Departing Employees: Practical Legal Guidance

by

Robert B. Fitzpatrick
rfitzpatrick@robertbfitzpatrick.com



BIOGRAPHY

Robert ("Bob") Brian Fitzpatrick is the principal in the law firm of Robert B. Fitzpatrick PLLC in Washington, D.C. where represents clients in employment law matters. Mr. Fitzpatrick has concentrated his practice in employment law disputes for more than fifty years. He has represented clients in individual and class actions. He has represented clients in employment discrimination, workplace harassment, retaliation, age discrimination, FMLA, ADA, whistleblower, wrongful termination, non-compete, trade secrets, Computer Fraud and Abuse Act, and wage and hour claims, among others. He counsels numerous executive clients regarding employment agreements and compensation issues. He has negotiated literally thousands of severance agreements. He is also a frequent speaker on employment law topics, and has written countless articles on employment law, a few of which can be found on his website and his blog, Fitzpatrick on Employment Law.

Prior to entering private practice, Mr. Fitzpatrick served as a staff attorney in the Jackson, Mississippi office of the Lawyers' Committee for Civil Rights Under Law in the late 1960's; as a staff attorney in the Office of General Counsel of the Equal Employment Opportunity Commission in the early 1970's; and with the Washington Research Project (now the Children's Defense Fund) training minority attorneys in the Deep South to litigate employment discrimination cases. He has been in private practice in Washington, D.C. since 1970. He is an avid hiker and kayaker. He is a Fellow of the College of Labor & Employment Lawyers, having been inducted as a Fellow at the first annual induction ceremony in 1996. He has been listed as one of The Best Lawyers in America® for at least 25 continuous years.

He is admitted to practice in all courts of the District of Columbia (Superior Court, D.C. Court of Appeals, and the Federal District Court of the District of Columbia), the Federal District Court for Maryland, the Federal District Court for the Northern District of Mississippi, the Supreme Court of the United States, the Federal Circuit, the Court of Federal Claims, and the United States Courts of Appeals for the District of Columbia as well as the Fourth and Sixth Circuits.

DISCLAIMER OF ALL LIABILITY AND RESPONSIBILITY

THE INFORMATION CONTAINED HEREIN IS BASED UPON SOURCES BELIEVED TO BE ACCURATE AND RELIABLE – INCLUDING SECONDARY SOURCES. DILIGENT EFFORT WAS MADE TO ENSURE THE ACCURACY OF THESE MATERIALS, BUT THE AUTHOR ASSUMES NO RESPONSIBILITY FOR ANY READER'S RELIANCE ON THEM AND ENCOURAGES READERS TO VERIFY ALL ITEMS BY REVIEWING PRIMARY SOURCES WHERE APPROPRIATE AND BY USING TRADITIONAL LEGAL RESEARCH TECHNIQUES TO ENSURE THAT THE INFORMATION HAS NOT BEEN AFFECTED OR CHANGED BY RECENT DEVELOPMENTS. THIS PAPER MAY CONTAIN LINKS OR REFERENCES TO OTHER THIRD-PARTY RESOURCES. SUCH LINKS OR REFERENCES ARE FOR THE CONVENIENCE OF THE READER. THE AUTHOR DOES NOT RECOMMEND OR ENDORSE THE CONTENTS OF THESE RESOURCES.

READERS OF THIS PAPER SHOULD CONTACT AN ATTORNEY TO OBTAIN ADVICE WITH RESPECT TO ANY PARTICULAR LEGAL MATTER. NO READER OF THIS PAPER SHOULD ACT OR REFRAIN FROM ACTING ON THE BASIS OF INFORMATION CONTAINED IN THIS PAPER WITHOUT FIRST SEEKING LEGAL ADVICE FROM COUNSEL IN THE RELEVANT JURISDICTION. ONLY YOUR INDIVIDUAL ATTORNEY CAN PROVIDE ASSURANCES THAT ANY PARTICULAR RULE, INFORMATION, OR INTERPRETATION OF THE LAW MAY BE APPLICABLE TO YOUR PARTICULAR SITUATION.

THIS PAPER IS PRESENTED AS AN INFORMATIONAL SOURCE ONLY. IT IS INTENDED TO ASSIST READERS AS A LEARNING AID; IT DOES NOT CONSTITUTE LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL ADVICE. IT IS NOT WRITTEN (NOR IS IT INTENDED TO BE USED) FOR PURPOSES OF ASSISTING CLIENTS, NOR TO PROMOTE, MARKET, OR RECOMMEND ANY TRANSACTION OR MATTER ADDRESSED; AND, GIVEN THE PURPOSE OF THE PAPER, IT MAY OMIT DISCUSSION OF EXCEPTIONS, QUALIFICATIONS, OR OTHER RELEVANT INFORMATION THAT MAY AFFECT ITS UTILITY IN ANY LEGAL SITUATION. THIS PAPER DOES NOT CREATE AN ATTORNEY-CLIENT RELATIONSHIP BETWEEN THE AUTHOR AND ANY READER. DUE TO THE RAPIDLY CHANGING NATURE OF THE LAW, INFORMATION CONTAINED IN THIS PAPER MAY BECOME OUTDATED. IN NO EVENT WILL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, OR OTHER DAMAGES RESULTING FROM AND/OR RELATED TO THE USE OF THIS MATERIAL.

Contents

I. INTRODUCTION I

II. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYEE I

a. Initial Contact With The Employee i

1. Never communicate with an attorney using your employer's e-mail system, accounts, or devices i
2. "Document Theft" – Unauthorized Removal/Copying/Access of Employer Documents iii
3. Preservation Obligations v

b. The Representation Agreement vi

c. Return of Property vi

1. Return of Employer Property vi
2. Return of Employee Property vii

d. Key Documents vii

1. All Agreements and Policies vii
2. Performance Improvement Plan viii
3. Restrictive Covenants viii

e. Post-Employment Considerations xii

1. Social Media xii
2. Unemployment Compensation xiv

f. Emotional Distress xvii

III. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYER XVIII

a. Privacy and Privilege xviii

1. Overview of Privilege xviii
2. For More Related Cases, See the Following: xviii

b. How does the company interpret its monitoring policy? xxiv

c. To what does the employer monitoring policy apply? xxv

d. Emerging Issue: Photocopiers Storing Confidential Information xxvii

e. Ensure Your Trade Secrets Are "Trade Secrets" xxvii

f. Authorized vs. Unauthorized Access xxviii

g. Control of Social Media Accounts xxix

1. The Stored Communications Act xxix

2. Failure to Consider Social Media During Drafting Can Unintentionally Limit the Reach of Restrictive Covenants xxix
3. Courts Look to Substance Over Form – Properly Drafted Non-Solicitation Agreements Can Reach "Passive" Solicitations xxx
4. Unexplored Boundaries xxxi
5. Going Forward xxxiii

h. Develop Policies for Mobile Computing and Work Shifting xxxiii

i. Create Document Return Policies xxxiii

j. Provide for Forfeiture and Clawbacks xxxiv

k. Keep Agreements Jurisdiction-Specific xxxiv

l. Keep Agreements Up-to-Date xxxiv

IV. ARTICLES AND OTHER SOURCES: XXXV

Practical Tips for Counsel for a Departing Employee

By Robert B. Fitzpatrick[1], Robert B. Fitzpatrick, PLLC Washington, D.C.

