court under seal, the legend is reprinted only up until the location of the footnote in the above text. The **[***18]** retrieved messages also list Stengart's lawyer's full name more than a dozen times and his e-mail address--comprised of the lawyer's first initial, full last name, and the law firm's name--more than three dozen times. Counsel for Loving Care submitted certifications in which they explain that they were aware the e-mails were between Stengart and her lawyer but believed the communications were not protected by the attorney-client privilege for reasons discussed below.

Loving Care and its counsel relied on an Administrative and Office Staff Employee Handbook that they maintain contains the company's Electronic Communication policy (Policy). The record contains various versions of an electronic communications policy, and Stengart contends that none applied to her as a senior company official. Loving Care disagrees. We need not resolve that dispute and assume the Policy applies in addressing the issues on appeal.

The proffered Policy states, in relevant part:

> **[*311]** The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice.
>
> . . . .
>
> E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.
>
> The principal purpose of electronic mail (*e-mail*) is for company business communications. Occasional personal use **[***20]** is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

The Policy also specifically prohibits "[c]ertain uses of the e-mail system" including sending inappropriate sexual, discriminatory, or harassing messages, chain letters, "[m]essages in violation of government laws," or messages relating to job searches, business activities unrelated to Loving Care, or political activities. The Policy concludes with the following warning: "Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment."

Stengart's attorney applied for an order to show cause seeking return of the e-mails and other relief. The trial court converted the application to a motion, which it later denied in a written opinion. The trial court concluded that the Firm did not breach the attorney-client privilege because the company's Policy placed Stengart on sufficient notice that her e-mails would be considered company property. Stengart's request to disqualify the Firm was therefore denied.

The Appellate **[***21]** Division granted Stengart's motion for leave to appeal. The panel reversed the trial court order and directed the Firm to turn over all copies of the e-mails and delete any record of them. *Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54, 973 A.2d 390 (App.Div.2009)*. Assuming that the Policy applied to Stengart, the panel found that "[a]n objective reader could reasonably conclude . . . that not all personal emails are necessarily company property." *Id. at 64, 973 A.2d 390*. In other words, an employee could "retain an expectation of privacy" in personal emails **[*312]** sent on a company computer given the language of the Policy. *Id. at 65, 973 A.2d 390*.

The panel balanced Loving Care's right to enforce reasonable rules for the workplace against the public policies underlying the attorney-client privilege. *Id. at 66, 973 A.2d 390*. The court rejected the notion **[**658]** that "ownership of the computer [is] the sole determinative fact" at issue and instead explained that there must be a nexus between company policies and the employer's legitimate business interests. *Id. at 68-69, 973 A.2d 390*. The panel concluded that society's important interest in shielding communications with an attorney from disclosure outweighed the company's interest in upholding the Policy. **[***22]** *Id. at 74-75, 973 A.2d 390*. As a result, the panel found that the e-mails were protected by the attorney-client privilege and should be returned. *Id. at 75, 973 A.2d 390*.

The Appellate Division also concluded that the Firm breached its obligations under *RPC 4.4(b)* by failing to alert Stengart's attorneys that it possessed the e-mails before reading them. The panel remanded for a hearing to determine whether disqualification of the Firm or some other sanction was appropriate.

We granted Loving Care's motion for leave to appeal and ordered a stay pending the outcome of this appeal.

II.

Loving Care argues that its employees have no expectation of privacy in their use of company computers based on the company's Policy. In its briefs before this Court, the company also asserts that by accessing e-mails on a personal account through Loving Care's computer and server, Stengart either prevented any attorney-client privilege from attaching or waived the privilege by voluntarily subjecting her e-mails to company scrutiny. Finally, Loving Care maintains that its counsel did not violate *RPC 4.4(b)* because the e-mails were left behind on Stengart's company computer--not "inadvertently sent," as per the *Rule*--and the **[*313]** Firm **[***23]** acted in the good faith belief that any privilege had been waived.

Stengart argues that she intended the e-mails with her lawyer to be confidential and that the Policy, even if it applied to her, failed to provide adequate warning that Loving Care would save on a hard drive, or monitor the contents of, e-mails sent from a personal account. Stengart also maintains that the communications with her lawyer were privileged. When the Firm encountered the arguably protected e-mails, Stengart contends it should have immediately returned them or sought judicial review as to whether the attorney-client privilege applied.

We granted amicus curiae status to the following organizations: the Employers Association of New Jersey (EANJ), the National Employment Lawyers Association of New Jersey (NELA--NJ), the Association of Criminal Defense Lawyers of New Jersey (ACDL--NJ), and the New Jersey State Bar Association (NJSBA).

EANJ calls for reversal of the Appellate Division decision. It notes the dramatic, recent increase in the use of non-business-related e-mails at work and submits that, by allowing occasional personal use of company property as a courtesy to employees, companies do not create a reasonable **[***24]** expectation of privacy in the use of their computer systems. EANJ also contends that the Appellate Division's analysis--particularly, its focus on whether workplace policies in the area of electronic communications further legitimate business interests--will unfairly burden employers and undermine their ability to protect corporate assets.

NELA--NJ and ACDL--NJ support the Appellate Division's ruling. NELA--NJ submits that an employee has a substantive right to privacy in her password-protected e-mails, even if accessed from an employer-owned computer, and that an employer's invasion of that privacy right must be narrowly tailored to the employer's **[**659]** legitimate business interests. ACDL--NJ adds that the need to shield private communications from disclosure is amplified when the attorney-client privilege is at stake.

[*314] NJSBA expresses concern about preserving the attorney-client privilege in the "increasingly technology-laden world" in which attorneys practice. NJSBA cautions against allowing inadvertent or casual waivers of the privilege. To analyze the competing interests presented in cases like this, NJSBA suggests various factors that courts should consider in deciding whether the privilege **[***25]** has been waived.

III.

Our analysis draws on two principal areas: the adequacy of the notice provided by the Policy and the important public policy concerns raised by the attorney-client privilege. Both inform the reasonableness of an employee's expectation of privacy in this matter. We address each area in turn.

A.

We start by examining the meaning and scope of the Policy itself. The Policy specifically reserves to Loving Care the right to review and access "all matters on the company's media systems and services at any time." In addition, e-mail messages are plainly "considered part of the company's business . . . records."

It is not clear from that language whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered. The Policy uses general language to refer to its "media systems and services" but does not define those terms. Elsewhere, the Policy prohibits certain uses of "the e-mail system," which appears to be a reference to company e-mail accounts. The Policy does not address personal accounts at all. In other words, employees do not have express notice that messages sent or received on a personal, web-based e-mail account are subject **[***26]** to monitoring if company equipment is used to access the account.

[*315] The Policy also does not warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by Loving Care.

The Policy goes on to declare that e-mails "are not to be considered private or personal to any individual employee." In the very next point, the Policy acknowledges that "[o]ccasional personal use [of e-mail] is permitted." As written, the Policy creates ambiguity about whether personal e-mail use is company or private property.

The scope of the written Policy, therefore, is not entirely clear.

B.

The policies underlying the attorney-client privilege further animate this discussion. The venerable privilege is enshrined in history and practice. *Fellerman v. Bradley, 99 N.J. 493, 498, 493 A.2d 1239 (1985)* ("[T]he attorney-client privilege is recognized as one of 'the oldest of the privileges for confidential

communications.'") (quoting 8 J. Wigmore, *Evidence* § 2290, at 542 (McNaughton rev.1961)). Its primary rationale is to encourage "free and full disclosure of information from the client to the attorney." *Ibid.* That, in turn, benefits the public, which "is well served by sound **[***27]** legal counsel" based on full, candid, and confidential exchanges. *Id. at 502, 493 A.2d 1239*.

HN1[↑] The privilege is codified at *N.J.S.A. 2A:84A-20*, and it appears in the *Rules of Evidence* as *N.J.R.E. 504*. Under the *Rule*, "[f]or a communication to be privileged it must initially be expressed by an individual in his capacity as a client in **[**660]** conjunction with seeking or receiving legal advice from the attorney in his capacity as such, with the expectation that its content remain confidential." *Fellerman, supra, 99 N.J. at 499, 493 A.2d 1239* (citing *N.J.S.A. 2A:84A-20(1)* and *(3)*).

HN2[↑] E-mail exchanges are covered by the privilege like any other form of communication. *See Seacoast Builders Corp. v. Rutgers, 358 N.J. Super. 524, 553, 818 A.2d 455 (App.Div.2003)* **[*316]** (finding e-mail from client to attorney "obviously protected by the attorney-client privilege as a communication with counsel in the course of a professional relationship and in confidence").

The e-mail communications between Stengart and her lawyers contain a standard warning that their contents are personal and confidential and may constitute attorney-client communications. The subject matter of those messages appears to relate to Stengart's working conditions and anticipated lawsuit **[***28]** against Loving Care.

IV.

Under the particular circumstances presented, how should a court evaluate whether Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney?

A.

Preliminarily, we note that the reasonable-expectation-of-privacy standard used by the parties derives from the common law and the Search and Seizure Clauses of both the *Fourth Amendment* and *Article I, paragraph 7 of the New Jersey Constitution.* The latter sources do not apply in this case, which involves conduct by private parties only. [3]

The common law source is the tort of "intrusion on seclusion," which can be found in the *Restatement (Second) of Torts § 652B* (1977). That section provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Restatement, supra, § 652B*. A high threshold must be cleared **[***29]** to assert a **[*317]** cause of action based on that tort. *Hennessey, supra, 129 N.J. at 116, 609 A.2d 11* (Pollock, J., concurring). A plaintiff must establish that the intrusion "would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object." *Restatement, supra, § 652B cmt. d*.

As is true in *Fourth Amendment* cases, the reasonableness of a claim for intrusion on seclusion has both a subjective and objective component. *See State v. Sloane, 193 N.J. 423, 434, 939 A.2d 796 (2008)* (analyzing *Fourth Amendment*); *In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr.S.D.N.Y.2005)* (analyzing common law tort). Moreover, whether an employee has a reasonable expectation of privacy in her particular work setting "must be addressed on a case-by-case basis." *O'Connor v. Ortega, 480 U.S. 709, 718, 107 S. Ct. 1492, 1498, 94 L. Ed. 2d 714, 723 (1987)* (plurality opinion) (reviewing public sector employment).

B.

A number of courts have tested an employee's claim of privacy in files stored on **[**661]** company computers by evaluating the reasonableness of the employee's expectation. No reported decisions in New Jersey offer direct guidance for the facts of this case. [4] In one **[***30]** matter, *State v. M.A., 402 N.J. Super. 353, 954 A.2d 503 (App.Div.2008)*, the Appellate Division found that the defendant had no reasonable expectation of privacy in personal information he stored on a workplace computer under a separate password. *Id. at 369, 954 A.2d 503*. The defendant had been advised

---

[3] In addition, a right to privacy can be found in *Article I, paragraph 1 of the New Jersey Constitution. Hennessey v. Coastal Eagle Point Co., 129 N.J. 81, 95-96, 609 A.2d 11 (1992)*.

[4] ***HN3***[↑] Under our rules, unpublished opinions do not constitute precedent and "are not to be cited by any court." *R. 1:36-3*. As a result, we do not address any unpublished decisions raised by the parties.

that all computers were company property. *Id. at 359, 954 A.2d 503*. His former employer consented to a search by the State Police, who, in turn, retrieved information tied to the theft of company funds. *Id. at 361-62, 954 A.2d 503*. The court reviewed the search in the context of the *Fourth Amendment* and found no basis for the **[*318]** defendant's privacy claim in the contents of a company computer that he used to commit a crime. *Id. at 365-69, 954 A.2d 503*.

Doe v. XYC Corp., 382 N.J. Super. 122, 887 A.2d 1156 (App.Div.2005), likewise did not involve attorney-client e-mails. In *XYC Corp.*, the Appellate Division found no legitimate expectation of privacy in an employee's use of a company computer to access websites containing adult and child pornography. *Id. at 139, 887 A.2d 1156*. In its analysis, **[***31]** the court referenced a policy authorizing the company to monitor employee website activity and e-mails, which were deemed company property. *Id. at 131, 138-39, 887 A.2d 1156*.

Certain decisions from outside New Jersey, which the parties also rely on, are more instructive. Among them, *National Economic Research Associates v. Evans, Mass. L. Rptr. No. 15, at 337 (Mass.Super.Ct. Sept. 25, 2006)[21 Mass. L. Rep. 337]*, is most analogous to the facts here. In *Evans*, an employee used a company laptop to send and receive attorney-client communications by e-mail. In doing so, he used his personal, password-protected Yahoo account and not the company's e-mail address. *Ibid.* The e-mails were automatically stored in a temporary Internet file on the computer's hard drive and were later retrieved by a computer forensic expert. *Ibid.* The expert recovered various attorney-client e-mails; at the instruction of the company's lawyer, those e-mails were not reviewed pending guidance from the court. *Ibid.*

A company manual governed the laptop's use. The manual permitted personal use of e-mail, to "be kept to a minimum," but warned that computer resources were the "property of the Company" and that e-mails were "not confidential" and could **[***32]** be read "during routine checks." *Id. at 338*.

The court denied the company's application to allow disclosure of the e-mails that its expert possessed. *Id. at 337*. The court reasoned,

> Based on the warnings furnished in the Manual, Evans [(the employee)] could not reasonably expect to communicate in confidence with his private attorney if Evans **[*319]** e-mailed his attorney using his NERA [(company)] e-mail address through the NERA Intranet, because the Manual plainly warned Evans that e-mails on the network could be read by NERA network administrators. The Manual, however, did not expressly declare that it would monitor the *content* of Internet communications. . . . Most importantly, the Manual did not expressly declare, or even implicitly suggest, that NERA would monitor the content **[**662]** of e-mail communications made from an employee's personal e-mail account via the Internet whenever those communications were viewed on a NERA-issued computer. Nor did NERA warn its employees that the content of such Internet e-mail communications is stored on the hard disk of a NERA-issued computer and therefore capable of being read by NERA.
>
> [*Id. at 338-39*.]

As a result, the court found the employee's expectation of **[***33]** privacy in e-mails with his attorney to be reasonable. *Id. at 339*.

In *Asia Global, supra*, the Bankruptcy Court for the Southern District of New York considered whether a bankruptcy trustee could force the production of e-mails sent by company employees to their personal attorneys on the *company's* e-mail system. *322 B.R. at 251-52*. The court developed a four-part test to "measure the employee's expectation of privacy in his 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*.]

Because the evidence was "equivocal" about the existence of a corporate policy banning personal use of e-mail and allowing monitoring, the court could not conclude that the employees' use of the company e-mail system eliminated any applicable attorney-client privilege. *Id. at 259-61*.

Both *Evans* and *Asia Global* referenced a formal ethics opinion by the American Bar Association that noted

[*34]** "lawyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [online service provider]." *See id. at 256* (citing ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 413 (1999)); *Evans, supra, 21 Mass. L. Rptr. No. 15, at 339 (same)*.

[*320] Other courts have measured the factors outlined in *Asia Global* among other considerations. In reviewing those cases, we are mindful of the fact-specific nature of the inquiry involved and the multitude of different facts that can affect the outcome in a given case. No one factor alone is necessarily dispositive.

According to some courts, employees appear to have a lesser expectation of privacy when they communicate with an attorney using a company e-mail system as compared to a personal, web-based account like the one used here. *See, e.g.*, *Smyth v. Pillsbury Co., 914 F. Supp. 97, 100-01 (E.D.Pa.1996)* (finding no reasonable expectation of privacy in unprofessional e-mails sent to supervisor through internal corporate e-mail system); *Scott v. Beth Israel Med. Ctr., Inc., 17 Misc. 3d 934, 847 N.Y.S.2d 436, 441-43 (N.Y.Sup.Ct.2007)* (finding no expectation of confidentiality when company e-mail used to send attorney-client messages). **[***35]** *But see Convertino v. U.S. Dep't of Justice, 674 F.Supp.2d 97, 2009 U.S. Dist. LEXIS 115050, *33-34 (D.D.C.2009)* (finding reasonable expectation of privacy in attorney-client e-mails sent via employer's e-mail system). As a result, courts might treat e-mails transmitted via an employer's e-mail account differently than they would web-based e-mails sent on the same company computer.