I. INTRODUCTION

This paper deals with the increasingly complex considerations surrounding the departure of an employee from his or her place of work. The focus is on the legal and practical matters which a practitioner, whether advising the employee or the company, should consider addressing attendant to the termination.

In particular, given the technological changes over the past decade or so, counsel must either herself/himself or some associated person must have a working knowledge of computer technology as well as social media. Without that facility, counsel in this era is almost by definition engaged in malpractice. Innumerable issues, beginning prior to termination and extending through the eve of trial, involve electronically stored information (ESI) as well as social media.

II. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYEE

a. Initial Contact With The Employee

Typically, the Employee will make contact with counsel within several days of his or her termination. More rarely, the Employee will contact counsel when he or she begins to suspect that termination is likely. While counsel has more leeway to shape events in the latter circumstance, in either event the initial phone call is crucial. Regardless of the other items which counsel discusses with this potential clients, there are a few matters which **must** be discussed with the employee at this stage:

1) Communication with attorneys and the Attorney-Client Privilege;

2) "Document Theft" – Unauthorized removal/access/copying of employer documents; and

3) Preservation obligations.

Each of these topics is discussed in turn.

1. Never communicate with an attorney using your employer's e-mail system, accounts, or devices

Counsel for the employee should warn clients *and potential clients* not to use any work-provided account or device to communicate with any attorney. Counsel should emphasize that this applies not only to work provided e-mail accounts, but also to personal e-mail accounts which the employee

[1] Robert Brian Fitzpatrick is the principal in the law firm of Robert B. Fitzpatrick, PLLC in Washington D.C. Mr. Fitzpatrick represents clients in employment law and employee benefits matters. He has concentrated his practice in employment law disputes for over forty years. Mr. Fitzpatrick received his J.D with honors from the George Washington University's National Law Center in 1967. He has been a member of the Bar of the District of Columbia since 1968.

accesses from a work-provided device, including a laptop computer, desktop computer, tablet, cell phone, or any other work-provided device. Counsel should explain that employers can monitor communications made on accounts or devices that they control, and that using employer-provided accounts or devices to communicate with an attorney can compromise the private and privileged nature of the communication. While the primary concern here is written communications, the employee should be advised that both written and verbal communications should be made using personal, not work-provided or work-related devices. Ideally, for reasons explained below, the employee would communicate exclusively from personal devices which are never used for work purposes.

Numerous courts have held that an employee does not have a reasonable expectation of privacy in e-mail communications transmitted from employer-owned devices. *See, e.g.*, *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (in light of an employer policy which placed employees on notice that they could not reasonably expect their internet activity at work would be private, "[employee] lacked a legitimate expectation of privacy in the files downloaded from the Internet [while at work]"); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (finding that there was no reasonable expectation of privacy where the employer had announced that it could inspect computer files); *Thygeson v. U.S. Bancorp*, CV-03-467-ST, 2004 U.S. Dist. LEXIS 18863; 34 Employee Benefits Cas. (BNA) 2097, at **68-69 (D. Or. Sept. 15, 2004) holding that there was no reasonable expectation of privacy in computer files and email where the employer's employee handbook stated that the employer had the right to monitor these communications); *Kelleher v. City of Reading*, Civ. A. No. 01-3386, 2002 U.S. Dist. LEXIS 9408, at **24-25 (E.D. Pa. May 29, 2002) (finding that there was no reasonable expectation of privacy in emails where the employer had stated to employees that no such expectation exists); *Garrity v. John Hancock Mut. Life Ins. Co.*, Civ. A. No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343; 146 Lab. Cas. (CCH) P59,541, at **4-6 (D. Mass. May 7, 2002) (holding that there was no reasonable expectation of privacy despite employee's use of a personal password to limit access, where the employer periodically reminded employees of its email policy that the employer had the right to inspect email usage.

Many courts have extended this rationale to the context of the attorney-client relationship to hold that the attorney-client privilege can be waived by the transmission of e-mails to or from employer-controlled accounts or devices. *See, e.g.*, *Long v. Marubeni America Corp.*, 05 Civ. 639 (GEL) (KNF), 2006 U.S. Dist. LEXIS 76594, at *8 (S.D.N.Y. Oct. 19, 2006) (holding that two employee's email exchanges with their attorneys on the employer provided email system were not protected by the attorney-client privilege where the employer had a policy that prohibited personal use of the computers and systems and provided for the employer's right to monitor communications on its systems, and the employer had notified employees that they had no right of privacy in their communications using the employer's systems); *Alamar Ranch LLC v. County of Boise*, Case No. CV-09-004-S-BLW, 2009 U.S. Dist. LEXIS 101866 (D. Idaho Nov. 2, 2009) (finding that a lawyer's emails sent to the employee / client's work were unprotected by privilege); *Kaufman v. SunGard Inv. Sys.*, Civ. A. No. 05-CV-1236 (JLL), 2006 U.S. Dist. LEXIS 28149, at **11-12 (D.N.J. May 9, 2006) (finding that an employee's emails to her attorney were not protected by the attorney client privilege where the employer's policy expressly provided that all communications on its systems were subject to monitoring); *Scott v. Beth Israel Med. Ctr., Inc.*, 847 N.Y.S.2d 436, 438-39 (2007) (finding that an

employee's communications with his attorney on the employer's systems were not protected by the attorney-client privilege where the employer had notified its employees that the employees had no right of privacy in communications using the employer's systems and that the employer reserved its right to access such communications); *Bonds v. Leavitt*, 647 F. Supp. 2d 541 (D. Md. 2009) (Titus, J.) (holding that where an employee has been notified that there is no reasonable expectation of privacy in that employee's use of the employer's communication systems, any privilege with respect to communications sent by that employee of those systems is waived); *Banks v. Mario Indus. Of Va., Inc.*, 650 S.E. 2d 687 (Va. 2007) (preparing an otherwise privileged communication on a company computer waived the employee's privilege); *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).

Other courts, however, have found that the attorney-client privilege may not be waived, depending on the circumstances of the particular case. *See, e.g.*, *Leventhal v. Knapek*, 266 F.3d 74 (2d Cir. 2001) (holding that an employee had a reasonable expectation of privacy in the contents of his work computer where the employee occupied a private office with a door, had exclusive use of the computer in his office, and did not share use of his computer with other employees or the public, notwithstanding an employer policy which prohibited using the computer for personal business); *Sims v. Lakeside Sch.*, 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. 2007) (holding that public policy demanded that an employee's privileged communications be protected); *Curto v. Med. World Commc'ns, Inc.*, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. 2006) (concluding that an employee had not waived privilege by leaving traces of privileged e-mails on a company computer, despite a company policy which stated that all e-mails viewed on company computers were subject to monitoring); *Nat'l Econ. Research Assocs. V. Evans*, 21 Mass. L. Rep. 337; 2006 Mass. Super. LEXIS 371 (Mass. Super. Ct. 2006) (checking email on company computer did not waive employee privilege); *Convertino v. Dep't of Justice*, 2009 U.S. Dist. LEXIS 115050 (D.D.C. Dec. 10, 2009) (Lamberth, J.) (holding that employees had reasonable expectation of privacy where the employer policy allowed the use of personal email, and where employees were not on notice that their emails were being monitored and stored).