Courts have also found that the existence of a clear company policy banning personal e-mails can also diminish the reasonableness of an employee's claim to privacy in e-mail messages with his or her attorney. *Compare Scott, supra, 847 **[**663]** N.Y.S.2d at 441* (finding e-mails sent to attorney not privileged and noting that company's e-mail policy prohibiting personal use was "critical to the outcome"), *with Asia Global, supra, 322 B.R. at 259-61* (declining to find e-mails to attorney were not privileged in light of unclear evidence as to existence of company policy banning personal e-mail use). We recognize that a zero-tolerance policy can be unworkable and unwelcome in today's dynamic and mobile workforce and do not seek to encourage that approach in any way.

The location of the company's computer may also **[***36]** be a relevant consideration. In *Curto v. Medical World Communications, Inc.*, **[*321]** 99 *Fed. Empl.* Prac. Cas. (BNA) 298 (E.D.N.Y. May 15, 2006), for example, an employee working from a home office sent e-mails to her attorney on a company laptop via her personal AOL account. *Id. at 301*. Those messages did not go through the company's servers but were nonetheless retrievable. *Ibid.* Notwithstanding a company policy banning personal use, the trial court found that the e-mails were privileged. *Id. at 305*.

We realize that different concerns are implicated in cases that address the reasonableness of a privacy claim under the *Fourth Amendment*. *See, e.g.*, *O'Connor, supra, 480 U.S. at 714-19, 107 S. Ct. at 1496-98, 94 L. Ed. 2d at 721-24* (discussing whether public hospital's search of employee workplace violated employee's expectation of privacy under *Fourth Amendment*); *United States v. Simons, 206 F.3d 392, 397-98 (4th Cir. 2000)* (involving search warrants for work computer of CIA employee, which revealed more than fifty pornographic images of minors); *M.A., supra, 402 N.J. Super. at 366-69, 954 A.2d 503* (involving *Fourth Amendment* analysis of State Police search of employee's computer, resulting in theft charges). **[***37]** This case, however, involves no governmental action. Stengart's relationship with her private employer does not raise the specter of any government official unreasonably invading her rights.

V.

A.

Applying the above considerations to the facts before us, we find that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop.

Stengart plainly took steps to protect the privacy of those emails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in **[*322]** messages to and from her lawyer discussing the subject of a future lawsuit.

In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails

sent via personal accounts can be forensically **[***38]** retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property.

Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which might harm the company in some way. *See* Muick v. Glenacre Elecs., 280 F.3d 741, 742-43 (7th Cir.2002); Smyth, supra, 914 F. Supp. at 98, 101; XYC Corp., supra, 382 N.J. Super. at 136-40, 887 A.2d 1156. They are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy. Our system strives to keep private the very type of conversations that took place here in order to foster probing and honest exchanges.

In addition, the e-mails bear a standard hallmark of attorney-client messages. They warn the reader directly that the e-mails are personal, confidential, and may be attorney-client communications. While a pro forma warning at the end of an e-mail might not, on its own, protect a communication, *see* Scott, supra, 847 N.Y.S.2d at 444, other facts present here raise additional privacy concerns.

Under all of the circumstances, we find that Stengart **[***39]** could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private.

[*323] It follows that the attorney-client privilege protects those e-mails. See Asia Global, supra, 322 B.R. at 258-59 (noting HN4[↑] "close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence"). In reaching that conclusion, we necessarily reject Loving Care's claim that the attorney-client privilege either did not attach or was waived. In its reply brief and at oral argument, Loving Care argued that the manner in which the e-mails were sent prevented the privilege from attaching. Specifically, Loving Care contends that Stengart effectively brought a third person into the conversation from the start--watching over her shoulder--and thereby forfeited any claim to confidentiality in her communications. We disagree.

HN5[↑] Stengart has the right to prevent disclosures by third persons who learn of her communications "in a manner not reasonably to be anticipated." *See* N.J.R.E. 504(1)(c)(ii). **[***40]** That is what occurred here. The Policy did not give Stengart, or a reasonable person in her position, cause to anticipate that Loving Care would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account. *See* Evans, supra, 21 Mass. L. Rptr. No. 15, at 339. The language of the Policy, the method of transmittal that Stengart selected, and the warning on the e-mails themselves all support that conclusion.

Loving Care also argued in earlier submissions that Stengart waived the attorney-client privilege. For similar reasons, we again disagree.

HN6[↑] A person waives the privilege if she, "without coercion and with knowledge of [her] right or privilege, made disclosure of any part of the privileged matter or consented to such a disclosure made by anyone." N.J.R.E. 530 (codifying N.J.S.A. 2A:84A-29). Because consent is not applicable here, we look to whether Stengart either knowingly disclosed the information contained in the e-mails or failed to "take reasonable steps to insure and maintain their **[*324]** confidentiality." [5] Trilogy **[**665]** Commc'ns, supra, 279 N.J. Super. at 445-48, 652 A.2d 1273.

As discussed previously, Stengart took reasonable steps to keep discussions with her attorney confidential: she elected not to use the company e-mail system and relied on a personal, password-protected, web-based account instead. She also did not save the password on her laptop or share it in some other way with Loving Care.

As to whether Stengart knowingly disclosed the e-mails, she certified that she is unsophisticated in the use of computers and did not know that Loving Care could read communications sent on her Yahoo account. Use

---

[5] Because Stengart's conduct satisfies both standards, we need not choose which **[***41]** one governs. *See* Kinsella v. NYT Television, 370 N.J. Super. 311, 317-18, 851 A.2d 105 (App.Div.2004) (noting "different approaches to determining whether the inadvertent disclosure of privileged materials results in a waiver" without adopting global rule) (citing Seacoast, supra, 358 N.J. Super. at 550-51, 818 A.2d 455 and State v. J.G., 261 N.J. Super. 409, 419-20, 619 A.2d 232 (App.Div.1993)); *see also* Trilogy Commc'ns, Inc. v. Excom Realty, Inc., 279 N.J. Super. 442, 445-48, 652 A.2d 1273 (Law Div.1994) (finding attorney's "[i]nadvertent disclosure through mere negligence should not be deemed to abrogate the attorney-client privilege").

of a company laptop alone does not establish that knowledge. Nor **[***42]** does the Policy fill in that gap. Under the circumstances, we do not find either a knowing or reckless waiver.

B.

Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. ***HN7***[] Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of **[*325]** public policy. *See* *Hennessey, supra, 129 N.J. at 99-100, 609 A.2d 11*; *Woolley v. Hoffman-LaRoche, Inc., 99 N.J. 284, 290-92, 491 A.2d 1257 (1985)*; *Pierce v. Ortho Pharm. Corp., 84 N.J. 58, 72-73, 417 A.2d 505 (1980)*. For example, an employee who spends long stretches of the workday getting personal, confidential legal advice from a private lawyer may be disciplined for violating a policy permitting only occasional personal use of the Internet. But employers have no need or basis to read the specific *contents* of personal, privileged, attorney-client communications in **[***43]** order to enforce corporate policy. Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual--that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password-protected e-mail account using the company's computer system--would not be enforceable.

VI.

We next examine whether the Firm's review and use of the privileged e-mails violated *RPC 4.4(b)*. ***HN8***[] The *Rule* provides that "[a] lawyer who receives a document and has reasonable cause to believe that the document was inadvertently sent shall not read the document or, if he or she has begun to do so, shall stop reading the document, promptly notify the sender, and return the document to the sender." According to the ABA Model Rules on which *RPC 4.4(b)* is patterned, the term "'document' includes e-mail or other electronic modes of transmission subject to being read or put into readable form." *Model Rules of Prof'l Conduct R.* 4.4 cmt. 2 (2004).

Loving Care contends that the *Rule* does not apply because Stengart left **[**666]** the e-mails **[***44]** behind on her laptop and did not send them inadvertently. In actuality, the Firm retained a computer forensic expert to retrieve e-mails that were automatically saved on the laptop's hard drive in a "cache" folder of temporary **[*326]** Internet files. Without Stengart's knowledge, browser software made copies of each webpage she viewed. Under those circumstances, it is difficult to think of the e-mails as items that were simply left behind. We find that the Firm's review of privileged e-mails between Stengart and her lawyer, and use of the contents of at least one e-mail in responding to interrogatories, fell within the ambit of *RPC 4.4(b)* and violated that rule.

To be clear, the Firm did not hack into plaintiff's personal account or maliciously seek out attorney-client documents in a clandestine way. Nor did it rummage through an employee's personal files out of idle curiosity. Instead, it legitimately attempted to preserve evidence to defend a civil lawsuit. Its error was in not setting aside the arguably privileged messages once it realized they were attorney-client communications, and failing either to notify its adversary or seek court permission before reading further. There is nothing **[***45]** in the record before us to suggest any bad faith on the Firm's part in reading the Policy as it did. Nonetheless, the Firm should have promptly notified opposing counsel when it discovered the nature of the e-mails. [6]

The Appellate Division remanded to the trial court to determine the appropriate remedy. It explained that a hearing was needed in that regard to consider

> the content of the emails, whether the information contained in the emails would have inevitably been divulged in discovery that would have occurred absent [the Firm's] knowledge of the emails' content, and the nature of the issues that have been or may in the future be pled in either this or the related Chancery action.
>
> [*Stengart, supra, 408 N.J. Super. at 76-77, 973 A.2d 390*.]

We agree. The forensically retrieved version of the e-

[6] The Firm argues that its position was vindicated by the trial court's ruling that the e-mails were not protected by the attorney-client privilege. That argument lacks merit. Stengart still had the right to appeal the trial court's ruling, as she did.

mails submitted to the Court is not easy to read or fully understand in isolation, and no record has yet been developed about the e-mails' full use. For the same **[***46]** reason, we cannot determine how confidential **[*327]** or critical the messages are. In deciding what sanctions to impose, the trial court should evaluate the seriousness of the breach in light of the specific nature of the e-mails, the manner in which they were identified, reviewed, disseminated, and used, and other considerations noted by the Appellate Division. As to plaintiff's request for disqualification, the court should also "balance competing interests, weighing the 'need to maintain the highest standards of the profession' against 'a client's right freely to choose his counsel.'" *Dewey v. R.J. Reynolds Tobacco Co., 109 N.J. 201, 218, 536 A.2d 243 (1988)* (quoting *Gov't of India v. Cook Indus., Inc., 569 F.2d 737, 739 (2d Cir.1978))*.

We leave to the trial court to decide whether disqualification of the Firm, screening of attorneys, the imposition of costs, or some other remedy is appropriate. Under the circumstances, we do not believe a remand to the Chancery judge is required; the matter may proceed before the Law Division judge assigned to the case.

[667]** VII.

For the reasons set forth above, we modify and affirm the judgment of the Appellate Division and remand to the trial court for further proceedings.

JUSTICES **[***47]** LONG, LaVECCHIA, ALBIN, WALLACE, RIVERA-SOTO, and HOENS join in CHIEF JUSTICE RABNER's opinion.

End of Document

United States v. Hamilton

United States Court of Appeals for the Fourth Circuit

October 24, 2012, Argued; December 13, 2012, Decided

No. 11-4847

Reporter
701 F.3d 404 *; 2012 U.S. App. LEXIS 25482 **

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. PHILLIP A. HAMILTON, Defendant-Appellant. ELECTRONIC PRIVACY INFORMATION CENTER, Amicus Supporting Appellant.

Subsequent History: US Supreme Court certiorari denied by *Hamilton v. United States, 133 S. Ct. 1838, 185 L. Ed. 2d 846, 2013 U.S. LEXIS 2811 (U.S., 2013)*

Post-conviction relief denied at *United States v. Hamilton, 2014 U.S. Dist. LEXIS 118250 (E.D. Va., Aug. 22, 2014)*

Prior History: **[**1]** Appeal from the United States District Court for the Eastern District of Virginia, at Richmond. Henry E. Hudson, District Judge. (3:11-cr-00013-HEH-1).

United States v. Hamilton, 778 F. Supp. 2d 651, 2011 U.S. Dist. LEXIS 39091 (E.D. Va., 2011)

Disposition: AFFIRMED.

Core Terms

email, district court, communications, sentencing, gratuity, enhancement, funding, privacy, waive, convictions, budget, marital communication, confidential, stenographer, confidences, preserved, marital

Case Summary

Procedural Posture
A jury convicted defendant of federal program bribery and extortion under color of official right. The convictions arose from charges that, while a state legislator, defendant secured state funding for a public university in exchange for employment by the university. Defendant appealed from the U.S. District Court for the Eastern District of Virginia, challenging his convictions and sentence.

Overview

The district court's conclusion that emails between defendant and his wife were not subject to the marital communications privilege constituted no abuse of discretion because defendant did not take steps to protect the emails in question, even after he was on notice of his employer's policy permitting inspection. The conclusion accorded with the admonition in Wolfle against freely extending the privilege to communications outside of which marital confidences could otherwise reasonably be preserved, and with the principle that one who was on notice that the allegedly privileged material was subject to search could waive the privilege when he made no efforts to protect it. The evidence was sufficient to convict for both bribery and extortion; the government presented evidence of an exchange of money (or gifts) for specific official action, and a jury could have implied intent from the circumstantial evidence. The district court properly instructed the jury on the specific requirements under *18 U.S.C.S. § 666*, including corrupt intent. The district court also properly enhanced defendant's sentence under *U.S. Sentencing Guidelines Manual § 2C1.1(b)(2)* (2011).

Outcome
The court affirmed the judgment of the district court.

LexisNexis® Headnotes

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Conclusions of Law

Criminal Law & Procedure > ... > Standards of

Review > Abuse of Discretion > Evidence

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Findings of Fact

HN1 De Novo Review, Conclusions of Law

An appellate court reviews evidentiary rulings, including rulings on privilege, for abuse of discretion, factual findings as to whether a privilege applies for clear error, and the application of legal principles de novo.

Evidence > ... > Marital Privileges > Confidential Communications > Scope

Evidence > ... > Marital Privileges > Confidential Communications > Waiver

HN2 Marital Privileges, Confidential Communications

Communications between spouses, privately made, are generally assumed to have been intended to be confidential, and hence they are privileged. This is so because marital confidences are regarded as so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails. But, of course, to be covered by the privilege, a communication between spouses must be confidential; voluntary disclosure of a communication waives the privilege.

Evidence > ... > Marital Privileges > Confidential Communications > Scope

HN3 Marital Privileges, Confidential Communications

Because the marital communications privilege suppresses relevant testimony, it should be allowed only when it is plain that marital confidence cannot otherwise reasonably be preserved.

Evidence > ... > Marital Privileges > Confidential Communications > Waiver

HN4 Confidential Communications, Waiver

A party waives the marital communications privilege when he fails to take adequate precautions to maintain confidentiality.

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Sufficiency of Evidence

HN5 De Novo Review, Sufficiency of Evidence

An appellate court upholds a jury verdict based on substantial, even if circumstantial, evidence, viewing the evidence in the light most favorable to the Government. When a defendant challenges the sufficiency of a jury's guilty verdict, he bears a heavy burden.

Criminal Law & Procedure > ... > Bribery > Public Officials > Elements

HN6 Public Officials, Elements

To establish the corrupt intent necessary for convictions for bribery of federal program funds and extortion under color of official right, violations of *18 U.S.C.S. §§ 666(a)(1)(B)* and *1951*, respectively, the Government must present evidence of an exchange of money (or gifts) for specific official action.

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > General Overview

Criminal Law & Procedure > Trials > Jury Instructions > Requests to Charge

HN7 Standards of Review, Abuse of Discretion

To demonstrate an abuse of discretion in refusing to give a jury instruction, a defendant must establish that his proposed instruction was (1) correct; (2) not substantially covered by the court's charge; and (3) dealt with some point in the trial so important, that failure to give the requested instruction seriously impaired the defendant's ability to conduct his defense.

Criminal Law & Procedure > ... > Appeals > Standards of Review > De Novo Review

Criminal Law & Procedure > ... > Appeals > Standards of Review > Plain Error

Criminal Law & Procedure > Sentencing > Sentencing Guidelines > General Overview

HN8 **Standards of Review, De Novo Review**

An appellate court reviews legal interpretations of the Sentencing Guidelines de novo. But when a defendant does not raise an argument in the district court, the court reviews only for plain error.

Criminal Law & Procedure > ... > Standards of Review > Plain Error > Burdens of Proof

Criminal Law & Procedure > ... > Appeals > Standards of Review > Plain Error

HN9 **Plain Error, Burdens of Proof**

To establish plain error, an appealing party must show that an error (1) was made, (2) is plain (i.e., clear or obvious), and (3) affects substantial rights. Moreover, an appellate court may exercise discretion to correct the error only if it seriously affects the fairness, integrity or public reputation of judicial proceedings.

Criminal Law & Procedure > ... > Sentencing Guidelines > Adjustments & Enhancements > General Overview

Criminal Law & Procedure > ... > Bribery > Public Officials > Penalties

HN10 **Sentencing Guidelines, Adjustments & Enhancements**

The Sentencing Guidelines require that a sentencing enhancement for bribery be based on the greater of the payment received or the benefit obtained. *U.S. Sentencing Guidelines Manual § 2C1.1(b)(2)* (2011).

Criminal Law & Procedure > ... > Standards of Review > Plain Error > Burdens of Proof

Criminal Law & Procedure > ... > Appeals > Standards of Review > Plain Error

HN11 **Plain Error, Burdens of Proof**

To succeed on a plain error argument, a defendant must demonstrate that any error affected his substantial rights.

Counsel: ARGUED: Charles B. Lustig, SHUTTLEWORTH, RULOFF, SWAIN, HADDAD & MORECOCK, PC, Virginia Beach, Virginia, for Appellant.

Richard Daniel Cooke, OFFICE OF THE UNITED STATES ATTORNEY, Richmond, Virginia, for Appellee.

ON BRIEF: Lawrence H. Woodward, Jr., SHUTTLEWORTH, RULOFF, SWAIN, HADDAD & MORECOCK, PC, Virginia Beach, Virginia, for Appellant.

Neil H. MacBride, United States Attorney, Alexandria, Virginia, Robert J. Seidel, Jr., Assistant United States Attorney, OFFICE OF THE UNITED STATES ATTORNEY, Norfolk, Virginia, for Appellee.

Marc Rotenberg, Alan Butler, David Jacobs, ELECTRONIC PRIVACY INFORMATION CENTER, Washington, D.C., for Amicus Supporting Appellant.

Judges: Before MOTZ and FLOYD, Circuit Judges, and Catherine C. EAGLES, United States District Judge for the Middle District of North Carolina, sitting by designation. Judge Motz wrote the opinion, in which Judge Floyd and Judge Eagles joined.

Opinion by: DIANA GRIBBON MOTZ

Opinion

[*406] DIANA GRIBBON MOTZ, Circuit Judge:

A jury convicted Phillip A. Hamilton of federal program bribery and extortion under color **[**2]** of official right. The convictions arose from charges that, while a state legislator, Hamilton secured state funding for a public university in exchange for employment by the university. Hamilton appeals, challenging his convictions and sentence. For the reasons that follow, we affirm.

I.

From 1988 to 2009, Hamilton served as a member of the Virginia House of Delegates. Ultimately he became Vice Chairman of the Appropriations Committee, which is responsible for the state budget. While serving as a legislator, he also worked as an administrator and then as a part-time consultant for the Newport News public schools system.

In August 2006, Hamilton arranged to meet with officials from Old Dominion University, a public university located in Norfolk, Virginia, to discuss state funding for a new Center for Teacher Quality and Educational Leadership that Old Dominion wanted to establish. Immediately prior to the meeting, Hamilton and his wife exchanged emails discussing their financial difficulties, and hope that the new Center would employ Hamilton. In their email exchange, Hamilton told his wife that he would "shoot for" a salary of $6,000 per month. Those emails, like all subsequent emails **[**3]** at issue in this case, were sent to or from Hamilton's public school workplace computer, through his work email account.

The Dean of the College of Education at Old Dominion, Dr. William Graves, testified that, after the initial meeting with Hamilton, Old Dominion President Roseann Runte directed the Dean to hire Hamilton, saying, "[t]hat man wants a job, make him director or something." Hamilton emailed his wife that the meeting "went well" and that he had "reinforced" the idea that "if and when an employment opportunity became available," he would like to be compensated "in the area of $6,000 per month." Hamilton also emailed Dean Graves and, after advising the Dean to "keep this under the radar," explained how best to obtain state funding for the Center. In this email, Hamilton further stated that, if funding for the Center was not included in the Governor's budget, "on my own, I will initiate legislation and/or a budget amendment to create such a center."

Four months later, on December 21, Hamilton emailed President Runte, reminding her of his interest in employment with the Center. The same day, Hamilton emailed David Blackburn, Director of Old Dominion's Program for Research and **[**4]** Evaluation in Public Schools, explaining that, because the Governor's budget did not include money for the Center, Hamilton had proposed a budget amendment to secure $1 million for the Center. Hamilton added: "My City retirement is reduced in May 2007. I will need to supplement my current [public school] income . . . by at least an equal amount . . . ." Director Blackburn replied: "Thanks for passing on budget request and specific salary need[.] I believe GA [General Assembly] will fund and you will be on board[.]"

Soon thereafter, Hamilton introduced legislation for the first of two $500,000 appropriations for the Center, both of which ultimately passed. Director Blackburn emailed Hamilton: "Are congratulations **[*407]** in order? Are you our new director?" In response, Hamilton reiterated his salary needs, noting "[o]f course, more than that is always appreciated." Director Blackburn then posted an announcement for the Center Director position, but did not interview any of the three applicants for the position. Instead, Hamilton was selected as Center Director, at a salary of $40,000 per year, even though he had not filed an application for the position. Dean Graves testified that, but for **[**5]** Hamilton's legislative assistance, the Center would not have offered Hamilton the position. Hamilton later suggested "flowing the money" for his Center employment through the school system payroll and generally concealing his position as Director of the Center. Hamilton explained at one point in an email to Blackburn, "looks like they are digging."

On the basis of the above evidence, the Government charged Hamilton with bribery concerning federal program funds in violation of *18 U.S.C. § 666(a)(1)(B) (2006)*, and extortion under color of official right in violation of *18 U.S.C. § 1951 (2006)*. The jury convicted him of both crimes. The district court then sentenced him to 114 months' imprisonment. Hamilton noted a timely appeal.

II.

Hamilton's most substantial appellate argument challenges the district court's admission into evidence of emails he sent to and received from his wife. He maintains that the admission of these emails violated the marital communications privilege. ***HN1***[↑] We review evidentiary rulings, including rulings on privilege, for abuse of discretion, *see NLRB v. Interbake Foods, LLC, 637 F.3d 492, 501 (4th Cir. 2011)*, factual findings as to whether a privilege applies for clear **[**6]** error, and the application of legal principles de novo. *In re Grand Jury Subpoena, 341 F.3d 331, 334 (4th Cir.*

2003).

HN2[] "Communications between . . . spouses, privately made, are generally assumed to have been intended to be confidential, and hence they are privileged." Wolfle v. United States, 291 U.S. 7, 14, 54 S. Ct. 279, 78 L. Ed. 617 (1934); *see also* United States v. Parker, 834 F.2d 408, 411 (4th Cir. 1987) (Powell, J.). This is so because "marital confidences" are "regarded as so essential to the preservation of the marriage relationship as to outweigh the disadvantages to the administration of justice which the privilege entails." Wolfle, 291 U.S. at 14. But, of course, to be covered by the privilege, a communication between spouses must be confidential; "voluntary disclosure" of a communication waives the privilege. Id. at 14-15. The Government maintains that Hamilton waived the marital communications privilege by communicating with his wife on his workplace computer, through his work email account, and subsequently failing to safeguard the emails.

Wolfle, the leading marital communications privilege case to have reached the Supreme Court, provides an analogy useful in resolving Hamilton's privilege claim. **[**7]** In *Wolfle*, the Court held that a defendant's communication with his wife did not come "within the privilege because of [his] voluntary disclosure" of the communication "to a third person, his stenographer." 291 U.S. at 14. The Court explained that, "[n]ormally husband and wife may conveniently communicate without stenographic aid, and the privilege of holding their confidences immune from proof in court may be reasonably enjoyed and preserved without embracing within it the testimony of third persons to whom such communications have been voluntarily revealed." Id. at 16-17. HN3[] Because **[*408]** "[t]he privilege suppresses relevant testimony," it "should be allowed only when it is plain that marital confidence cannot otherwise reasonably be preserved," and "[n]othing in this case suggests any such necessity." Id. at 17.

In Hamilton's case, email has become the modern stenographer. Like the communications to the stenographer in Wolfle's time, emails today, "in common experience," are confidential. *See* id. at 15; *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 413 (1999) (noting that email "pose[s] no greater risk of interception or disclosure than other modes of communication commonly **[**8]** relied upon as having a reasonable expectation of privacy" and so there is generally "a reasonable expectation of privacy in its use").

But just as spouses can "conveniently communicate without" use of a stenographer, they can also "conveniently communicate without" using a work email account on an office computer. *See* Wolfle, 291 U.S. at 16. Therefore, as in *Wolfle*, it is hardly "plain that marital confidence cannot . . . reasonably be preserved" without according the privilege to the spousal communications at issue here. *See* id. at 17. Accordingly, that one may generally have a reasonable expectation of privacy in email, at least before a policy is in place indicating otherwise, does not end our inquiry.

Hamilton ignores this guidance from *Wolfle* and focuses solely on the fact that, in 2006, when he used his workplace email system to send the emails for which he claims privilege, his public school employer had no computer usage policy. This is true, but the school system adopted a computer policy well prior to the 2009 investigation of, and 2011 charges against, Hamilton. The computer policy, as revised in 2008, expressly provides that users have "no expectation of privacy in their **[**9]** use of the Computer System" and "[a]ll information created, sent[,] received, accessed, or *stored* in the . . . Computer System is subject to inspection and monitoring at any time." Moreover, it is undisputed that forms accepting this policy were electronically signed in Hamilton's name, and that Hamilton had to acknowledge the policy by pressing a key to proceed to the next step of the log-on process, every time he logged onto his work computer. The district court concluded that these facts established that Hamilton had waived any privilege he had in the emails.

Hamilton contends that he did not waive the privilege because he "had no reason to believe, at the time he sent and received the emails, that they were not privileged," and he could not waive his privilege retroactively. Amicus, the Electronic Privacy Information Center, adds that it seems "extreme" to "require an employee to scan all archived e-mails and remove any that are personal and confidential every time the workplace use policy changes," when "employees may not even be aware that archived e-mails exist or know where to find them." EPIC Br. at 18.

In an era in which email plays a ubiquitous role in daily communications, **[**10]** these arguments caution against lightly finding waiver of marital privilege by email usage. But the district court found that Hamilton did not take *any* steps to protect the emails in question, even after he was on notice of his employer's policy permitting inspection of emails stored on the system at the employer's discretion. As outlined above, the record

provides ample support for these factual findings.

In similar circumstances, we have held that a defendant did not have an "objectively reasonable" belief in the privacy of files on an office computer after his employer's **[*409]** policy put him "on notice" that "it would be overseeing his Internet use." *United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000)*; *see also In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)* (listing employer's maintenance of relevant usage policy, monitoring of employee email, third-party right of access to email, and employee's awareness of the policy as key factors suggesting no expectation of privacy). Our sister circuits have also made clear that ***HN4***[] a party waives the marital communications privilege when he "fails to take adequate precautions to maintain . . . confidentiality." *See SEC v. Lavin, 111 F.3d 921, 930, 324 U.S. App. D.C. 162 (D.C. Cir. 1997)*; **[**11]** *see also United States v. De La Jara, 973 F.2d 746, 749-50 (9th Cir. 1992)*.

Thus, the district court's conclusion that the emails were not subject to the marital communications privilege constitutes no abuse of discretion. Rather, that conclusion accords with the admonition in *Wolfle* against freely extending the privilege to communications outside of which marital confidences can "otherwise reasonably be preserved," *291 U.S. at 17*, and with the principle that one who is on notice that the allegedly privileged material is subject to search may waive the privilege when he makes no efforts to protect it.

III.

We can more quickly resolve Hamilton's remaining contentions.

A.

First, Hamilton challenges the sufficiency of the evidence. ***HN5***[] We uphold a jury verdict based on substantial, even if circumstantial, evidence, viewing the evidence in the light most favorable to the Government. *United States v. Stewart, 256 F.3d 231, 249 (4th Cir. 2001)*. As Hamilton acknowledges, "[w]hen a defendant challenges the sufficiency of a jury's guilty verdict . . . he bears a heavy burden." Hamilton has not met that burden.

HN6[] To establish the corrupt intent necessary for the convictions at issue here, the Government **[**12]** had to present evidence of "an exchange of money (or gifts) for specific official action." *United States v. Jennings, 160 F.3d 1006, 1014 (4th Cir. 1998)*. The Government did this, offering a broad range of evidence, admittedly much of it circumstantial, indicating that Hamilton used his position as a state legislator to obtain state funds for the Center, in exchange for a paid position at the Center. Hamilton may be correct that "the Government produced no email, or witness, to say that Hamilton *communicated* to any one that he would not support funding for the research center unless he received a job in return." But intent can be implied—and it is the jury's role to make such factual inferences. *See United States v. Engle, 676 F.3d 405, 418 (4th Cir. 2012)*. Thus, we find Hamilton's sufficiency of the evidence argument meritless.

B.

Hamilton next argues that the district court committed reversible error in failing to instruct the jury on the difference between a bribe, which requires intent to engage in a quid pro quo, and a gratuity, which does not require corrupt intent, but only a "payment for or because of some official act." *See Jennings, 160 F.3d at 1013* (internal quotation marks **[**13]** omitted). We review asserted jury instruction errors for abuse of discretion. *United States v. Shrader, 675 F.3d 300, 308 (4th Cir. 2012)*. ***HN7***[] To demonstrate such abuse, Hamilton must establish that his proposed instruction was "(1) correct; (2) not substantially covered by the court's charge; and (3) deal[t] with some point in **[*410]** the trial so important, that failure to give the requested instruction seriously impaired the defendant's ability to conduct his defense." *Id.*

In this case, the district court did not abuse its discretion in refusing to instruct the jury as to a gratuity. Hamilton's suggestion that this refusal could have caused confusion fails, for he concedes that the Government did not pursue a gratuity theory. The court properly instructed the jury on the specific requirements under *§ 666*, including corrupt intent, which might not be required for gratuity. Thus, Hamilton can point to no confusion the jury may have faced as to the intent requirements of *§ 666* and his proposed instruction was "substantially covered by the court's charge."

Nor can Hamilton show that failure to give the requested instruction "seriously impaired" his defense. *See Shrader, 675 F.3d at 308*. Although **[**14]** we have not yet ruled as to whether *§ 666* covers gratuities as well as bribes, *see Jennings, 160 F.3d at 1015*, even if the statute does cover gratuities, failure to instruct on gratuity could not have prejudiced Hamilton in any way. *Section 666* provides no less severe sentence for gratuities; thus instructing the jury as to gratuity would

only have provided an additional ground on which to convict Hamilton. *See 18 U.S.C. § 666*.

C.

Finally, Hamilton asserts two reasons why he believes the district court erred in its application of a fourteen-level sentencing enhancement. ***HN8***[] We review legal interpretations of the Sentencing Guidelines de novo. *United States v. McKenzie-Gude, 671 F.3d 452, 462-63 (4th Cir. 2011)*. But when a defendant does not raise an argument in the district court, we review only for plain error. *United States v. Strieper, 666 F.3d 288, 295 (4th Cir. 2012)*. ***HN9***[] "To establish plain error, the appealing party must show that an error (1) was made, (2) is plain (i.e., clear or obvious), and (3) affects substantial rights." *United States v. Lynn, 592 F.3d 572, 577 (4th Cir. 2010)*. Moreover, we "may exercise . . . discretion to correct the error only if it seriously affects the fairness, **[**15]** integrity or public reputation of judicial proceedings." *Id.* (internal quotation marks omitted).

Hamilton initially argues, as he did in the district court, that in determining the proper sentencing enhancement, the court should have relied on the value of the payment he received—approximately $87,000—rather than the value of the benefit Old Dominion obtained. Yet Hamilton admits that ***HN10***[] the Sentencing Guidelines require that the enhancement be based on the *greater of* the payment received or the benefit obtained — and there is no dispute the benefit to Old Dominion was greater than the payment Hamilton received. *See U.S. Sentencing Guidelines Manual § 2C1.1(b)(2)* (2011). Accordingly, this argument fails.

Hamilton raises, for the first time on appeal, the additional argument that, in calculating his sentencing enhancement, the district court should have determined the benefit to Old Dominion based on the net, rather than the gross, value of the state appropriation Old Dominion obtained. *See U.S.S.G. § 2C1.1* cmt. But, even if the district court did err in calculating the enhancement based on the full value of the first $500,000 payment that Old Dominion received, that error does not provide **[**16]** a basis for reversal on plain error review.