As reflected in many of the cases above, the attorney should be careful to notify his or her clients not only to avoid sending privileged, confidential, or otherwise personal emails using the company's email system, but to avoid sending such emails using company computers or devices altogether. Even where the employee sends such communications using personal, password-protected email accounts, the mere fact that company computers, servers, and/or other devices were used to send the messages may threaten the employee's reasonable expectation of privacy in such communications, and therefore jeopardize any privilege or confidentiality which might have otherwise attached to such emails. This is particularly true where, as in the hypo above, the company has an explicit policy that it reserves the right to monitor all employee communications made on or sent from company computers or devices.

2. <u>"Document Theft" – Unauthorized Removal/Copying/Access of Employer Documents</u>

Employers are increasingly protective of the confidential and proprietary information contained in work-related documents. At the same time, given the increasing portability of electronically stored

information, employees are more likely than ever to copy, retain, or obtain work-related documents which they believe would be helpful in their future career and/or which they feel are their own work-product. While, for many reasons, the problems created by this behavior are particularly acute for electronically stored information, the removal of hard-copy documents should not be overlooked. The employee should be warned that document theft can greatly, and sometimes fatally, compromise her ability to recover against her former employer.

In many cases the employee will possess a large amount of employer documents, whether acquired in the normal course of business, shortly before (or after) termination or, most commonly, both. In this event, the employee should be notified that she will likely be required to return this information to the employer and delete any copies which remain stored on her electronic devices.

The reasons for this are manifold, and will be covered in greater detail later, but document theft will generally violate numerous obligations to which the employee is subject under common, statute, and contract.

The statutory obligations which document theft is most likely to implicate are:

1) The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.*; and

2) The version of the Uniform Trade Secrets Act applicable in the employee's state[2].

The Computer Fraud and Abuse Act is implicated if the employee accessed the employer's documents "without authorization" or exceeded her authorization in accessing the employer's documents. The circuits are deeply split as to how to interpret this element. The First, Fifth, Seventh, and Eleventh Circuits have adopted a broad interpretation of the CFAA under which an employee can be found to have "exceeded" her authorization, or to have lacked authorization, to access files if she intended to make use of those files which were against the employer's interests or which were prohibited by employer policies. *See U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (accessing data employee was otherwise authorized to access but for a prohibited purpose was a violation); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010) (accessing information employee was otherwised authorized to access for the purpose of committing fraud was a violation); *Int'l Airport Ctrs. L.L.C. v. Citrin*, 440 F.3d 318 (7th Cir. 2006) (deleting information from a company-issued laptop after termination, and therefore after employee's authorization to use the laptop had been revoked, was a violation); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (using a program to "scrape" a large quantity of information from a website which the individual was otherwise authorized to access was a violation). The Fourth and Ninth Circuits have adopted a narrow interpretation. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (Cert. dismissed Jan. 2, 2013) (downloading proprietary employer information before resigning for the purpose of competing with employer not a violation); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (same).

---

[2] As of May 2013, the Uniform Trade Secrets Act has been adopted in some form by all states except New York, North Carolina, and Massachusetts.

Despite the existence of the Uniform Trade Secrets Act, the definition of the sort of information which can constitute a "trade secret" varies from state to state. That said, a trade secret is generally information which: 1) Is secret; 2) Derives its value from its secrecy; 3) Which the Company takes reasonable precautions to keep secret; and 4) which is not readily available from public sources. While simply removing trade secrets information is not a crime – indeed, the employee's own knowledge may sometimes constitute a trade secret – employee's counsel should caution him or her against its use on behalf of any future employer. That said, as was well put by a Virginia Circuit Court:

> [The] protection given to trade secrets is a shield, sanctioned by the courts, for the preservation of trust in confidential relationships; it is not a sword to be used by employers to retain employees by the threat of rendering them substantially unemployable in the field of their experience should they decide to resign.

Shenandoah Studios of Stained Glass, Inc. v. Waters, 27 Va. Cir. 464 (Warren Cty. Cir. Ct. 1983).

In addition to the above statutory obligations, the employee will likely be subject to both contractual obligations (non-disclosure agreements, restrictive covenants, confidentiality agreements, and contractual provisions which specifically relate to the use of proprietary employer information) and common law obligations (fidicuary duties, especially the duty of loyalty) which may be implicated by document theft.

You should exercise extreme caution in taking possession or making use of documents which the employee may have obtained from her employer in violation of her statutory, common law, or contractual duties. Nevertheless some courts, in appropriate circumstances, have sanctioned such use. *See Quinlan v. Curtiss-Wright*, 204 N.J. 239 (2010).

3. Preservation Obligations

Counsel should notify the client or potential client of the need to preserve all potentially relevant information. While this includes all hard-copy and electronically stored information which is potentially relevant to the case, it also includes the "metadata" associated with those documents. This metadata is particularly susceptible to inadvertent alteration which, in some cases, can have a potentially serious adverse impact on the employee's ability to maintain a cause of action.

Counsel should be careful to spell out the broad nature of this obligation. For example, not only should the employee not *destroy* documents, but he or she should refrain from altering, copying, or even accessing potentially relevant documents, to the extent possible, in order to preserve the metadata associated with those documents. In cases where metadata (for example, the creation date of documents, the identity of the individual(s) who accessed, altered, or viewed a document, and/or the date on which the document was most recently altered) is likely to play an important role, counsel should seriously consider having relevant devices forensically imaged by a professional.

Beyond devices, however, employee should be counseled that the preservation obligation extends to information contained in commonly used cloud accounts, including all social media accounts (especially Facebook, LinkedIn, Twitter, YouTube, Gmail, etc.). The employee should not alter or delete information on those accounts. Even information which does not seem relevant on its face,

for example, a picture of the employee enjoying a vacation with his or her family, may be potentially relevant depending on the allegations alleged. For example, the above-mentioned picture might be relevant if the employee later attempts to recover damages for emotional distress.

b. The Representation Agreement

Increasingly, employers are responding to suits filed by employees by initiating litigation or counterclaims against the plaintiff – typically because the client has downloaded documents from the employer's systems – your representation agreement should address that possibility. Most importantly, you should specifically address whether or not your firm is responsible to represent the client in that event and, if so, how you will be compensated.

c. Return of Property

1. Return of Employer Property

As stated, oftentimes the client, prior to retaining you, already has in his/her possession hard copies of documents and/or digital/electronic documents that are not personal, but rather relate to the business of the employer. Some courts (*e.g. Quinlan v. Curtiss-Wright*, 204 N.J. 239 (2010)) have indicated that, in some circumstances, the employee may retain the documents, and employee's counsel may use the documents in evaluating and prosecuting claims. Other courts, have found various bases upon which the employer can proceed against the employee because the employee retained and used the documents. *See, e.g. Resource Ventures, Inc. v. Resources Mgmt. Intern., Inc.*, 42 F. Supp. 2d 423 (D. Del. 1999) (cause of action for conversion regarding misappropriated documents);

Sometimes, the employee has acquired the documents in the normal course of business. All too many employers still do not have strict rules prohibiting their employees from having company documents on their personal computers or in hard copy at home. Increasingly, employers are putting in place confidentiality agreements, non-disclosure agreements, employment agreements, electronic usage agreements, and other policies that prohibit or restrict the "export" of documents outside of the workplace.