HN11[] To succeed on a plain error argument, a defendant must demonstrate that any error affected his substantial rights, which here required Hamilton to demonstrate that the net benefit received by Old Dominion **[*411]** was $400,000 or less and so merited a lesser sentencing enhancement. *See U.S.S.G. § 2B1.1(b)(1)*. Hamilton made no such showing. Indeed, in imposing the fourteen-level sentencing enhancement, the district court considered only the first $500,000 payment to Old Dominion. But the University actually received, and the district court could have considered, two $500,000 payments. Additionally, Hamilton has not shown that the district court plainly erred if it assumed the entire $500,000 Old Dominion received constituted the net benefit, given that Hamilton offered no evidence of some lesser portion of the $500,000 that was analogous to "profit." *Cf. United States v. Quinn, 359 F.3d 666, 679-80 (4th Cir. 2004)* (involving contracts for for-profit companies).

In sum, Hamilton has not demonstrated that the alleged error was plain or affected his substantial rights.

IV.

Because we find each of Hamilton's claims on appeal to be without merit, we affirm **[**17]** the judgment of the district court.

AFFIRMED

End of Document

Aventa Learning, Inc. v. K12, Inc.

United States District Court for the Western District of Washington

November 8, 2011, Decided; November 8, 2011, Filed

CASE NO. C10-1022JLR

Reporter
830 F. Supp. 2d 1083 *; 2011 U.S. Dist. LEXIS 129928 **

AVENTA LEARNING, INC., et al., Plaintiffs, v. K12, INC., et al., Defendants.

Prior History: *Aventa Learning, Inc. v. K12 Inc., 2011 U.S. Dist. LEXIS 159422 (W.D. Wash., Mar. 27, 2011)*

Core Terms

laptop, email, attorney-client, communications, counterclaims, Earnout, summary judgment motion, motion to dismiss, projections, materials, copies, saved, misrepresentation, waived, summary judgment, confidential, courts, stored, files, electronic communication, individual plaintiff, accessed, calculation, shareholder, denies, risk capital, good faith, privileged, employees, models

Counsel: **[**1]** For Michael J Axtman, James J Benitez, Dr. Ronald P Benitez, Elizabeth A Benitez, Robert E. Harbison, Suzanne M Harbison, Plaintiffs: Michael A. Goldfarb, LEAD ATTORNEY, KELLEY DONION GILL HUCK & GOLDFARB, PLLC, SEATTLE, WA; Christopher M Huck, KELLEY DONION GILL HUCK & GOLDFARB, SEATTLE, WA.

For Aventa Learning, Inc., a Washington corporation, Plaintiff: Christopher M Huck, KELLEY DONION GILL HUCK & GOLDFARB, SEATTLE, WA; Michael A. Goldfarb, KELLEY DONION GILL HUCK & GOLDFARB, PLLC, SEATTLE, WA.

For KC Distance Learning, Inc., a Delaware corporation, Defendant, Counter Claimant: Ronald L Berenstain, Sean C Knowles, PERKINS COIE (SEA), SEATTLE, WA; Sarah J Crooks, PERKINS COIE (OR), PORTLAND, OR.

For K12, Inc, a Delaware corporation, KAYLEIGH SUB TWO, LLC, a Delaware limited liability company, Defendants: Steven P Caplow, DAVIS WRIGHT TREMAINE (SEA), SEATTLE, WA.

For Michael J Axtman, James J Benitez, Counter Defendants: Michael A. Goldfarb, LEAD ATTORNEY, KELLEY DONION GILL HUCK & GOLDFARB, PLLC, SEATTLE, WA; Christopher M Huck, KELLEY DONION GILL HUCK & GOLDFARB, SEATTLE, WA.

Judges: JAMES L. ROBART, United States District Judge.

Opinion by: JAMES L. ROBART

Opinion

[*1089] ORDER ON MOTIONS FOR SUMMARY JUDGMENT, FOR DISMISSAL **[**2]** OF COUNTERCLAIMS, AND FOR PROTECTIVE ORDER

I. INTRODUCTION

Before the court are three motions: (1) Plaintiffs Micheal J. Axtman and James J. Benitez's motion to dismiss Defendant KC Distance Learning, Inc.'s ("KCDL") counterclaims (Dkt. # 58); (2) Defendants K12, Inc. ("K12"), Kayleigh Sub Two LLC, and KCDL's motion for a protective order (Dkt. # 61); and (3) KCDL's motion for summary judgment (Dkt. # 81). K12, Inc. and Kayleigh Sub Two LLC have joined in KCDL's motion for summary judgment. (Joinder (Dkt. # 84).) Having reviewed the motions, and all materials filed in support and opposition thereto, and having heard the oral argument of counsel concerning the motion for summary judgment and the motion to dismiss on November 3, 2011, [1] the court GRANTS IN PART and DENIES IN PART KCDL's motion for summary

[1] No party requested oral argument or a hearing with regard to Defendants' motion for a protective order, and the court deems the declarations and other papers submitted by the parties to be sufficient for purposes of its ruling.

judgment, DENIES Mr. Axtman and Mr. Benitez's motion to dismiss KCDL's counterclaims, [2] and GRANTS Defendants' motion for a protective order.

II. FACTUAL AND PROCEDURAL BACKGROUND

A. Background Related to Defendants' Motion for Summary Judgment

Plaintiff Aventa Learning, Inc. ("Aventa") is a Washington corporation founded in 2002 by Mr. Axtman and Mr. Benitez. (Am. Compl. (Dkt. # 26) ¶¶ 1, 4, 9.) Aventa assists schools in bringing their educational curricula online. (*Id.* ¶ 4.) The individual plaintiffs, Mr. Axtman, Mr. Benitez, Dr. Ronald P. Benitz, Elizabeth A. Benitez, Robert E. Harbison, and Susanne M. Harbison are the sole shareholders in Aventa. (*Id.* ¶ 5.)

Mr. Axtman and Mr. Benitez remain the president and secretary of Aventa, respectively. (Knowles Decl. (Dkt. # 82) Ex. C (Axtman Dep.) at 7:10-77:24.) Prior to cofounding Aventa, Mr. Benitez was employed as a corporate finance analyst at an investment banking firm. (*Id.* Ex. B (Benitez Dep.) at 207:1-5, 207:25-208:2.) In addition, both men were previously employed at Apex Learning, which is an online education company. (*Id.* Ex. B (Benitez **[**4]** Dep.) at 212:16-213:9; Ex. C (Axtman Dep.) at 20:10-18.) At Apex, Mr. Axtman was responsible for creating business projections. (*Id.* Ex. C. at 20:10-18.)

KCDL is a provider of distance learning programs. Pursuant to an Asset Purchase Agreement ("APA"), dated January 10, 2007, KCDL acquired substantially all of the assets of Aventa. (Knowles Decl. Ex. M.) Knowledge Learning Corporation ("KLC") acquired KCDL as part of a larger acquisition of another company. (*Id.* **[*1090]** Ex. A ("Brown Dep.") at 20:7-21:10.) After the acquisition, KLC hired Stephen Brown as the Chief Executive Officer of KCDL with the intent to expand KCDL. (*Id.*) In the fall of 2006, Mr. Brown began negotiating with Mr. Axtman and Mr. Benitez regarding the acquisition of Aventa by KCDL. (*See id.* Ex. H.)

KCDL regularly developed five-year financial projection models as part of its annual budgeting process. (*Id.* Ex. D. (Solis Dep.) at 68:15-24, 71:20-72:10.) The models include projections of revenues by business line, costs, expenses, net income, gross margin, and Earnings Before Interest, Taxes, Depreciation, and Amortization ("EBITDA") for each of the five subsequent fiscal years. (*See id.* Ex. L at KCDL011986.) On October 19, **[**5]** 2006, Mr. Brown responded by email to Aventa's request for KCDL's EBITDA projections, stating that KCDL projected 2009 EBITDA of $16 million and 2011 of $37 million. (*Id.* Ex. I at KCDL001348.) These projections were taken from an August 2006 EBITDA model that reflected an assumption that KCDL would acquire Aventa ("the August 2006 Buy Model"). (*Id.* Ex. A ("Brown Dep.") at 70:18-71:6, 71:10-16; Ex. F at KCDL014499; Ex. G at KCDL034319.)

On November 30, 2006, Mr. Brown emailed Mr. Axtman and Mr. Benitez two five-year models dated October 20, 2006, one reflecting financial projections assuming that KCDL would acquire Aventa'a assets (the "October 2006 Buy Model"), and another reflecting financial projections assuming that KCDL would not. (*Id.* Ex. L.) The October Buy Model contained revenue projections for each of KCDL's lines of business by year from 2007 through 2011 and projected total EBITDA for that period to be $86 million. (*Id.* at KCDL011986.) While the August 2006 Buy Model projected EBITDA for 2009 and 2011 to be $16 million and $37 million, respectively, the October 2006 Buy Model projected EBITDA for 2009 and 2011 to be $12 million and $41 million, respectively. (Knowles Decl. **[**6]** Ex. I at KCDL001348; Ex. L at KCDL011986.) Nevertheless, Mr. Brown told Mr. Axtman that the numbers changed only because Mr. Brown had incorporated the new Aventa numbers (which Mr. Axtman and Mr. Benitez had previously provided) into the October 2006 Buy Model. (*See* Goldfarb Decl. (Dkt. # 86) Ex. F (Axtman Dep.) at 139:18-143:11.)

On January 10, 2007, KCDL, Aventa and the individual Plaintiffs executed the APA. (*Id.* Ex. N.) The APA provides consideration to Aventa for the sale of its assets to KCDL, as follows: (1) $2.34 million at closing; (2) the "Aventa Earnout," worth up to $3.3 million, based primarily on the 2007 performance of Aventa's assets; and (3) the "Additional Earnout," a future payment equal to "six percent (6%) of the Assumed Equity Value" of KCDL at a certain future point. (*Id.* at KCDL115629-34; Axtman Decl. (Dkt. # 87) Ex. H (APA) § 2.03(c)(i).) The **[**7]** Assumed Equity Value for calculating the Additional Earnout was to be derived by taking KCDL's trailing 12-month period EBITDA and applying a multiplier that increased based on the number of years that Mr. Axtman and Mr. Benitez served as senior

[2] On November 2, 2011, **[**3]** Defendants voluntarily dismissed counterclaims four and five for breach of the duty of loyalty and for misrepresentation, respectively. (Dkt. # 100.) Accordingly, the court denies Plaintiffs' motion to dismiss these two counterclaims as moot.

executives of KCDL after the transaction. (Knowles Decl. Ex. N at PLTF000051-53.)

Aventa received $2.34 million at closing and $3.3 million pursuant to the Aventa Earnout in 2008. (Knowles Decl. Ex. C (Axtman Dep.) at 166:16-18, 167:9-15; Ex. B (Benitez Dep.) at 147:23-148:3, 148:13-149:4.) KCDL has place an additional $1.7 million in escrow, representing its calculation of the Additional Earnout, pending resolution of this lawsuit. (Knowles Decl. ¶¶ 23, 25.) Further, in connection with the **[*1091]** APA, or about January 12, 2007, Mr. Axtman and Mr. Benitez each executed an employment agreement with KCDL. (Answer (Dkt. # 55) ¶ 13.)

On February 15, 2007, Mr. Axtman and Mr. Benitez received an updated 5-year model dated February 9, 2007 ("the February 2007 Model"). (Knowles Decl. Exs. O, P; C (Axtman Dep.) 181:16-25; Ex. B (Benitez Dep.) 153:4-16.) In this model, KCDL's total projected EBITDA for the five-year period from 2007 through 2011 was $45 million **[**8]** (Knowles Decl. Ex. P at KCDL020018-9), which was significantly less than the $86 million projected EBITDA total for the same period reflected in the October 2006 Buy Model (*id.* Ex. L at KCDL011986).

Shortly after receiving the February 2007 Model, Mr. Axtman testifies that he spoke with Mr. Brown who reassured him that the numbers in the February 2007 Model were artificially low, and that the accurate model was still the "October 2006 Buy Model." (Goldfarb Decl. (Dkt. # 86) Ex. F (Axtman Decl.) at 184:5-189:8.) Mr. Axtman also passed Mr. Brown's reassurances onto Mr. Benitez. (*Id.* at 185:19-23; *see also* Axtman Decl. Ex. F at KCDL019950 (describing February 2007 Model to Mr. Benitez as "a sandbag.")

As contemplated in the APA, immediately after the asset purchase closed, Mr. Axtman and Mr. Benitez joined KCDL as Vice Presidents in charge of KCDL's Aventa Learning business line. (Knowles Decl. Ex. C (Axtman Dep.) 170:11-24; Ex. B. (Benitez Dep.) 150:24-151:1.) Mr. Axtman and Mr. Benitez immediately became members of the senior executive team and participated in weekly senior staff meetings with Mr. Brown and other senior executives. (*Id.* Ex. C (Axtman Dep. at 171:1-20); Ex. B. (Benitez **[**9]** Dep.) at 151:2-19; Ex. A. (Brown Dep.) at 262:8-263:12.) Mr. Axtman and Mr. Benitez also became involved in other aspects of KCDL's business. They prepared financial projections and 5-year models and participated in KCDL's budgeting process. (*Id.* Ex. A (Brown Dep.) 263:13-264:3, 265:23-266:7, 268:16-24; Ex. Q; Ex. C (Axtman Dep.) 195:1-196:14; Ex. B (Benitez Dep.) at 179:12-180:6, 187:11-21; Ex. D (Solis Dep.) 245:20-246:10.) In October 2008, Mr. Axtman joined KCDL's Board of Directors. (*Id.* Ex. C (Axtman Dep.) 205:8-25.) In early 2009, Mr. Axtman became the head of the iQ Academies business line at KCDL. (*Id.*)

On July 26, 2010, K12 announced that it had purchased KCDL. (Am. Compl. ¶ 39.) The sale of KCDL constituted a "change of control" transaction under the APA allowing KCDL to elect to pay the Additional Earnout. (Knowles Decl. ¶ 23; Ex. M at KCDL115633.) Aventa disputed KCDL's calculation and demanded access to KCDL's books, records, and facilities. (*Id.* ¶ 24.) On January 19, 2011, KCDL paid $1.7 million as the Additional Earnout payment into an escrow account pending resolution of this lawsuit. (*Id.* ¶¶ 23, 25.) On March 14, 2011, KCDL provided Aventa with its response to the dispute, **[**10]** as well as approximately 50,000 pages of records. (*Id.* ¶ 26.)

Plaintiffs initiated this lawsuit on June 2, 2010. Plaintiffs allege violation of the Washington State Securities Act ("WSSA"), *RCW 21.20.010 et seq.* (Am. Compl. ¶¶ 43-50), the tort of misrepresentation (*id.* ¶¶ 51-60), breach of the implied covenant of good faith and fair dealing (*id.* ¶¶ 61-66), a claim for declaratory relief (*id.* ¶¶ 67-69), and entitlement to equitable relief such as a constructive trust over Aventa's assets, an injunction, or an accounting (*id.* ¶¶ 70-74). Defendants have moved for summary judgment with regard to all of Plaintiffs' claims. (SJ Mot. (Dkt. # 81).)

[*1092] B. Background Related to Motion to Dismiss

In their answer to Plaintiffs' amended complaint, Defendants assert counterclaims against Mr. Axtman and Mr. Benitez. (KCDL Answer (Dkt. # 55) at 13-22, ¶¶ 1-69 (Counterclaims).) Defendants' allegations arise in connection with the employment agreements executed by Mr. Axtman and Mr. Benitez, and their eventual separation from KCDL. (*Id.* ¶¶ 13-26.) Defendants allege that the employment agreements at issue contained loyalty, non-compete, and non-interference clauses. (*Id.* ¶¶ 14-17.) Defendants also allege that **[**11]** the employment agreements required Mr. Axtman and Mr. Benitez to return all property, records, and other files at the end of their employment that Mr. Axtman or Mr. Benitez had prepared for or received from KCDL during their employment. (*Id.* ¶ 18.) In addition to his employment agreement, Defendants allege that Mr. Axtman executed a separation agreement with KCDL and KCL. (*Id.* ¶¶ 19-22.)

Defendants allege that, prior to and following his separation from KCDL, Mr. Axtman formed and promoted a new company to compete with KCDL, that Mr. Axtman interfered with KCDL's clients, and that he improperly accessed proprietary information belonging to KCDL. (*Id.* ¶¶ 23-26.) They also allege the Mr. Benitez improperly accessed KCDL's proprietary information. (*Id.* ¶ 26.)