Many times, counsel for the employee would be well advised to work with the employee to return the documents, regardless how they were obtained. Having said that, when the documents have not been obtained in the normal course of business, the return of the documents creates significant dilemmas for employees' counsel. On the one hand, counsel wants her/his client to "do the right thing" and return the documents, but the downside could well be to expose the client to an after-acquired evidence defense, as well as potential civil, and even criminal, exposure. Normally, in my experience, if counsel initiates the return of the documents, the risk of civil, much less criminal, liability, significantly dissipates. Needless to say, counsel needs to fully advise the client regarding the risks and the pros and cons associated with this process.

While returning the documents may sound simple to some, my experience has been that, where management counsel is uncooperative or simply technologically dim, the return of the documents can technologically become somewhat complicated. The principal complication is, in layperson's language, the digital "separation" of employer ESI from employee ESI as, all too often, the

employer documents are on the employee's personal laptop and not necessarily readily segregable from the employee's personal ESI. With the cooperation of management counsel, there are cost-effective protocols to separate the two and return employer documents.

2. Return of Employee Property

We all know the scenario of the employer calling the employee into a meeting at which, invariably, an HR representative is present to terminate the employee effective immediately, and then have the employee escorted out of the facility. Sometimes, the employer gives the employee, under the supervision of an HR representative, a brief opportunity to gather her/his personal possessions and is then escorted out of the facility, carrying the possessions in a cardboard box. I can't begin to count the number of times that I have heard that same story, and the same reaction of every employee: They treated me like a common criminal. I was humiliated and had to be escorted out the door with a cardboard box filled with pictures of my family. I will never forget or forgive them for treating me that way.

Smarter employers arrange to "freeze" the employee's work site and arrange for the employee to return to the facility after hours or on a weekend to retrieve her/his personal possessions. It is good practice for the employer to assure that no one tampers with the employee's worksite.

The other exiting scenario that I have heard on countless occasions goes as follows: "So, Mr. Fitzpatrick, I came back the following weekend to retrieve my personal possessions, and I could not find such-and-such or this-and-that, all of which had disappeared."

Another approach by employers is to arrogate to itself the task of determining what belongs to the employee, packing it all up and fed-exing it to the employee. With great frequency, what arrives by federal express is not everything that belongs to the employee, and the already tenuous relationship is yet further frayed.

d. Key Documents

1. All Agreements and Policies

1. Early on, counsel for the employee needs to determine the agreements and policies applicable to the employee. We first ask the employee to provide us with a copy of all such documents, and once we enter an appearance, we ask the same of management counsel. Among the documents that should be on counsel's "checklist" are the following:

    a. The employee's offer letter;

    b. Any written employment agreement;

    c. Any non-compete agreement;

    d. Any non-solicitation agreement;

    e. Any confidentiality or non-disclosure agreement;

f. The employee handbook;

g. The employer's personnel policies and procedures;

h. Any alternative dispute resolution (ADR) agreement or program;

i. Any agreement or program shortening statutes of limitation;

j. Any social media policies;

2. Performance Improvement Plan

Many times, the first phone call from the employee has been triggered byb the employer placing the employee on a performance improvement plan (PIP). And, almost universally, the first issue that counsel needs to address with the employee is the employee's reluctance to sign the PIP. Despite repeated blandishments by the employer that the employee "must" sign the PIP, most employees do not want to sign because they perceive that act to be an acknowledgment of the accuracy of the underlying basis of the PIP. And, sometimes, employers actually put language before the signature that indeed suggests that the employee does acknowledge that her/his job performance was questionable.

Employers ought to clearly and boldly state that by signing the PIP, the employee merely acknowledging that s/he received and read the document. In addition, employers ought allow employees to add any disclamatory language before signing the PIP. We all know that it is extraordinarily rare the employee, immediately upon receipt of the PIP, embraces it wholeheartedly. The reality that we all are familiar with, is that the employee initially rejects, at least in part, the notion that her/his performance has been questionable. As, supposedly, a PIP is a tool to salvage the employee whose performance is off-base, the employer should give the employee some space to absorb the PIP. In my experience, if indeed the employee is treated as though their performance can be resurrected, the percentage of cases in which it does increases significantly. Unfortunately, the PIP has become all-too-often just the "paper trail" used to support a decision, already made, to terminate the employee, and the PIP is merely "window dressing" in an attempt to convince Judge and Jury that the employee was given a full and fair opportunity to turn their performance around. Employee's counsel should work with the employee to respond to the PIP in writing in a respectful and disarming manner. Counsel should advise the client, without rhetorical flourishes, to rebut the factual premise(s) for the PIP, but then to embrace the reality that the employer has the ultimate power to impose the PIP regardless of how the employee may, rightly or wrongly, perceive her/his job performance. If the PIP lacks a specific improvement plan, we counsel our clients to delineate such a plan, describing what the employee intends to do to address performance deficiencies outlined in the PIP. If the employer does not reject the employee's plan, and the employee meets all of the bogies set forth in her/his plan, the employer, when it terminates, has potentially lost its argument that it gave the employee an opportunity to improve. Indeed, the employee may have converted the PIP into an offensive weapon for the employee to use in future adversarial proceedings.

3. Restrictive Covenants

Employees are increasingly likely to be subject to some form of restrictive covenant. In addition to traditional non-compete and non-solicitation agreements, employee's counsel should also be sensitive to the possibility that more traditional clauses, such as confidentiality and non-disclosure provisions, could form the basis for a back-door non-compete down the road, especially in states, such as New York, which adhere to the "inevitable disclosure" doctrine.

Many employers will require their employees to execute restrictive covenants either at the time of hire or at some point during the course of employment, and will merely ask that the employee "reaffirm" those documents at the time of his or her departure. Others, however, will attempt to include new or additional restrictive covenants in severance agreements, settlement agreements, or other separation documents. Any such provisions should be scrutinized by both the departing employee and counsel.

A. *Enforceability and Reason for Termination*

Whether a court will enforce a restrictive covenant against a terminated employee is a context-sensitive decision. While counsel for a departing employee should review any existing or potential restrictive covenants to determine both their scope and their enforceability as a matter of course, the topic of the enforceability of restrictive covenants in various termination scenarios bears special analysis here.