Based on these factual allegations, Defendants assert six counterclaims. Defendants assert that both Mr. Axtman and Mr. Benitez breached their employment agreements with KCDL. (*Id.* ¶¶ 27-34, 40-45.) They assert that Mr. Axtman breached his separation agreement with KCDL by copying, deleting, and destroying records and proprietary information that were on the KCDL laptop that was in his possession following the termination of his work **[**12]** relationship with KCDL. (*Id.* ¶¶ 35-39.) They also allege that both Mr. Axtman and Mr. Benitez breached their duty of loyalty to KCDL (*id.* ¶¶ 46-54), committed the tort of misrepresentation (*id.* ¶¶ 55-63), and converted KCDL's property by accessing, copying, downloading, deleting or erasing KCDL's electronic records following the termination of their employment (*id.* ¶¶ 64-69). Plaintiffs have moved to dismiss each of these counterclaims. (Mot. to Dismiss (Dkt. # 58).)

C. Background Related to Motion for Protective Order

As a part of the APA, both Mr. Axtman and Mr. Benitez signed employment agreements with KCDL. (KCDL Answer at 14, ¶ 13 (Counterclaims).) [3] KCDL subsequently issued both men laptop computers. (Axtman Decl. re: P.O. (Dkt. # 68) ¶ 6; Benitez Decl. re: P.O. (Dkt. # 69) ¶ 6.) Both men transferred privileged attorney-client communications that had been created prior to their employment **[*1093]** with KCDL onto their new laptop computers. (*See* Axtman Decl. re: P.O. ¶¶ 3-4, 8-9; Benitez Decl. re: P.O. 3-4, 8-9.) Both men have testified that they stored these files locally on their laptops, and did not believe that their local files were transferred to KCDL's or KLC's servers. [4] (Axtman **[**13]** Decl. re: P.O. ¶ 12; Benitez Decl. re: P.O. ¶ 12.) Both men also continued to produce attorney-client privileged communications in the form of emails on their work laptops after execution of the APA and the commencement of their employment at KCDL. (*Id.*)

KLC performs the human resources function for KDLC. [5] (1st Keegan Decl. (Dkt. # 63) ¶ 2.) This function includes administration of all benefits, employer relations, and policy promulgation. (*Id.*) KLC also provides technology services for KCDL, including email. (*Id.*)

KLC has an Employee Handbook governing it and its subsidiaries and affiliates that contains an Electronic Communications Policy that provides, in part:

> All resources used for electronic communications are KLC property and should generally be used only for KLC business.
> * * *
>
> Electronic communications are not private. KLC reserves the right to access, search, inspect, monitor, record, and disclose any file or stored communication, with **[**15]** or without notice to the employee, at any time for any reason to ensure that such communications are being used for legitimate business reasons. Deleted e-mail messages may also be restored from the system.

(1st Keegan Decl. ¶ 3, Ex. 2 at 21.) [6] KLC regularly

[3] Defendants now assert that "[Mr.] Benitez and [Mr.] Axtman were employed by KLC and assigned to KCDL." (Mot. for P.O. (Dkt. # 61) at 2 (citing 1st Keegan Decl. (Dkt. # 63) ¶ 2).) Both Mr. Benitez and Mr. Axtman deny that they were ever employed by KLC, and insist that they were only employed by KLC's subsidiary KCDL. (Axtman Decl. re: P.O. (Dkt. # 68) ¶5; Benitez Decl. re: P.O. (Dkt. # 69) ¶ 5; *see generally* Surreply (Dkt. # 74).) Indeed, Mr. Axtman and Mr. Benitez have moved (as part of their sur-reply) to strike portions of Defendants' reply that that asserts that Mr. Axtman's and Mr Benitez's employment agreements with KCDL did not accurately reflect their employer or relationship with KCDL. (Sur-reply at 2.) The court, however, does not believe that the dispute is material for purposes of this motion, because it is undisputed that "KLC performed the complete human resources function for KCDL, including administration of all benefits, **[**14]** employee relations, and policy promulgation." (1st Keegan Decl. (Dkt. # 63) ¶ 2.)

[4] Despite this belief, some of these materials were in fact transferred at some point onto Defendants' servers. (*See* P.O. Mot. (Dkt. # 61) at 1; P.O. Reply (Dkt. # 70) at 4.)

[5] Although Mr Axtman and Mr. Benitez both deny that they were ever employed by KLC, neither has disputed that KLC performed the human services function for KDLC during the period of their employment, including the promulgation of company policies.

[6] KLC also has a second, more detailed, policy entitled the Electronic Communications and Computer Usage Policy. (1st Keegan Decl. ¶ 4, Ex. 3.) This policy is set forth on KLC's

enforces this policy. (*Id.* ¶ 5.) Employees' laptops have been reviewed by the company, and employees have been disciplined, including having their employment terminated, for violations. (*Id.*)

Defendants have produced testimony that it is the pattern and practice of KLC to provide all employees, including those assigned to its affiliates and subsidiaries, with copies of the Employee Handbook upon hiring, and that (in accord with this policy and practice) Mr. Axtman and Mr. Benitez would have received this Handbook upon the commencement of their employment. **[*1094]** (*Id.* ¶ 6; *see also* 2nd Keegan Decl. (Dkt. # 72) ¶ 3.)

Mr. Axtman and Mr. Benitez, however, have both testified that to the best of their knowledge they never received copies of KLC's employee handbook, and were not aware of KLC's policies prior to their transfer of privileged files onto their KCDL laptops. (Axtman Decl. re: P.O. ¶ 13; Benitez Decl. **[**17]** re: P.O. ¶ 13.) In addition, Defendants have not produced copies of "Employee Acknowledgements" signed by either Mr. Axtman or Mr. Benitez concerning their receipt of KLC's policies or its handbook.

Nevertheless, Defendants have produced a copy of a template letter from Mr. Brown that was sent to all Aventa Employees who were being retained by KCDL following execution of the APA by Aventa and KCDL. (*See* 1st Keegan Decl. ¶ 6, Ex. 4.) The letter specifically instructs the new KCDL employees from Aventa to review the employee handbook. (*Id.* Ex. 4 at 2.) Neither Mr. Axtman nor Mr. Benitez specifically deny receiving a copy of this letter. (*See generally* Benitez Decl. & Axtman Decl.) Further, the letter directs the new employees to contact Mr. Axtman with any questions concerning the transition. (*Id.* Ex. 4 at 3.)

Despite Mr. Axtman's and Mr. Benitez's inability to specifically recall receiving a copy of the KLC Handbook (*see* Axtman Decl. re: P.O. ¶ 13; Benitez Decl. re: P.O. ¶ 13), there can be no doubt that Mr. Benitez received a copy by at least November 19, 2007, and that both men received a copy by February 23, 2009. Defendants have produced a copy of a November 19, 2007 email to a new **[**18]** hire at KCDL, on which Mr. Benitez was copied, and which attaches a copy of the KLC Handbook. (2nd Keegan Decl. Ex. 1.) The email describes the KLC Handbook as the employee handbook, and specifically asks the new KCDL hire to review it with regard to company policies. (*Id.*) Mr. Benitez does not specifically deny receiving this email. (*See generally* Benitez Decl.) Further, Defendants have produced a copy of a February 23, 2009 email addressed to both Mr. Axtman and Mr. Benitez, which also attaches the KLC Handbook. (2nd Keegan Decl. Ex. 2.) Neither Mr. Axtman nor Mr. Benitez has specifically denied receiving this email. (*See generally* Axtman Decl. & Benitez Decl.)

After his employment with KCDL ended, Mr. Axtman returned his laptop to the company in late 2009. He did not, however, make a claim with regard to any privileged documents contained on his laptop until May 12, 2011, nearly a year and half after he relinquished the laptop to the company. (Crooks Decl. (Dkt # 62) ¶¶ 7-8, Ex. 5.)

Mr. Benitez was terminated on September 28, 2010, but initially refused to return his company laptop. He asserted that he had saved years worth of privileged communications on his laptop. Counsel for Defendants **[**19]** asserted that Mr. Benitez had no expectation of privacy with regard to contents on the laptop, and insisted that he return it because it was company property. (Crooks Decl. Ex. 1.) Mr. Benitez ultimately returned the laptop on January 21, 2011 (*id.* ¶ 3), but only after Defendants had agreed to a "review protocol" that would require Defendants to sequester the asserted privileged material prior to reviewing the remainder of the laptop's contents (*id.* Ex. 2).

The emails or other documents at issue in this motion include asserted privileged communications (1) from before execution of the APA in January 2007, which Mr. Benitez and Mr. Axtman saved on their KCDL laptops in a folder in Microsoft Outlook (which was a program provided by the company), (2) from Mr. Axtman's and Mr. Benitez's web-based personal email **[*1095]**

---

intranet site, which is known as KLCentral. (2nd Keegan Decl. (Dkt. # 72) ¶ 4.) Defendants provided testimony that Mr. Benitez and Mr. Axtman had access and were granted logins to KLCentral, and as senior managers were expected to know the contents of company policies that were set forth on KLCentral. (*Id.* ¶¶ 4-5.) Nevertheless, both Mr. Axtman and Mr. Benitez testified that they did not use or access KLCentral, and were not aware of and did not review the Electronic Communications and Computer Usage Policy on KLCentral. (Axtman Decl. re: P.O. ¶ 14; Benitez Decl. re **[**16]** P.O. ¶ 14.) In addition, Mr. Benitez testified that he "do[es] not believe [he] was even provided a username and password to access KLCentral." (*Id.*) As a result of this factual dispute concerning Mr. Benitez's ability to even access KLCentral, the court does not consider the Electronic Communications and Computer Usage Policy in its analysis of the privilege issues, but rather confines its analysis to the Electronic Communications Policy contained within the company handbook.

accounts, which they saved and imported into Microsoft outlook on their KCDL laptops, and (3) from Mr. Axtman's and Mr. Benitez's post-acquisition work email accounts, which they saved in Microsoft Outlook on their KCDL laptops. In addition, Plaintiffs assert that some of these privileged materials may be residing on Defendants' computers and servers. Defendants seek a protective **[**20]** order from the court declaring that these documents are not privileged and/or that the privilege has been waived.

III. ANALYSIS

A. Motion for Summary Judgment

1. Standards

Defendants have moved for summary judgment of all claims against them in Plaintiffs' amended complaint. (*See* SJ Mot.) Summary judgment is appropriate if the evidence, when viewed in the light most favorable to the non-moving party, demonstrates "that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." *Fed. R. Civ. P. 56(a)*; *see Celotex Corp. v. Catrett, 477 U.S. 317, 322, 106 S. Ct. 2548, 91 L. Ed. 2d 265 (1986)*; *Galen v. Cnty. of L.A., 477 F.3d 652, 658 (9th Cir. 2007)*. The moving party bears the initial burden of showing there is no genuine issue of material fact and that he or she is entitled to prevail as a matter of law. *Celotex, 477 U.S. at 323*. If the moving party meets his or her burden, then the non-moving party "must make a showing sufficient to establish a genuine dispute of material fact regarding the existence of the essential elements of his case that he must prove at trial" in order to withstand summary judgment. *Galen, 477 F.3d at 658*.

2. Statute of Limitations

Defendants assert **[**21]** that the three-year statute of limitations has run with regard to Plaintiffs' WSSA and misrepresentation claims. They argue that Plaintiffs' claims under the WSSA and for misrepresentation are based on their allegations that the financial projections and EBITDA calculations contained in the October 2006 Buy Model were false or misleading. They further assert, however, that Mr. Axtman and Mr. Benitez had notice of their claims no later than February 2007, and therefore, Plaintiffs' claims, which were filed in June 2010, are time-barred.

There is no dispute that Mr. Axtman and Mr. Benitez received three sets of financial projections between October 2006 and February 2007 — all of which are dramatically different from one another. Defendants assert that the receipt of these varying financial projections and EBITDA calculations placed Plaintiffs on notice that the October 2006 Buy Model was false or misleading. The statute of limitations for a WSSA claim is three years from the date on which the violation was or could have been discovered in the exercise of reasonable care. *RCW 21.20.430(4)(b)*. In addition, causes of action for misrepresentation must be brought within three years and accrue **[**22]** when the aggrieved party has discovered the facts constituting misrepresentation. *See RCW 4.16.080(4)* (three-year statute of limitations for fraud); *Young v. Savidge, 155 Wn. App. 806, 230 P.3d 222, 230 (Wash. Ct. App. 2010)* (applying statute of limitations from *RCW 4.16.080(4)* to claims for misrepresentation).

A cause of action accrues when the plaintiff knew or should have known all the facts underlying the essential elements of the action. *Reichelt v. Johns-Manville Corp., 107 Wn.2d 761, 733 P.2d 530, 534 (Wash. 1987)*; *1000 Virginia Ltd. Partnership v. Vertecs Corp., 158 Wn.2d 566, 146 P.3d 423, 428 (Wash. 2006)*. In Washington, the general rule is that when a plaintiff is placed on notice by some appreciable harm occasioned by another's wrongful conduct, the plaintiff must make further diligent inquiry **[*1096]** to ascertain the scope of the actual harm. *Green v. A.P.C., 136 Wn.2d 87, 960 P.2d 912, 916 (Wash. 1998)*. It is not necessary for the plaintiff to be aware that he has a legal cause of action. *Reichelt, 733 P.2d at 534-35*. But an injured plaintiff who reasonably suspects that a specific wrongful act has occurred is on notice that legal action must be taken. *Id. at 534*. The plaintiff is charged with what a reasonable inquiry would have discovered. **[**23]** *Green, 960 P.2d at 916*.

Washington, however, allows equitable tolling of the statute of limitations when justice requires. *Thompson v. Wilson, 142 Wn. App. 803, 175 P.3d 1149, 1154 (Wash. Ct. App. 2008)*; *see also Stueckle v. Sceva Steel Buildings, Inc., 1 Wn. App. 391, 461 P.2d 555, 557 (Wash. Ct. App. 1970)* ("The statute of limitations may be tolled by the concealment of material facts, misrepresentation, or a promise to pay in the future."). "Equitable tolling is permitted where there is evidence of bad faith, deception or false assurances by the defendant and the exercise of diligence by the plaintiff." *Thompson, 175 P.3d at 1154*; D. DeWolf, K. Allen & D. Caruso, 25 Wash. Prac. § 16.19 (2010) ("Washington recognizes an equitable tolling principle. . . .").

Plaintiffs assert that after receiving the October 2006 Buy Model, Mr. Brown reassured them that the differences between the projections in this model and the projections in the August 2006 Buy Model were due to the inclusion of the new Aventa numbers into the October 2006 Buy Model. (*See* Goldfarb Decl. Ex. F (Axtman Dep.) at 139:18-143:11.) Plaintiffs further contend that after receiving the February 2007 Model, Mr. Brown again reassured them that the numbers in **[**24]** the February 2007 Model were artificially low, and that the accurate model was still the October 2006 Buy Model. (*Id.* at 184:5-189:8.) On this summary judgment motion, the court must view the evidence in the light most favorable to Plaintiffs. Applying this standard, and taking into account the reassurances issued by Mr. Brown, the court cannot conclude that reasonable minds could not differ as to the commencement of the running of the statute of limitation in February 2007 or the tolling of the statute by Mr. Brown's reassurances concerning the differences in the various models Plaintiffs' received. These are material issues of fact which must be reserved for the jury. Accordingly, the court denies Defendants' motion for summary judgment with regard to the statute of limitations.

3. Plaintiffs' WSSA Claim

Defendants contend that neither the sale of Aventa's assets to KCDL nor the Additional Earnout under the APA constitute a security under Washington law, and therefore, Plaintiffs' WSSA claim must fail. (SJ Mot. at 12-18.) Although the court previously rejected Defendants' argument in this regard in the context of their motion to dismiss (*see* Order (Dkt. # 54) at 11-18), Defendants **[**25]** have raised the issue again here on summary judgment.

There are two essential elements to a WSSA claim: "(1) a fraudulent or deceitful act committed (2) in 'connection with the offer, sale or purchase of any security.'" *Kinney v. Cook, 159 Wn.2d 837, 154 P.3d 206, 209-10 (Wash. 2007)* (quoting *RCW 21.20.010*). [7] It is the second prong of this **[*1097]** test that is once again at the heart of the present dispute.

WSSA broadly defines a "security," in pertinent part, as follows:

> "Security" means any . . . stock; . . . investment contract; investment of money or other consideration in the risk capital of a venture with the expectation of some valuable benefit to the investor where the investor **[**26]** does not receive the right to exercise practical and actual control over the managerial decisions of the venture; . . . or, in general, any interest or instrument commonly known as a "security". . . .