Some courts have declined to enforce a non-compete agreement against an employee who is terminated in "bad faith" – especially if the termination is close in time to the procurement of the restrictive covenant. *See Robinson v. Computer Serv. Ctrs., Inc.*, 346 So. 2d 940 (Ala. 1977); *Am. Credit Bureau, Inc. v. Carter*, 462 P.2d 838 (Ariz.Ct. App. 1969); *Rao v. Rao*, 718 F.2d 219 (7th Cir. 1983) (all refusing to enforce restrictive covenants against employees terminated in bad faith). However, bad faith is not the only circumstance which may influence a court's decision regarding the enforceability of a restrictive covenant. In *Gomez v. Chua Med. Corp.*, 510 N.E.2d 191 (Ind. Ct. App. 1987), the Indiana Court of Appeals described four basic scenarios under which an employee might depart from an employer: 1) a voluntary departure; 2) a discharge for good cause; 3) a bad faith discharge; and 4) termination without either good cause or bad faith. Of these circumstances, the Court in *Gomez* noted that otherwise valid covenants are "clearly enforceable" when the employee departs voluntarily. Where the employee is discharged in bad faith, equity will generally bar enforcement of the covenant. However, the court declined to require that the employer demonstrate "good cause" for an employee's termination as a requisite for the enforcement of an otherwise valid restrictive covenant. *See also* Andrew J. Gallo*, A Uniform Rule for Enforcement of Non-Competition Contracts Considered in Relation to "Termination" Cases,* 1 U. Pa. J. Lab. & Emp. L. 719 (Fall 1998).

Other courts have declined to enforce otherwise reasonable restrictive covenants against an employee who is discharged without cause, who is constructively discharged, or who is terminated due to a downturn in business. *See Bailey v. King*, 398 S.W.2d 906 (Ark. 1966) (refusing to enforce when employee was terminated without cause); *Bishop v. Lakeland Animal Hosp., PC*, 644 N.E.2d 33 (Ill. App. Ct. 1994) (endorsing position of Seventh Circuit that "implied promise of good faith" prevents enforcement of restrictive covenants when employee is terminated without cause);

Insulation Corp. of Am. v. Brobston, 667 A.2d 729 (Pa. Super. Ct. 1995) ("The employer who fires an employee for failing to perform in a manner that promotes the employer's business interests deems the employee worthless. Once such a determination is made by the employer, the need to protect itself from the former employee is diminished…[u]nder such circumstances, we conclude that it is unreasonable as a matter of law to permit the employer to retain unfettered control over that which it has effectively discarded as worthless to its legitimate business interests.").

This is an issue that has resulted in various approaches by the state courts. In *Ruhl v. FA Bartlett Tree Expert Co.*, 225 A.2d 288 (Md. 1967), the Court of Appeals noted that "Ruhl's employment [had] been terminated by Bartlett through no fault of Ruhl's" and had it been otherwise, "a different legal situation might well have been presented." *Citing MacIntosh v. Brunswick Corp.*, 215 A.2d 222 (Md. 1965). Similarly, in *SIFCO Indus. Inc. v. Advanced Plating Tech., Inc.*, 867 F. Supp. 155 (S.D.N.Y. 1994), the court held that covenants not to compete were unenforceable where, upon acquiring the company with whom the employees had entered into covenants, the successor company terminated employees' positions by closing factory at which employees worked.

The Montana Supreme Court has held that employers are ordinarily not permitted to enforce a non-compete provision where the employer terminates the employment relationship. *Wrigg v. Junkermier, Clark, Campanella, Stevens, P.C.*, 265 P.3d 646 (Mt. 2011). Where an employee in Montana is terminated without cause, "courts should scrutinize highly a covenant's enforcement given the involuntary nature of the departure… An employer's decision to end the employment relationship reveals the employer's belief that the employee is incapable of generating profits for the employer. It would be disingenuous for an employer to claim that an employee was worthless to the business and simultaneously claim that the employee constituted an existential competitive threat." 265 P.3d at 652.

By contrast, Florida took a different approach in *Twenty Four Collection v. Keller*, 389 So. 2d 1062 (Fla. Dist. Ct. App. 1980). There, defendant-former employee had been discharged by plaintiff-former employer and was subject to a non-competition agreement which became effective "[i]n the event of the termination, voluntarily or involuntarily," of defendant's employment. Reversing a lower court's attempt to fashion an equitable remedy, the Court of Appeals held that "[t]here is no doubt either of the applicability of [Fla. Stat. § 542.12(2) (1977)] nor the enforceability of agreements which come within its terms" and further finding that the non-compete agreement to which defendant was subject "is specifically validated" by Fla. Stat. § 542.12(2) (1977). Finally, the Court held that, in general, the only authority it possesses of the terms of non-competitive agreements is "to determine, as the statute provides, the reasonableness of its time and area limitations." *Cf. also Ins. Assocs. Corp. v. Hansen*, 723 P.2d 190 (Idaho Ct. App. 1986) (enforcing non-compete without addressing circumstances of termination); *Weber v. Tillman*, 913 P.2d 84 (Kan. 1996) (enforcing non-compete without addressing fact that defendant was terminated without cause); *Cellular One, Inc. v. Boyd*, 653 So. 2d 30 (La. Ct. App. 1995) (no difference in analysis applied in upholding non-competes against two employees, one who resigned and one who was terminated); *Hogan v. Bergen Bruswig Corp.*, 378 A.2d 1164 (N.J. Super Ct. App. Div. 1977) (not addressing circumstances of dismissal).

Several courts have shown reluctance to enforce even otherwise reasonable agreements against employees who are discharged without cause (*Bailey v. King*, 398 S.W.2d 906 (Ark. 1966)), who are constructively discharged (*Bishop v. Lakeland Animal Hosp., PC*, 644 N.E.2d 33 (Ill. App. Ct. 1994); *Ma & Pa., Inc. v. Kelly*, 342 N.W.2d 500 (Iowa 1984) or who would otherwise suffer "undue hardship" for being terminated through no fault of their own (*MacIntosh v. Brunswick Corp.*, 215 A.2d 222 (Md. 1965)). *See also Post v. Merrill Lynch, Pierce, Fennerr & Smith, Inc.*, 397 N.E.2d 358 (N.Y. 1979) ("Where the employer terminates the employment relationship without cause,…his action necessarily destroys the mutuality of obligation on which the covenant rests"); *In re UFG Int'l Inc.*, 225 B.R. 51 (Bankr. S.D.N.Y. 1998) ("an employer cannot hobble his employee by terminating him without cause and then enforcing a restriction that diminishes his ability to find comparable employment.") The Virginia Supreme Court, in *Clinch Valley Physicians, Inc. v. Garcia*, 414 S.E.2d 599 (Va. 1992), affirmed a lower court's decision not to enforce a covenant not to compete because the employee's termination had occurred when his contract lapsed. Interpreting the contract narrowly to require "cause" for termination, the Supreme Court affirmed.

B. *Regardless of Enforceability, Exercise Caution*

Regardless of whether the restrictive covenant is ultimately determined to be enforceable, counsel for a departing employee should exercise caution in both her interpretation of the covenant(s) and in the advice which she provides to her client. Even unenforceable restrictive covenants can result in costly litigation, and the employee may not be the only target. In addition to bringing actions against the former employee for breach of his contractual obligations, it is growing increasingly common for a former employer to bring actions against the former employee's new employer. Such causes of action can include:

1) Tortious interference with contract – if the new employer knew of the employee's restrictive covenants and caused, induced, or encouraged the employee to violate them; and

2) Misappropriation of trade secrets – a statutory claim which will vary based on the content of the forum state's version of the Uniform Trade Secrets Act.

Needless to say, some employers quickly decide that the employee is simply not worth the trouble and attempt to resolve their legal issues by the expedient measure of terminating the employee.

C. *Advising the Employee*

In advising the departing employee, you should therefore be careful to discuss the following items:

1) The employee should be careful to stay well within the bounds of his or her restrictive covenants;

2) Even if the covenants are unenforceable, or would likely be limited by a court, the employee should be aware that the cost of engaging in the legal proceedings necessary to achieve this outcome would potentially be quite significant;

3) If the employee is worried that his new employment might violate restrictive covenants to which he or she is subject, the most efficient solution is to negotiate a carve out or compromise with the former employer as part of the departing employee's separation / settlement agreement.

4) If that cannot be achieved, then the employee should consider asking his or her new employer for indemnification as to any legal expenses which he or she may incur in the course of defending against future action(s) brought by his or her former employer.

Even if the employee is not subject to a restrictive covenant, counsel should emphasize that he or she will remain subject to various statutory and common-law requirements which could restrict his or her ability to compete with his or her former employer. While many of these are discussed in more detail below, they include:

1) Fiduciary duties, and especially the Duty of Loyalty;

2) The Computer Fraud and Abuse Act; and

3) The relevant version(s) of the Uniform Trade Secrets Act.

e. Post-Employment Considerations

1. Social Media

A. *Ownership*

In *PhoneDog v. Kravitz*, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), plaintiff sued a former employee, alleging that the username, password, and "followers" of a twitter account created by the former employee constituted trade secrets within the meaning of the California Uniform Trade Secrets Act ("UTSA"), Cal. Civ. Code § 3426.1. The username and password had originally been provided to defendant by plaintiff. Defendant moved to dismiss for failure to state a claim, arguing that the followers of the account "have been publicly available for all to see at all times", and that the account password "do not derive any actual or potential independent economic value under the UTSA because they do not provide any substantial business advantage." Defendant further argued that he, not plaintiff, initially created the password, and that plaintiff did not make reasonable efforts to maintain its secrecy. The Court denied defendant's motion to dismiss for failure to state a claim, with regards to plaintiffs claims for misappropriation of trade secrets and conversion, holding simply that because plaintiff had sufficiently described the subject matter of the trade secret with particularity, and has alleged that plaintiff failed to relinquish the account's password, plaintiff had sufficiently stated a claim, and that defendant's additional challenges would await summary judgment. However, the court dismissed plaintiff's claims for intentional and negligent interference with prospective economic advantage, explaining that California law does not protect "potential" relationships which are "at most a hope for an economic relationship and a desire for a future benefit." Explaining that the "nature of PhoneDog's purported economic relationship" with the account's followers was unclear, the Court agreed with defendant that plaintiff had failed to allege actual disruption of any relationship or harm therefrom.

An employer can claim ownership of an Executive's LinkedIn account that it required the Executive to open and maintain, according to the holding in *Eagle v. Morgan*, No. 11-4303, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011). In *Eagle*, the employer had required the executive to open the account, maintain it, use it to advertise the employer's credentials and services. The employer was also involved in the creation, operation, and monitoring of the account. The employer's victory on this point was not unequivocal, however. While the court refused to dismiss the employer's claim for "misappropriation of an idea" and unfair competition, it did dismiss the employer's claims for misappropriation of trade secrets and conversion. In dismissing the latter two causes of action, which were based around the executive's use of the "connections" and other content of the LinkedIn page, the court held that such information did not constitute a trade secret because it was publicly posted on the internet.

B. *Access Issues*

Legislation restricting the ability of employers to request usernames, passwords, and/or access to the social media accounts of current and former employees has been enacted or considered in numerous states, including Illinois (Public Act 097-0875, 820 ILCS 55/10, effective Jan. 1, 2013), Maryland (Md. H.B. 964, S.B. 433, Labor & Empl. § 3-712, effective Oct. 1, 2012), Michigan (Public Act No. 478, effective Dec. 28, 2012), Minnesota (Minn. SF 2565, introduced March 27, 2012), Massachusetts, and California (A.B. No. 1604, introduced Feb. 7, 2012).

The Maryland legislation was birthed as a result of a controversy that ensued between the Maryland Department of Public Safety and Correctional Services and the ACLU of Maryland when, back in 2010, the Department required job applicants to submit usernames and password information related to their social media sites, purportedly to check for gang affiliations. The Department suspended and then dropped the requirement after protests by the ACLU. In this correspondence, the ACLU asserted that the Department's conduct violated the Stored Communications Act, 18 U.S.C. § 2701-11 and its Maryland analog, Md. Courts & Jud. Proc. Art., § 10-4A-01, *et seq.* The ACLU also noted that the Department's conduct may give rise to violations of the common law tort of invasion of privacy and arguably chilled the First Amendment rights of employees. The ACLU argued that "there can be little question but that forced 'authorization,' such as that demanded of [the applicant], is not proper authorization under the SCA, given the disparate bargaining power of the employer and employee or applicant." In the wake of the ACLU's allegations, some commentators, such as Orin Kerr of the George Washington University School of Law, have likened surrendering social media passwords to handing over the keys to one's home. *See* Editorial Staff, "Job Seekers Need Protection for Their Social Media Accounts", *SF Examiner* (March 25, 2012).

Two United States Senators have requested that the Department of Justice and EEOC review the matter, citing an uptick in requests by employers for job applicants' username and password for social media sites. The letter to DOJ notes that this practice appears to violate Facebook's terms of service and cites cases which, according to the authors, may subject employers who request usernames and passwords from applicants to liability. *See* Blumenthal, Richard "Blumenthal, Schumer: Employer Demands for Facebook and Email Passwords as a Precondition for Job

Interviews May Be a Violation of Federal Law; Senators Ask Feds to Investigate", Richard Blumenthal U.S. Senator for Connecticut Website (March 25, 2012) (available at www.blumenthal.senate.gov) *See also Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *Pietrylo v. Hillstone Rest. Group*, Civ. No. 06-5754, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009). The letter follows with a request that the DOJ issue a legal opinion regarding whether requesting and using job applicants' social media passwords violates current federal law, including the Stored Communications Act and the Computer Fraud and Abuse Act.

On another front, Facebook recently threatened to sue employers who request that job applicants provide access to their Facebook profiles. Facebook's Chief Privacy Officer, Mr. Erin Egan, in a statement issued March 23, 2012, stated: "We'll take action to protect the privacy and security of our users, whether by engaging policymakers or, where appropriate, by initiating legal action." Mr. Egan indicated that asking for someone else's Facebook password violates Facebook's user agreement.