RCW 21.20.005(12)(a). "[T]he definition of security 'embodies a flexible rather than a static principle, one that is capable of adaptation to meet the countless and variable schemes devised by those who seek the use of the money of others on the promise of profits.'" *Cellular Eng'g, 820 P.2d at 946, 118 Wn.2d 16* (quoting *SEC v. W.J. Howey, 328 U.S. 293, 299, 66 S. Ct. 1100, 90 L. Ed. 1244 (1946)*). However, "[t]he essential attribute of a security is an investment 'premised on a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others.'" *Firth v. Lu, 103 Wn. App. 267, 12 P.3d 618, 623 (Wash. Ct. App. 2000)* (quoting *United Housing Found. v. Forman, 421 U.S. 837, 852, 95 S. Ct. 2051, 44 L. Ed. 2d 621 (1975)*).

Whether or not an investment scheme or contract constitutes a security is a question of law. *Swartz v. Deutsche Bank, No. C03-1252MJP, 2008 U.S. Dist. LEXIS 36139, 2008 WL 1968948, at *22 (W.D. Wash. May 2, 2008)* (citing *De Luz Ranchos Inv. Ltd. v. Coldwell Banker & Co., 608 F.2d 1297, 1299-1301 (9th Cir. 1979)*); *see also Haberman v. Washington Pub. Power Supply Sys., 109 Wn.2d 107, 744 P.2d 1032, 1047 (Wash. 1987)* **[**27]** ("[W]e note that federal courts consistently determine as a matter of law whether investment schemes are securities.") (citing cases)). [8] In

---

[7] It is unlawful for any person, in connection with the offer, sale or purchase of any security, directly or indirectly:

> (1) To employ any device, scheme, or artifice to defraud;
>
> (2) To make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they are made, not misleading; or
>
> (3) To engage in any act, practice, or course of business which operates or would operate as a fraud or deceit upon any person.

RCW 21.20.010.

[8] ". . . Washington courts have looked to federal law in determining whether a transaction involves a 'security.'" *Shinn v. Thrust IV, Inc., 56 Wn. App. 827, 786 P.2d 285, 298 (Wash. Ct. App. 1990)* (citing *State v. Philips, 108 Wn.2d 627, 741 P.2d 24, 28 (Wash. 1987)*); *see also RCW 21.20.900* (policy of the WSSA is to make uniform the law and to coordinate its

determining whether a transaction constitutes the sale of a security, the court should consider substance over form, consistent with the purpose of the act to protect the investing public. Cellular Eng'g, 820 P.2d at 946.

Defendants assert that the issue of whether the APA or the Additional Earnout is a security should be analyzed under the test for an "investment contract" as stated in Howey, 328 U.S. at 301. (SJ Mot. at 13.) Washington courts apply a modified *Howey* test which defines an "investment contract" security as "(1) an investment of money (2) in a common enterprise and (3) the efforts of the promoter or a third party must have been fundamentally **[**28]** significant ones that affected the investment's success or failure." Ito Int'l Corp. v. Prescott, Inc., 83 Wn. App. 282, 921 P.2d 566, 571-72 (Wash. Ct. App. 1996); *see also* Cellular Eng'g, 820 P.2d at 946. The third prong of the modified *Howey* test looks to whether the profits on an enterprise "come 'primarily' or 'substantially' from the efforts of others." Id. at 946 (citing Sec. & Exch. Comm'n v. Glenn W. Turner Enters., Inc., 474 F.2d 476, 482 (9th Cir. 1973)). Defendants assert that Plaintiffs fail to satisfy the third element of this test.

[*1098] Although Plaintiffs defend their position that the Additional Earnout is a security under the "investment contract" analysis (*see* SJ Resp. (Dkt. # 85) at 12-17), they also argue that the Additional Earnout constitutes a security under the "risk capital" formulation that is also contained within the statutory definition (*see id.* at 11-12 (citing RCW 21.20.005(12)(a)). [9] "A risk capital investment may arise 'where the investor does not receive the right to exercise practical and actual control over the managerial decisions of the venture.'" Ultimate Timing, LLC v. Simms, No. C08-1632-MJP, 2010 U.S. Dist. LEXIS 64957, 2010 WL 2650705, at *2 (W.D. Wash. June 29, 2010) (citing Sauve v. K. C., Inc., 91 Wn.2d 698, 591 P.2d 1207 (Wash. 1979)) **[**29]** (applying an earlier version of RCW 21.20.005(12) that did not include "risk capital," but describing a risk capital investment as one "with a reasonable expectation of a valuable benefit but without the right to control the enterprise."). Courts in Washington, while recognizing that "the risk capital definition is distinct from the definition of an investment contract," nevertheless "appear to combine their analyses of both concepts under the *Howey* definition." Ultimate Timing, 2010 U.S. Dist. LEXIS 64957, 2010 WL 2650705, at *2 (citing Ito Int'l, 921 P.2d at 571). One court has declared: "Adoption of the 'risk capital' approach . . . does not obviate the *Howey* test that has heretofore been applied by the Washington courts." State v. Philips, 45 Wn. App. 321, 725 P.2d 627, 630 (Wash. Ct. App. 1986).

A recent decision in the Western District of Washington, interpreting **[**31]** Washington law on this issue, is instructive. In Ultimate Timing, 2010 U.S. Dist. LEXIS 64957, 2010 WL 2650705, plaintiff made an investment in an enterprise devoted to the commercialization and marketing of a race timing system in exchange for a 20% ownership and profit interest in the enterprise. 2010 U.S. Dist. LEXIS 64957, [WL] at *2. The plaintiff, however, conceded that he "spent substantial time and effort marketing the timing system to race directors and race timers during the time he was working with [the company]." *Id.* He also negotiated on behalf of the company. *See* Ultimate Timing, LLC v. Simms, 715 F. Supp. 2d 1195, 1209 (W.D. Wash. 2010). The *Ultimate Timing* court found that under either the "risk capital" or the "investment contract" analysis of "security," the plaintiff's own description of the investment required dismissal of the claim. Ultimate Timing, 2010 U.S. Dist. LEXIS 64957, 2010 WL 2650705, at *2. The court found that the plaintiff's "capital contribution was not an

---

interpretations and administration with related federal regulation).

[9] Plaintiffs also assert that the Additional Earnout constitutes a security because certain federal regulations and courts treat "phantom stock" or a stock appreciation right ("SAR") as a security, and prior to the execution of the APA, Mr. Axtman and Mr. Benitez were promised a "phantom equity interest" in KCDL and certain KCDL officers characterized the transaction as providing Plaintiffs with "phantom stock," "a **[**30]** phantom SAR plan," or "phantom equity" in KCDL. (*See* SJ Resp. at 9-11.) Nowhere does the APA itself refer to "phantom stock," "phantom equity," or "phantom SARs." In deciding whether a security is at issue here, the court must look to the substance or realities of the transaction. Sauve v. K. C., Inc., 91 Wn.2d 698, 591 P.2d 1207, 1208 (Wash. Ct. App. 1979) ("In determining whether a given transaction constitutes a 'security' within the meaning of these statutes, form should be disregarded for substance, and the emphasis should be on economic reality.") Accordingly, the court is less concerned with the informal nomenclature used by various parties either before or after the transaction, and more concerned with the actual terms of the APA. Further, Plaintiffs have failed to provide one case in which a court has concluded that an asset purchase agreement, which includes the type of future cash earnout payment at issue here, constitutes the purchase of a security. Accordingly, the court concludes that the proper analysis is to consider the APA and its Additional Earnout under the modified *Howey* test or the "rick capital" formulation.

investment contract because [the company's] profitability turned on [the **[*1099]** plaintiff's] own ability to market the system to timers and races." *Id.* The court also found that the plaintiff's capital contribution "[l]ikewise . . . was not a 'risk capital investment' because [the plaintiff] **[**32]** exercised practical or actual control over the entity." *Id.*

Like the result in *Ultimate Timing*, the result here is also the same under either the "investment contract" or "risk capital" formulation. There is no dispute that immediately following the execution of the APA, both Mr. Axtman and Mr. Benitez joined KCDL as Vice Presidents in charge of KCDL's Aventa Learning business line. (*See* Knowles Decl. Ex. C (Axtman Dep.) at 170:11-24l; Ex. B (Benitez Dep.) at 150:24-151:1.) Indeed, Mr. Axtman's and Mr. Bentiez's employment agreements are attached as exhibits to the APA and require that they become "Vice President[s], Sales" immediately after the transaction. (Knowles Decl. Ex. N at PLTF000054.) In addition, there is no dispute that Mr. Axtman and Mr. Benitez became members of KCDL's six-person executive team, which was responsible for strategic and operational decisions with respect to all of KCDL's business, immediately after the transaction closed in January 2007. (Knowles Decl. Ex. A (Brown Dep.) at 262:18-263:12.)

Mr. Axtman and Mr. Benitez try to minimize these significant contributions by asserting that they did not have the authority to hire and fire employees (SJ Resp. at 12), **[**33]** although Mr. Benitez admitted that immediately after the transaction, he and Mr. Axtman "could hire a sales team." (2nd Knowles Decl. (Dkt. # 93) Ex. B (Benitez Dep.) at 88:16-89:10.) They also try to minimize their involvement by asserting that they traveled for work extensively promoting sales or worked from home. (SJ Resp. at 12.) However, both testified that they did in fact typically participate in weekly executive meetings — albeit via telephone. (2nd Knowles Decl. Ex. B (Benitez Dep.) at 151:12-19; Ex. C (Axtman Dep.) at 171:1-20.) In any event, in this day and age of almost ubiquitous connectivity via cellular telephones and laptop computers, the court finds Mr. Axtman's and Mr. Benitez's travel schedules or the location of their remote offices to be immaterial with regard to the significance of their contributions to company management. Indeed, the court finds that the involvement of Mr. Benitez and Mr. Axtman to be at least as significant, if not more so, than the plaintiff in *Ultimate Timing.* Accordingly, the court finds that neither the APA nor the Additional Earnout meets the definition of either an investment contract or a risk capital investment, and accordingly is not **[**34]** a security under the WSSA. Defendants are entitled to summary judgment on Plaintiffs' WSSA claim, and the court dismisses the claim.

4. Plaintiffs' Misrepresentation Claim

"In order to prevail on a claim for intentional misrepresentation, [the plaintiff] must show: '(1) representation of an existing fact, (2) materiality, (3) falsity, (4) the speaker's knowledge of its falsity, (5) intent of the speaker that it should be acted upon by the plaintiff, (6) plaintiff's ignorance of its falsity, (7) plaintiff's reliance on the truth of the representation, (8) plaintiff's right to rely upon the representation, and (9) damages suffered by the plaintiff.'" *Poulsbo Group, LLC v. Talon Dev., LLC, 155 Wn. App. 339, 229 P.3d 906, 909-10 (Wash. Ct. App. 2010)* (quoting *W. Coast, Inc. v. Snohomish Cnty., 112 Wn. App. 200, 48 P.3d 997, 1000 (Wash. Ct. App. 2002))*. A material misrepresentation is one to which a reasonable person would attach importance when determining whether to participate in a transaction. *Aspelund v. Olerich, 56 Wn. App. 477, 784 P.2d 179, 183 (Wash. Ct. App. 1990)*. "Each element must be established by **[*1100]** 'clear, cogent and convincing evidence.'" *Id.* (quoting *Stiley v. Block, 130 Wash.2d 486, 505, 925 P.2d 194, 200 (Wash. 1996))*. Defendants **[**35]** assert that Plaintiffs have failed to prove by the necessary evidentiary standard (1) the existence of a material false representation, and (2) their right to rely upon it. (SJ Mot. at 18-21.)

Plaintiffs' misrepresentation claim arises out of Defendants' presentation to them of certain models (such as the October 2006 Buy Model, and others described above) projecting the performance of KCDL following its acquisition of Aventa. The heart of Plaintiffs' misrepresentation claim is the allegation that Defendants presented the October 2006 Buy Model as a good-faith estimate of KCDL's EBITDA, when in fact it was not generated in good faith. (Am. Compl. ¶ 33.) As noted above, the standard of proof for an intentional misrepresentation claim is high, and may prove to be a hurdle too high for Plaintiffs to clear at trial. The court, nevertheless, finds that given the disputed nature of the testimony concerning the methods used to develop the various models received by Mr. Axtman and Mr. Benitez both before and after execution of the APA, conflicting testimony concerning the rigor underpinning these models and their reliability or lack thereof, as well as Defendants' and other witnesses' various **[**36]** statements to Plaintiffs about these models, Plaintiffs have raised sufficient material factual issues

regarding the existence of a false representation to survive summary judgment.

With regard to the issue of Plaintiffs' right to rely upon the alleged misrepresentations, the court finds Plaintiffs have raised sufficient material factual issues to survive summary judgment on this issue, as well. The reliance issue is not, as Defendants assert, whether Plaintiffs were entitled to rely on the projections as a "guarantee of future performance" (SJ Mot. at 21) — clearly they were not. Rather, the issue is whether they were entitled to rely upon Defendants' representations about the rigor of the analysis underpinning the models — for example, that the projections were reasonable, based on fair assumptions or methodology, and supported by a significant capital plan.

Further, contrary to Defendants' assertions, Plaintiffs were not required to make further inquiry once Defendants had made representations or reassurances to Plaintiffs concerning the rigor of the models. "A party to whom a positive, distinct and definite representation has been made is entitled to rely on that representation and **[**37]** need not make further inquiry concerning the particular facts involved." *Douglas Nw., Inc. v. Bill O'Brien & Sons Constr., Inc., 64 Wn. App. 661, 828 P.2d 565, 577 (Wash. 1992)*; *see also ABN Amro Mortg. V. Greene, No. C04-0450C, 2005 U.S. Dist. LEXIS 33534, 2005 WL 2207027, at * 3 (W.D. Wash. Aug. 10, 2005)* (applying Washington law). This rule is applied if the misrepresentations are made to induce conduct, the misrepresentations succeed in inducing conduct, and the complaining party was actually deceived and mislead by the misrepresentations. *Jenness v. Moses Lake Dev. Co., 39 Wn.2d 151, 234 P.2d 865, 869 (Wash. 1951)* (quoting *Cunningham v. Studio Theatre, Inc., 38 Wn.2d 417, 229 P.2d 890, 894 (Wash. 1951)*). When applying this rule, "it is immaterial that the means of knowledge are open to the complaining party, or easily available to him, and that he may ascertain the truth by proper inquiry or investigation." *Jenness, 234 P.2d at 869* (quoting *Cunningham, 229 P.2d at 894*). Accordingly, the court denies Defendants' motion for summary judgment on Plaintiffs' misrepresentation claim.

5. Duty of Good Faith and Fair Dealing Claim

The implied duty of good faith and fair dealing "obligates parties [to a contract] to cooperate with each other so **[*1101]** that each may obtain **[**38]** the full benefit of performance." *Badgett v. Sec. State Bank, 116 Wn.2d 563, 807 P.2d 356, 360 (Wash. 1991)*. The duty prevents a contracting party from engaging in conduct that frustrates the other party's right to the benefits of the contract. *Woodworkers of Am. v. DAW Forest Prods. Co., 833 F.2d 789, 795 (9th Cir. 1987)*. Plaintiffs' claim for breach of the duty of good faith and fair dealing is based on allegations that KCDL, through it management bonus plan and certain accounting methods, artificially suppressed EBITDA generation, which undermined and limited Plaintiffs' expected compensation under the Additional Earnout. [10] (Am. Compl. ¶¶ 61-66.)

Although Defendants acknowledge that Washington courts recognize an implied duty of good faith and fair dealing in every contract, *see Betchard-Clayton, Inc. v. King, 41 Wn. App. 887, 707 P.2d 1361, 1364 (Wash. Ct. App. 1985)*, they correctly assert that the duty of good **[**39]** faith and fair dealing "does not extend to obligate the party to accept a material change in the terms of its contract," nor "inject substantive terms into the parties' contract." *Badgett, 807 P.2d at 360* (internal citations and quotation marks omitted). Accordingly, they move to dismiss Plaintiffs' claim on summary judgment, arguing that no provision of the APA requires KCDL to maximize EBITDA. (SJ Mot. at 22.)