Courts are divided as to the discovery of social media passwords in particular. As reported by Ethan Wall on the Richman Greer Blog, some courts have ordered individuals to supply passwords to Facebook and other websites. *See* Ethan Wall, "Judge Orders Divorce Couple to Turn Over Facebook Password to Lawyers", Richman Greer P.A. (Dec. 5, 2011) (available at: http://richmangreerblog.com/2011/12/judge-orders-divorce-couple-to-turn-over-facebook-password-to-lawyers/); *See also Gallion v. Gallion*, FA 114116955S (Ct. Super. Ct. Sept. 30, 2011). However, as noted by Daniel E. Cummins at the Tort Talk blog, the court in *Kalinowski v. Kirschenheiter & Nat'l Indemn. Co.*, No 6779 of 2010 (C.P. Luz. Co. 2011), other courts have refused to order the production of social media passwords. *See* Daniel E. Cummins, "Judge Van Jura of Luzerne County Bucks the Trend on Facebook Discovery in a Facts-Specific Case", Tort Talk Blog (Dec. 4, 2011) (available at: http://www.torttalk.com/2011/12/judge-van-jura-of-luzerne-county-bucks.html). Note that the court in *Zimmerman*, which ordered discovery of Facebook materials, emphasized that its decision should not be read to open the door to unlimited discovery of a party's private social media accounts. *Zimmerman*, 2011 Pa. Dist. & Cnty. Dec. LEXIS 187.

2. Unemployment Compensation

A. *In General*

While eligibility for unemployment benefits will obviously vary from state to state, a few precepts hold. First, as described above, when negotiating a settlement agreement, plaintiff's counsel should include a *defensible* reason for her client's termination which is non-performance based. When it is plausible, termination as part of a company-wide reduction in force in which the client's position was eliminated is to be preferred. However, it is often the case that the Company plans to replace the client, no other individuals were terminated, or other factors exist which would render such an explanation implausible. In an event, when agreeing to the reason for termination, plaintiff's termination, plaintiff's counsel should be careful that the given reason does not compromise the client's interests in obtaining unemployment compensation.

Another common clause in separation and/or settlement agreements is for the employer to agree not to oppose any application for unemployment benefits. Such clauses must be handled carefully

by both employee's and employer's counsel to avoid any implication that the employer would be required or encouraged to mislead any state agency which may contact them regarding the circumstances surrounding the employee's departure. Sample language for such a clause is included below.

> Employer agrees that it will not actively contest any claim for unemployment compensation that Employee may choose to make. Nothing in this Agreement will, or is intended to, prevent Employer from providing accurate and truthful responses to inquiries from Employer's third party unemployment compensation administrator, or any state or local agency administering such benefits.

B. *Retaliatory Opposition to Application for Unemployment Benefits*

If an employer chooses to oppose an employee's application for unemployment benefits the employee may have a claim for retaliation in appropriate circumstances. An interesting split has developed in the federal district courts as to whether an employer's opposition to a former employee's application for unemployment benefits, if motivated by a retaliatory animus, is actionable. The weight of authority, particularly after *Burlington N. & Sante Fe R.R. Co. v. White*, 126 S. Ct. 2405 (2006), has been to find that such conduct is actionable. Indeed, as it arises after the termination of the employment relationship – and thus potentially after the execution of the waiver of claims contained in a separation agreement – such claims may be difficult to extinguish. *See Steele v. Schafer*, 535 F.3d 689, 696 (D.C. Cir. 2008) (noting in*dicta* that plaintiff's claim that employer retaliated by falsely contesting plaintiff's unemployment benefits "involve[d] conduct that… the Supreme Court has already indicated can support a retaliation claim" in *Burlington v. White*); *Koger v. CT. Woody*, No. 3:09-cv-90, 2009 U.S. Dist. LEXIS 77433 (E.D. Va. Aug. 28, 2009) (protection under Title VII extends to both employees and "former employees" and a frivolous denial of unemployment benefits may constitute retaliation); *Roa v. LAFE*, 955 A.2d 930 (N.J. App. Div. 2008) (employer's post-termination conduct in terminating medical benefits and opposing request for unemployment stated cause of action);*Petrunich v. Sun Bldg. Sys., Inc.*, 2006 U.S. Dist. LEXIS 69043 (M.D. Pa. Sept. 26, 2006) ("under the standard articulated in [*Burlington Northern*], the opposition to [a plaintiff's] claim for unemployment compensation benefits [may be] an adverse employment action because it [could]).

In *Williams v. W.D. Sports, N.M., Inc.*, 497 F.3d 1079 (10th Cir. 2007) the Tenth Circuit addressed a situation in which an employee was terminated after filing a grievance regarding gender discrimination with the Human Rights Division of the New Mexico Department of Labor. Shortly afterwards, the employee was terminated, and was told by the employer's President that, if she challenged him, he would "ruin your marriage." Subsequently the employer opposed plaintiff's request for unemployment benefits on the basis that plaintiff was terminated "for cause" due to sexual misconduct, drinking, and theft of company property. No evidence was provided to substantiate these charges. During the hearing on plaintiff's unemployment benefits application, the employer's attorney allegedly said "[i]f you will drop your Human Rights [discrimination] claim, I won't fight you on your unemployment." Williams was later awarded unemployment benefits. The district court, in a ruling handed down prior to *Burlington Northern*, dismissed plaintiff's claim for retaliation with respect to unemployment benefits, finding that because plaintiff had suffered no

delay or cessation of benefits that the employer's opposition did not constitute an adverse influence. *Williams v. W.D. Sports N.M., Inc.*, 2005 U.S. Dist. LEXIS 46146 (D.N.M. Feb. 25, 2005). The Tenth Circuit reversed under the holding of*Burlington Northern*, holding that a jury could have concluded that the employer's conduct was sufficiently adverse that it might have dissuaded plaintiff from making or supporting a charge of discrimination. *Williams*, 497 F.3d 1079 (10th Cir. 2007); *See also* Michael R. Lied, *Employer's Challenge to Unemployment Benefits May be Evident of Unlawful Retaliation*, Illinois State Bar Assoc., Section on Labor & Employment Law Newsletter (Feb. 8, 2008) (available at: http://www.howardandhoward.com/news/pub.asp?id=94); Daniel M. Combs, *Employer's Stated Willingness Not to Oppose Unemployment Benefits Claim if Employee Dropped Lawsuit Could be Retaliation*, Sherman & Howard Client Advisory (Oct. 2008) (available at:http://www.sah.com/docs/news/UnemploymentRetaliationAdvisoryOct2008.pdf).