The issue, however, is not the injection of a substantive term into the APA, but rather whether KCDL exercised its discretion with regard to accounting methods and other factors affecting the calculation of EBITDA following execution of the APA in good faith. "The covenant of good faith applies when the contract gives one party discretionary authority to determine a contract term; it does not apply to *contradict* contract terms." *Goodyear Tire & Rubber Co. v. Whiteman Tire, Inc., 86 Wn. App. 732, 935 P.2d 628, 632 (Wash. Ct. App. 1997)* (italics in original). As stated by the court:

> The duty of good faith and fair dealing applies when one party has discretionary authority to determine certain terms of the contract, such as quantity, price, or time. . . . The covenant may be relied upon only when **[**40]** the manner of performance under a specific contract term allows for discretion on the part of either party. . . . However, it will not contradict terms or conditions for which a party has

[10] "[T]he APA provides that the Additional Earnout is calculated based on a percentage of, 'equal to six percent (6%) of the Assumed Equity Value' of KCDL." (Am. Compl. ¶ 18 (quoting APA § 2.03(c)).) "Assumed Equity Value" is in turn based on KCDL's EBITDA. (*Id.* ¶ 27; Knowles Decl. Ex. M (APA) § 203(c).)

bargained.

Id. (quoting Amoco Oil Co. v. Ervin, 908 P.2d 493, 498 (Colo. 1995)); *see also* Craig v. Pillsbury Non-Qualified Pension Plan, 458 F.3d 748, 752 (8th Cir. 2006) ("Ordinary contract principles require that, where one party is granted discretion under the terms of Tthe contract, that discretion must be exercised in good faith — a requirement that includes the duty to exercise the discretion reasonably.") (applying Washington law).

Under the APA, Plaintiffs' Additional Earnout was based, in part, on KCDL's calculation of its EBITDA. The determination of EBITDA is not an exact science, and can be affected by a range of accounting and other factors within Defendants' discretion. Plaintiffs presented evidence that following execution of the APA, KCDL implemented certain accounting policy changes that suppressed its EBITDA calculation. (*See* Goldfarb Decl. Ex. P (Beaton Supp. Expert Report) ¶ 31(a)-(e).) For example, certain KCDL employees questioned the value received for shared services charged **[**41]** to KCDL by KLC, which **[*1102]** reduced EDITDA. (*Id.* ¶ 31(e); Benitez Decl. Ex. E at KCDL086560; Goldfarb Decl. Ex. S at 15.) While Defendants submit evidence that KCDL revised its bonus plan to incentivize the maximization of EBITDA (Cogan Decl. (Dkt. # 83)), [11] this evidence does not negate the existence of a material issue of fact in light of the evidence presented by Plaintiffs. Accordingly, the court denies Defendants' motion for summary judgment on this issue. [12]

6. Claim for Declaratory Relief

Defendants have moved for summary judgment of Plaintiffs' claim for declaratory relief. Plaintiffs contend that they have been denied "reasonable access to KCDL's information and documents relating to EBITDA and the booking of transactions effecting EBITDA." (Am. Compl. ¶ 68.) Defendants assert that the claim should be dismissed on summary judgment because:

> . . . KCDL provided Aventa with financial and accounting information to permit it to investigate the basis for the dispute. Aventa has received the information to which it is entitled pursuant to the APA.

(SJ Mot. at 23.) Defendants assert this bald statement without a scintilla of factual support. By way of contrast, Plaintiffs have submitted evidence of a continuing dispute concerning the adequacy of **[**44]** Defendants' production of documents and information as required under the APA relating to KCDL's calculation of EBITDA. (SJ Resp. at 24 (citing Goldfarb Decl. Exs. T, U).) The court, accordingly, denies Defendants' motion for summary judgment on this issue.

7. Individual Plaintiffs

Defendants assert that the claims of the individual plaintiffs — Aventa's shareholders — should be dismissed because **[*1103]** the individual plaintiffs lack standing. A plaintiff must have a personal stake in the outcome of the case to bring suit. Gustafson v. Gustafson, 47 Wn. App. 272, 734 P.2d 949, 952 (Wash. Ct. App. 1987). "Ordinarily, a shareholder cannot sue for

[11] In their opposition to Defendants' motion for summary judgment, Plaintiffs move to strike Mr. Cogan's declaration on grounds that KCDL did not disclose Mr. Cogan as an expert witness in any of its ***Federal Rule of Civil Procedure 26(a)*** initial disclosures, even though KCDL had supplemented those disclosures only one month prior to filing its motion for summary judgment. (SJ Resp. at 23-24.) Because the court has denied Defendants' motion for summary judgment on this issue even in light of Mr. Cogan's declaration, Plaintiffs' request to strike Mr. Cogan's declaration is moot. Further, KCDL has stated that Plaintiffs were permitted the opportunity to depose Mr. Cogan prior to filing their response to KCDL's motion for summary judgment **[**42]** (SJ Reply (Dkt. # 92) at 12 n. 8 (citing 2nd Knowles Decl. ¶ 6)), and thus prejudice, if any, would appear to be minimal. In any event, the court's decision with regard to Mr. Cogan's declaration here does not preclude Plaintiffs from raising the issue of the admissibility of Mr. Cogan's testimony at trial in a motion in limine, if appropriate.

[12] The APA provides that, if KCDL and Aventa cannot resolve any dispute concerning the calculation of the Additional Earnout payment, they shall submit the dispute to an independent accounting firm for "final, binding and conclusive" resolution. (Knowles Decl. Ex. M at KCDL115634.) In their motion for summary judgment, Defendants assert, in a one-sentence argument, that the APA requires arbitration before an independent accounting firm regarding any dispute over KCDL's calculation of the Additional Earnout. (SJ Mot. at 22.) In addition, Defendants address the issue in one sentence and a footnote within their reply memorandum. (SJ Reply at 12 & n. 9.) Likewise, Plaintiffs addressed the issue in three sentences within a footnote of their responsive memorandum. (SJ Resp. at 23, n. 4.) The court finds the parties' discussion of the issue wholly inadequate **[**43]** for purposes of any determination, and declines to consider this issue based on the sparse "briefing" provided by the parties. *See, e.g.,* Indep. Towers of Wash. v. Wash., 350 F.3d 925, 929 (9th Cir. 2003) ("As the Seventh Circuit observed in its now familiar maxim, '[j]udges are not like pigs, hunting for truffles buried in briefs.'") (quoting United States v. Dunkel, 927 F.2d 955, 956 (7th Cir. 1991)).

wrongs done to a corporation, because the corporation is viewed as a separate entity, and the shareholder's interest is too remote to meet the standing requirements." *Id. at 953*. "Even a shareholder who owns all or most of the stock, but who suffers damages only indirectly as a shareholder, cannot sue as an individual." *Sabey v. Howard Johnson & Co., 101 Wn. App. 575, 5 P.3d 730, 735 (Wash. Ct. App. 2000)*. There are two exceptions to this rule: "(1) where there is a special duty, such as a contractual duty, between the wrongdoer and the shareholder; and (2) where the shareholder suffered **[**45]** an injury separate and distinct from that suffered by other shareholders." *Id.* The special duty must have "its origin in circumstances independent of the stockholder's status as a stockholder." *Hunter v. Knight, Vale & Gregory, 18 Wn. App. 640, 571 P.2d 212, 216 (Wash. Ct. App. 1977)*.

With regard to the first exception, Defendants assert that there is no evidence that they owed any special duty to the individual plaintiffs — independent of their status as stockholders of Aventa, and Plaintiffs have asserted none. (*See* SJ Resp. at 24.) With regard to the second exception, Defendants argue that although the individual plaintiffs signed the APA, they did so expressly in their capacity as shareholders of Aventa (Knowles Decl. Ex. M at KCDL115666-68), providing certain representations and warranties to KCDL (*see id.* at KCDL115636-48 (Articles III & IIIA)). Plaintiffs have not disputed these facts. Further, Plaintiffs have provided no evidence that the individual plaintiffs suffered any injury separate and distinct from those allegedly suffered by Aventa. The claims they assert are identical to those asserted by Aventa, and any injury they have allegedly incurred arises by virtue of their status as an Aventa **[**46]** shareholder.

Earlier in these proceedings, the court declined to dismiss the claims of the individual plaintiffs on Defendants' motion to dismiss. (Order (Dkt. # 54) at 9-10.) As the court noted in its prior ruling, however, neither party had cited any authority for its position. (*Id.* at 9.) Further, the posture of the case and the standards guiding the court were obviously different in the context of Defendants' motion to dismiss. The court now finds that Defendants have met their initial burden of showing that they are entitled to prevail on this issue as a matter of law, and Plaintiffs have failed to demonstrate a genuine issue of material fact in response. [13] Accordingly, the court grants Defendants' motion for summary judgment dismissing the claims of the individual plaintiffs. [14]

[*1104] B. Motion to Dismiss Counterclaims

1. Standards

The same standards applicable on a motion to dismiss a plaintiff's claim apply when considering a **[**48]** motion to dismiss a defendant's counterclaim. *See, e.g., In re Wash. Mut., Inc. Secs., Derivative & ERISA Litig., No. 08-md-1919 MJP, 2011 U.S. Dist. LEXIS 33531, 2011 WL 1158387, at *3 (W.D. Wash. Mar. 25, 2011)*. To survive a motion to dismiss, the counterclaim must have "facial plausibility [which exists] when the pleaded factual content allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal, 556 U.S. 662, 129 S.Ct. 1937, 1940, 173 L. Ed. 2d 868 (2009)*. In reviewing the counterclaim, the court must assume the facts to be true and construe them in the light most favorable to the nonmoving party. *Cervantes v. United States, 330 F.3d 1186, 1187 (9th Cir. 2003)*.

2. Counterclaims One and Three - Alleged Breach of Employment Contract by Mr. Axtman and Mr. Benitez

To state a counterclaim for breach of contract, KCDL

---

[13] In its earlier order denying dismissal of the individual plaintiffs, the court relied on *Far West Fed. Bank v. Office of Thrift Supervision-Direct-OR, 119 F.3d 1358, 1363-64 (9th Cir. 1997)*. On summary judgment, it is apparent that the factual circumstances here are not in accord with *Far West*. In *Far West*, the written agreement at issue explicitly identified the individual investors as intended beneficiaries. **[**47]** *Id. at 1364* & n.2. In addition, there was evidence that breach of the contract would inflict injury upon the investors personally because they were induced by the defendant's promises to recapitalize the plaintiff thrift to the tune of tens of millions of dollars prior to execution of the agreement between the thrift and defendants. Here, the individual plaintiffs are not express beneficiaries under the APA, nor have plaintiffs provided evidence of individualized injury — separate from their status as Aventa's shareholders.

[14] The court notes that although it is dismissing the claims of the individual plaintiffs on summary judgment, both Mr. Axtman and Mr. Benitez remain parties to this lawsuit as defendants to KCDL's cross-claims. Because Mr. Axtman and Mr. Benitez are no longer plaintiffs in this matter, they now would be properly viewed as third-party defendants to KCDL's claims. The court directs the parties to revise the caption in this matter so that it accurately reflects Mr. Axtman's and Mr. Benitez's current status in this litigation.

must allege that the employment contracts between itself and Mr. Axtman and Mr. Benitez, respectively, impose a duty, that the duty has been breached, and that the breach proximately caused damages to KCDL. *Nw. Indep. Forest Mfrs. v. Dep't of Labor & Indus., 78 Wn. App. 707, 899 P.2d 6, 9 (Wash. Ct. App. 1995)*. KCDL has adequately alleged that the employment contracts impose **[**49]** duties upon Mr. Axtman and Mr. Benitez, including (1) a duty of fidelity and loyalty to KCDL (KCDL Answer ¶¶ 14-15 (Counterclaims)), (2) a duty not to engage in any competitive business for a defined period of time (*id.* ¶ 16), (3) a duty not to interfere with KCDL's business relationships with its clients (*id.* ¶ 17), and (4) a duty to maintain all of KCDL's records and files prepared for or received from KCDL as the sole and exclusive property of KCDL, to not copy KCDL materials, and to promptly return to KCDL upon termination of their employment relationship all property belonging to KCDL (*id.* ¶ 18).

KCDL has also adequately alleged breach of the employment contracts by both men. KCDL has alleged that both Mr. Axtman and Mr. Benitez copied and destroyed proprietary information belonging to KCDL (*id.* ¶¶ 29-30, 44), that Mr. Axtman intentionally interfered with KCDL's business relationship with a client (*id.* ¶¶ 31-32), and that Mr. Axtman's plan to launch a new company that competed with KCDL and his incorporation of that company, violated the employment contract (*id.* ¶¶ 23, 33). KCDL has also adequately alleged damages with regard to these claims. (*Id.* ¶¶ 34, 45.) Plaintiffs' assertions **[**50]** that KCDL was not damaged by these alleged breaches or that Mr. Axtman's new company never actually competed with KCDL may be arguments more appropriate for summary judgment, but they do not succeed here on a motion to dismiss. Defendants' allegations with regard to counterclaims one and three are sufficient under the applicable standards recited above. Accordingly, the court denies Plaintiffs' motion to dismiss counterclaims one and three.

3. Counterclaim Two - Alleged Breach of the Separation Agreement by Mr. Axtman

Plaintiffs assert that Defendants have failed to state a claim for breach of Mr. Axtman's separation agreement with KCDL on the basis of Mr. Axtman's copying of KCDL proprietary information following **[*1105]** his separation from the company because the separation agreement does not prohibit the copying of documents. (Mot. to Dismiss at 7-8.) KCDL, however, has alleged that the contract prohibits tampering with or using KCDL proprietary information following termination of Mr. Axtman's work relationship. (*See* KCDL Answer ¶¶ 21, 36 (Counterclaims).) Further, KCDL has alleged that the Separation Agreement required Mr. Axtman to return all KCDL property, including copies of electronic **[**51]** materials (*id.* ¶22), and that, irrespective of these requirements, Mr. Axtman downloaded KCDL records onto an electronic storage device or external hard drive following his separation from the company (*id.* ¶ 25). Accordingly, KCDL has properly alleged breach of the separation agreement based on Mr. Axtman's copying of KCDL's files. The court denies Plaintiffs' motion to dismiss counterclaim two.

4. Counterclaim Six - Conversion

Under Washington law, the elements of conversion are an unjustified, willful interference with a chattel which deprives a person entitled to the property of possession. *Potter v. Wash. State Patrol, 165 Wn.2d 67, 196 P.3d 691, 696 (Wash. 2008))*. The plaintiff must also plead that it has some property interest in the goods allegedly converted. *Coto Settlement v. Eisenberg, 593 F.3d 1031, 1039 (9th Cir. 2010)* (citing *Meyers Way Dev. Ltd. Partnership v. Univ. Sav. Bank, 910 P.2d 1308, 1320, 80 Wn. App. 655 (1996)*). Washington courts look to the Restatement (Second) of Torts when analyzing conversion claims. *See, e.g., Brown ex rel. Richards v. Brown, 157 Wn. App. 803, 239 P.3d 602, 611 (Wash. Ct. App. 2010)* (citing and quoting the *Restatement (Second) of Torts § 223 cmt. b* (1965)). The Restatement recognizes claims **[**52]** for conversion in variety of circumstances, including wrongfully detaining chattel, destroying or altering chattel, exceeding the authorized use of chattel, and misusing chattel. *See Restatement (Second) Torts §§ 221-241*.

Plaintiffs assert that Defendants' counterclaim for conversion should be dismissed because simply accessing KCDL's files or copying them does not deprive KCDL of possession of the original electronic records remaining in KCDL's possession. (*See* Mot. to Dismiss at 14.) However, the court finds that KCDL's allegations that Mr. Axtman and Mr. Benitez copied, accessed, and destroyed KCDL's electronic files constitute "wrongfully detaining," "exceeding the authorized use of," or "misusing" those files, thereby depriving KCDL of its possession or control over such files. The fact that KCDL has access to another copy of the files at issue does not mean that it was not deprived of its possession of the copies accessed, made, or destroyed by Plaintiffs. Further, the court can find no logical basis for distinguishing between theft of copy and

theft of the original electronic document. After all, the copy of the original (although allegedly created by Plaintiffs) would belong **[**53]** to Defendants as well. Courts dealing with this issue have begun to update the tort of conversion so that it keeps pace with the contemporary realities of widespread computer use. *See, e.g.,* E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc., 688 F. Supp. 2d 443, 455 (E.D. Va. 2009) ("[Plaintiff's] claim for conversion, even if based exclusively on the transfer of copies of electronic information, survives [defendant's] motion to dismiss."); Thyroff v. Nationwide Mut. Ins. Co., 8 N.Y.3d 283, 864 N.E.2d 1272, 832 N.Y.S.2d 873 (N.Y. 2007) ("[T]he tort of conversion must keep pace with the contemporary realities of widespread computer use," and therefore, "electronic records that [are] stored on a computer . . . [are] subject to a claim of conversion . . . ."). The court denies **[*1106]** Plaintiffs' motion to dismiss counterclaim six for conversion.

C. Motion for Protective Order

KCDL asserts in its motion for a protective order that Mr. Axtman and Mr. Benitez have waived any privilege with regard to attorney-client communications that they saved onto their KCDL laptop computers. Because this court's jurisdiction is based on diversity [15] and the underlying claims are predicated on state law, the privilege issues are governed **[**54]** by state law. *See* Fed. R. Evid. 501 ("[I]n civil actions and proceedings, with respect to an element of a claim or defense as to which State law supplies the rule of decision, the privilege of a . . . person . . . shall be determined in accordance with State law."); In re Cal. Pub. Utils. Comm'n, 892 F.2d 778, 781 (9th Cir. 1989) ("In diversity actions, questions of privilege are controlled by state law."). Washington's attorney-client privilege applies to confidential communications and advice between an attorney and client and extends to documents that contain a privileged communication. State v. Perrow, 156 Wn. App. 322, 231 P.3d 853, 855 (Wash. Ct. App. 2010). In Washington, the party asserting the attorney-client privilege has the burden of proving all the elements of privilege, including the absence of waiver. *See* Dietz v. Doe, 131 Wn.2d 835, 935 P.2d 611, 618-19 (Wash. 1997); *see also* Perrow, 231 P.3d at 856. Mr. Axtman and Mr. Benitez bear the burden of proving that the attorney-client privilege attached to the communications at issue, and that they did not waive the attorney-client privilege with regard to materials that they accessed and saved on their KCDL laptop computers.

1. Mr. Axtman's Laptop

Washington courts have held that "[w]hen a client reveals information to a third-party, the attorney-client privilege is waived unless the third-party is necessary for the communication or has retained the attorney for a common interest." Zink v. City of Mesa, 162 Wn. App. 688, 256 P.3d 384, 403 (Wash. Ct. App. 2011) (citing Morgan v. City of Fed. Way, 166 Wn.2d 747, 213 P.3d 596, 601 (Wash. 2009)). Following his separation from KCDL, Mr. Axtman returned his laptop to the company in late 2009. He did not, however, assert the attorney-client privilege with regard to any documents contained on the laptop until May 12, 2011, nearly a year and half following his relinquishment of the computer. (Crooks Decl. ¶¶ 7-8, Ex. 5.) Once Mr. Axtman relinquished the laptop to KCDL (a third-party outside of his attorney-client relationship) without asserting privilege or taking any precautions to protect the privacy of materials that he had saved on the laptop, he no longer had any reasonable expectation of confidentiality with regard to those materials. Accordingly, under Washington law, he waived any privilege **[**56]** that may have been applicable. *See* Zink, 256 P.3d at 403; Morgan, 213 P.3d at 601. Such waiver would encompass all of the materials he placed or saved from any source onto his KCDL laptop computer. His belated attempt to assert the attorney-client privilege approximately a year and a half later is futile. Any privilege that may have existed with regard to these materials was extinguished by his unconditional relinquishment of the laptop and cannot be subsequently resurrected. Accordingly, the court grants Defendants' motion with regard to documents that Mr. Axtman saved onto his KCDL laptop computer, and that may now be **[*1107]** stored on either his laptop or on Defendants' servers.

2. Mr. Benitez's Laptop

The court's analysis of both waiver and whether the attorney-client privileged ever attached to certain communications or materials that Mr. Benitez saved on his KCDL laptop stands on different grounds. Unlike Mr. Axtman, Mr. Benitez did not relinquish his KCDL laptop to the company without first asserting attorney-client privilege over certain materials contained on it, and without securing a sequestration agreement with regard to those materials from KCDL. The question with regard

---

[15] KCDL removed this action from **[**55]** King County Superior Court to this court on the basis of diversity jurisdiction. (Am. Compl. ¶ 2.)

to Mr. **[**57]** Benitez's assertion of privilege is whether, in light of KCDL's policies concerning the use of its laptop computers by its employees, Mr. Benitez had any reasonable expectation of privacy with regard to attorney-client communications he saved on his laptop, or whether the act of saving those communications onto his KCDL laptop served to waive any privilege that may have existed.

As discussed above, KLC performs the human resource functions for KDLC, including policy promulgation. (1st Keegan Decl. (Dkt. # 63) ¶ 2.) Although both Mr. Benitez and Mr. Axtman have denied ever being employed by KLC as opposed to KDLC (Axtman Decl. re: P.O. ¶ 5; Benitez Decl. re: P.O. ¶ 5), neither has denied KLC's human resources role with regard to KDLC. Further, although Mr. Benitez testifies that "to the best of [his] knowledge, [he] never received a copy of KLC's Employee Handbook" (Benitez Decl. re: P.O. ¶ 13), Defendants have presented evidence that Mr. Benitez received two emails dated November 19, 2007 and February 23, 2009, both of which included the KLC Handbook as an attachment. (2nd Keegan Decl. Exs. 1 & 2.) Mr. Benitez does not ever expressly deny receiving these emails. In light of Defendants' **[**58]** undisputed evidence of Mr. Benitez's receipt of these two emails, Mr. Benitez's best recollections that he did not receive the handbook must yield. Based on the evidence presented, the court must conclude that Mr. Benitez did in fact receive copies of the KLC Employee Handbook on more than one occasion.

In any event, Mr. Benitez was a vice-president of KCDL and a member of KCDL's executive committee. (Knowles Decl. Ex. B (Benitez Dep.) at 150:24-151:1, 151:2-19; Ex. A (Brown Dep.) at 262:8-263:12.) As a senior level manager, Mr. Benitez was "expected to know the contents of company policies so [he] could properly manage and supervise employees." (2nd Keegan Decl. ¶4.) Accordingly, Mr. Benitez is fairly charged with constructive knowledge of the company's policies concerning electronic communications. *See, e.g.*, Scott v. Beth Israel Med. Center, Inc., 17 Misc. 3d 934, 847 N.Y.S.2d 436, 441 (Sup. Ct. 2007) ("[Former employee's] effort to maintain that he was unaware of [former employer's] email policy barring personal use is rejected. As an administrator, [former employee] had constructive knowledge of the policy.").

KLC's handbook contains an Electronic Communications policy which clearly states that "[e]lectronic **[**59]** communications are not private." (1st Keegan Decl. ¶ 3, Ex. 2.) The policy also states that "[a]ll resources used for electronic communications are KLC property" and "should generally be used only for KLC business." (*Id.*) Finally, the policy states that KLC "reserves the right to access, search, inspect, monitor, record, and disclose any file or stored communication . . . at any time and for any reason." (*Id.*)

Washington law protects only confidential communications between an attorney and a client. Morgan, 213 P.3d at 601 ("To qualify for attorney-client privilege, a communication must be made in confidence.") **[*1108]** For the privilege to apply, the client must have a reasonable expectation that the communications are confidential and will be kept confidential. *In re Siegfried, 42 Wn. App. 21, 708 P.2d 402, 404-05 (Wash. Ct. App. 1985)* (analyzing psychologist-patient communications privilege which "are privileged to the same extent, and are subject to the same conditions, as are confidential communications between attorney and client"). If a client is informed that there may be disclosure to a third-party, there is no reasonable expectation of confidentiality and the privilege never attaches. *See* Hertog v. City of Seattle, 138 Wn.2d 265, 979 P.2d 400, 411 (Wash. 1999) **[**60]** (analyzing psychologist-patient communications); *see also* State v. Side, 105 Wn. App. 787, 21 P.3d 321, 324-25 (Wash. Ct. App. 2001) (analyzing psychologist-patient communications, the court held that "[a] patient who is warned that communications may not be kept confidential has no reasonable expectation of confidentiality and any privilege is waived.").

Based on the company policy described above, Mr. Benitez could not have had a reasonable expectation of confidentiality with regard to communications or other materials that he created or received on his KCDL laptop following the acquisition of Aventa and that were saved or stored on his KCDL laptop or the Defendants' servers. The laptop itself was not his property, and the company reserved the right to access and disclose any file or stored communication at any time. Thus, Mr. Benitez cannot meet his burden of proving that any expectation of confidentiality he might have entertained was reasonable. [16] Accordingly, the court finds that the

[16] Mr. Benitez argues that Defendants must show that he received the company policy before transferring the emails to his laptop. First, as discussed above, the burden of establishing the existence of the attorney-client privilege, including lack of waiver, is on Plaintiffs. *See* Dietz, 935 P.2d at 618-19; *see also* Perrow, 231 P.3d at 856. Second, Defendants did provide evidence of that the Employee

attorney-client privilege never attached with regard to emails or communications that Mr. Benitez created and sent or that he received after the Aventa acquisition, which were stored on his KCDL laptop or the Defendants' **[**61]** servers. [17]

In addition, to the extent that Mr. Benitez saved attorney-client privileged communications or documents created before the Aventa acquisition onto his KCDL laptop, he waived any privilege that may have previously attached to these materials. [18] Although Washington courts have not yet addressed this issue specifically, most state and federal courts evaluating **[*1109]** whether an employee has waived the attorney-client privileged status of personal communications transmitted, stored, or saved onto a company computer or laptop, have applied the four-factor test initially set forth in *In re Asia Global, 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)*. *See* *In re Reserve Fund Secs. & Derivative Litig., 275 F.R.D. 154, 159-60 (S.D.N.Y. 2011)* (describing *Asia Global* as "widely adopted" and listing myriad cases). The *Asia Global* factors are: (1) does the company maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or email, **[**63]** (3) do third parties have a right of access to the computer or emails, and (4) did the corporation notify the employee, or was the employee aware, of the policy. *Asia Global, 322 B.R. at 257*.

With regard to the first factor, the company's policy states that "resources used for electronic communications . . . should generally be used only for KLC business." (1st Keegan Decl. ¶ 3, Ex. 2 at 21.) Although the company policy does not place an outright ban on any personal use, personal use is discouraged. Further, the policy expressly warns employees that electronic communications are not private. Consequently, it would not be reasonable for an employee to believe that such communications stored on company hardware would be confidential. With regard to the second factor, not only does the company policy expressly state that any stored communication or file can be monitored, recorded **[**64]** and disclosed, the company does in fact conduct such monitoring. (1st Keegan Decl. ¶ 5.) Although there is no evidence that KCDL ever specifically monitored Mr. Benitez's computer during his employment, courts have found that a policy permitting such monitoring meets this factor. *See, e.g.,* *Scott, 847 N.Y.S.2d at 442*. For the third factor, the policy expressly allows the company to access information and to disclose it. Finally, the court has previously addressed the fourth factor and found that Mr. Benitez had both actual and constructive notice of the company's policies. Accordingly, the *Asia Global* factors have been met, and the court concludes that Mr. Benitez waived any privilege that may have attached to the communications or files at issue here when he saved or stored them on his KCDL laptop computer. [19]

Some courts have found an exception maintaining **[**65]** an employee's expectation of privacy at least with regard to attorney-client communications accessed on personal, password-protected, web-based email — even if the employee accesses the web-based account using the company's computer system and the company maintains a policy against such use. *See, e.g.,* *Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 990 A.2d 650, 665 (N.J. 2010)* ("Because of the important public policy concerns underlying the attorney-client privilege, even . . . a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client

---

Handbook was sent to all new Aventa employees upon commencement of employment. (*See* 1st Keegan Decl. ¶ 6, Ex. 4.) Even if Mr. Benitez received the policy after he transferred his privileged email to his laptop, upon receiving the policy and learning that his laptop was not confidential, he should have promptly taken steps to protect the privileged material. Instead, he did nothing for years and did not attempt to assert the privilege until his employment with KCDL had ended. Based on this inaction, the court finds that it would be no defense to waiver even if Mr. Benitez had not receive the policy until after he had transferred confidential communications to his laptop.

[17] Although the court previously held that Mr. Axtman waived any applicable privilege when he unconditionally relinquished **[**62]** his laptop to KCDL following his separation from the company, the court's analysis here concerning Mr. Benitez would also apply to Mr. Axtman as additional grounds for granting Defendants' motion for a protective order.

[18] Although the court has already found that privilege did not attach to files or communications that Mr. Benitez created or received on KCDL laptop following the acquisition of Aventa, this waiver analysis would also apply to these files or communications as an additional ground for granting Defendants' motion.

[19] Although the court previously found that Mr. Axtman waived any privilege when he unconditionally relinquished his laptop to KCDL, the court's waiver analysis with regard to Mr. Benitez under the *Asia Global* factors would be equally applicable to Mr. Axtman, and provides additional grounds for finding waiver of the privilege in his case.

communications, if accessed on a personal, password-protected e-mail account using the company's computer system — would not be enforceable."). In particular, Mr. Benitez and Mr. Axtman rely upon *Sims v. Lakeside School, No. C06-1412RSM, 2007 U.S. Dist. LEXIS 69568, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007)*. In *Sims*, the court found that, based on the school/employer's policy, the employee had no reasonable expectation of privacy in the **[*1110]** contents of his laptop, and that his absence of privacy rights also extended to the emails he sent and received on the school's accounts. *2007 U.S. Dist. LEXIS 69568, [WL] at *1*. The court, nevertheless, **[**66]** held to the contrary with regard to web-based emails sent and received by the plaintiff on his school laptop. *2007 U.S. Dist. LEXIS 69568, [WL] at *2*. The *Sims* court does not provide a rationale for its distinction other than general public policy grounds and the importance of the attorney-client privilege. *Id.*

Although this court is in accord with regard to the value of the attorney-client privilege, it does believe that *Sims* is applicable here. The *Sims* court does not specifically address choice of law, but it appears to have based its analysis on federal law. *See id.* Here, the court's analysis must be grounded in and consistent with its view of Washington law. Washington has a policy of "strictly limiting the attorney-client privilege to its purpose." *Sitterson v. Evergreen Sch. Dist. No. 114, 147 Wn. App. 576, 196 P.3d 735, 741 (Wash. Ct. App. 2008)*. In *Sitterson*, the court was considering whether to adopt an approach to inadvertent production of the attorney-client communications which (1) never waived the privilege, or (2) which considered the circumstances of the case. *Id. at 740-42*. The *Sitterson* court found that a non-waiver rule "is inconsistent with Washington's policy." *Id. at 741*. The court stated:

> The privilege is so **[**67]** limited because it sometimes results in the exclusion of relevant and material evidence, contrary to the philosophy that justice requires the fullest disclosure of the facts. . . . Consequently, employing the attorney-client privilege to prohibit testimony must be balanced against the benefits to the administration of justice stemming from the general duty to give what testimony one is capable of giving. . . . These considerations weigh toward taking a broader view of waiver than the [defendant] proposes.

Id. (citations and quotations omitted). As a result, the court rejected a rule in which inadvertent disclosure could never waive the attorney-client privilege. Instead, the court adopted a "balanced approach," in which the court considered a variety factors surrounding the inadvertent disclosure in determining whether waiver had occurred. *Id. at 741-42*.

Following *Sitterson*, this court believes that Washington would also take a broader view of the waiver issue here, and adopt a balanced approach and not a non-waiver rule concerning web-based personal email accounts that are accessed through an employee's company computer or laptop. Accordingly, the court does not believe that decisions **[**68]** such as *Stengart* or *Sims*, which adopt a no-waiver rule concerning web-based personal email accounts accessed through an employee's company-issued computer or laptop, are applicable in Washington. Applying the balanced-approach outlined in *Asia Global*, the court can find no reason to distinguish between emails that were sent from or received on the company's email system and emails that were accessed through the company's laptop on Mr. Benitez's or Mr. Axtman's web-based email accounts. The company's policy here was broad. It applied to "[a]ll resources used for electronic communications" and stated that these resources were KLC property. (1st Keegan Decl. ¶3, Ex. 2.) Further, the policy reserved the company's right "to access, search, . . . or disclose *any file or stored communication.*" (*Id.* (italics added).) To the extent that Mr. Benitez's or Mr. Axtman's emails from their web-based personal email accounts are stored on their KCDL laptops or the Defendants' servers, those emails would be encompassed by the policy. Accordingly, based on the *Asia Global* factors analyzed above, any privilege that once may have applied to these communications is waived.

[*1111] IV. CONCLUSION

Based on the forgoing, **[**69]** the court GRANTS in part and DENIES in part Defendants' motion for summary judgment (Dkt. # 81), DENIES Plaintiffs' motion to dismiss the counterclaims (Dkt. # 58), and GRANTS Defendants' motion for a protective order (Dkt. # 61).

Dated this 8th day of November, 2011.

/s/ James L. Robart

JAMES L. ROBART

United States District Judge

End of Document