A minority of courts, including several decisions which predate*Burlington Northern*, adhere to the view that an employer's decision to exercise its legal right to oppose unemployment benefits does not constitute prohibited retaliation. Among those authorities is Judge Mae A. D'Agostino of the Northern District of New York who held, in *Burnett v. Trinity Inst. Homer Perkins Ctr., Inc.*, 2011 U.S. Dist. LEXIS 48999 (N.D.N.Y. May 6, 2011) that "defendant's decision to exercise its legal rights and oppose plaintiff's receipt of unemployment benefits… cannot serve as a basis for a retaliation claim." *See also Powell v. Honda of Am.*, No. 06-cv-979, 2008 U.S. Dist. LEXIS 56991 (S.D. Ohio July 22, 2008) (refusing as futile for failure to state a claim plaintiff's request to amend complaint to include cause of action for retaliation for opposition to request for unemployment benefits – the court, relying on pre-*Burlington Northern* authority, found that opposition was "not retaliatory in nature" because it was "clearly the employer's right and duty."); *Roman v. Cornell Univ.*, 53 F. Supp. 2d 223, 245 (N.D.N.Y. 1999) (holding that a retaliation based on opposing plaintiff's application for unemployment benefits could not survive a motion for summary judgment because it was "not an adverse employment action"); *Kowalski v. Kowalski Heat Treating, Co.*, 920 F. Supp. 799, 805 (N.D. Ohio 1996) (opposition to unemployment benefits was not the sort of adverse action contemplated by Ohio Legislature); *Baker v. Summit Unlimited, Inc.*, 855 F. Supp. 375 (N.D. Ga. 1994) (granting summary judgment for the defendant because it had a right to defend the unemployment action after plaintiff pursued benefits); As noted in *Adamchik v. Compservices, Inc.*, No. 10-949, 2010 U.S. Dist. LEXIS 130133 (W.D. Penn. Dec. 9, 2010), the viability of these decisions, many of which predate *Burlington Northern* or rely upon pre-*Burlington Northern*authority to support their conclusions, is an open question. *See also Mohamed v. Sanofi-Aventis Pharms.*, 2009 U.S. Dist. LEXIS 119871 (S.D.N.Y. Dec. 22, 2009) ("[i]n the wake of *Burlington*…, there is now a substantial question as to the validity of precedent holding that a post-termination [event] may not be an adverse employment [action]") (citations omitted).

Retaliation is particularly likely to be found where opposition to unemployment benefits is meritless. For example, in *Williams*, the President admitted at trial that the grounds asserted during the unemployment hearing did not form the basis for plaintiff's termination. Similarly, in *Wright v. Life Start Ctrs., Inc.*, 2000 U.S. Dist. LEXIS 16424 (N.D. Ill. Oct. 19, 2000) the defendant-former employer made false statements during an unemployment hearing which resulted in the initial denial of plaintiff's unemployment benefits. The Court, in a pre-*Burlington Northern* decision, reasoned that this constituted a sufficient adverse action to give rise to a cause of action for retaliation. Many

other courts have reached similar conclusions. *SeeBetts v. Container Corp.*, No. 95-1064, 1997 U.S. App. LEXIS 10648 (7th Cir. May 7, 1997) (holding that *Robinson v. Shell Oil Co.*, 117 S. Ct. 843 (1997) made clear that Title VII extends to former employees, and thus that it could apply to opposition to unemployment benefits); *Liverpool v. Conway, Inc.*, 2009 WL 1362965 (E.D.N.Y. May 15, 2009) (refusing to dismiss for failure to state a claim plaintiff's claim for retaliation based on allegedly meritless opposition to unemployment benefits); *Grace v. Starwood Hotels & Resorts Worldwide, Inc.*, C.A. No. 6-1203, 2008 U.S. Dist. LEXIS 10951 (W.D. Pa. Feb. 14, 2008) (opposing unemployment benefits can constitute retaliation however, here the Court found that defendant-former employer established that its conduct was in accordance with its regular practice and plaintiff failed to meet his burden of proof under *McDonnell Douglas*). However, even post-*Burlington Northern*, if the employer possessed a legitimate reason for terminating Plaintiff, it is unclear whether opposing unemployment benefits can constitute retaliation. *See Spencer v. CSL Plasma, Inc.*, No. 3:10-cv-00262, 2011 U.S. Dist. LEXIS 102846 (W.D. Ky. Sept. 12, 2011) (while opposition to unemployment benefits can constitute retaliation, if defendant has legitimate, non-discriminatory basis for its actions plaintiff must still meet burden-shifting obligations under *McDonnell Douglas*); *Hatton v. United Parcel Serv.*, No. 05-97-JBC, 2006 U.S. Dist. LEXIS 47734 (E.D. Ky. July 7, 2006) (no claim for retaliatory denial of unemployment benefits, at least where employee presented no evidence to rebut employer's contention that opposition was made in good faith).

One of the remaining questions is whether a non-frivolous opposition to unemployment benefits, animated by retaliatory intent, gives rise to a violation, or whether only challenges to unemployment benefits which are both frivolous and retaliatory in nature are prohibited. This debate mirrors that which is discussed in our paper on retaliatory counterclaims.

f. Emotional Distress

Counsel should determine whether the employee has been seeing a mental health practitioner, when the individual began such therapy, and whether events at work triggered therapy and whether events at work and the emotional consequences are the exclusive subject for discussion with the therapist. Counsel ought obtain a release from the employee so that the therapist's records can be obtained. Counsel ought not to advance an emotional distress claim, even in a demand letter, without first determining whether highly personal matters are being exposed to the discovery process. In short, counsel ought advise the employee that an allegation of emotional distress over and above what has been characterized as "garden variety" emotional distress will expose the employee to highly intrusive discovery, including the release of the therapist's records to the employer, a deposition of the therapist, and a Rule 35 mental examination of the employee. And, in a handful of jurisdictions, even the allegation of "garden variety" emotional distress can expose the employee to such intrusive discovery.

Now, having forewarned the client does not necessarily mean that a claim of significant emotional distress ought not be pled. Rather, the employee should be allowed to make a fully informed decision as to whether or not to proceed with such a claim for damages.

III. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYER

a. Privacy and Privilege

1. Overview of Privilege

In Convertino v. Dep't of Justice, 674 F. Supp. 2d 97; 2009 U.S. Dist. LEXIS 115050 (D.D.C. Dec. 10, 2009), Judge Lamberth summarized the issue as follows:

> The question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable. In order for documents sent through e-mail to be protected by the attorney-client privilege there must be a subjective expectation of confidentiality that is found to be objectively reasonable. There are four factors to determine reasonableness: (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? Each case should be given an individualized look to see if the party requesting the protection of the privilege was reasonable in its actions. *Id.* at *33.

2. For More Related Cases, See the Following:

   A. *United States v. Hamilton, 701 F.3d 404, 406 (4th Cir. 2012), cert. denied, 2013 U.S. LEXIS 2811 (Apr. 15, 2013).*

In *Hamilton*, a criminal case, the Fourth Circuit affirmed a district court finding that e-mails between the defendant and his wife were not protected by the marital privilege. The court found as follows:

While the court noted the importance of the protections provided by the marital communications privilege, it ultimately found that Hamilton's employer had put him on advance notice of periodic inspections of any and all email stored on the employer's system. The court also noted that Hamilton was required to acknowledge this email inspection policy each time he logged on to his office computer.

The court also noted that Hamilton never took precautions to separate and protect his personal emails, even after repeatedly acknowledging the policy. Hamilton used his work email account, on his office computer, to send emails to his wife. These facts were sufficient for the court to find that the district court did not abuse its discretion when ruling that the emails were not protected by the marital communications privilege.

For more information on this case, *see*:

1. Robert B. Fitzpatrick, Fourth Circuit Issues Startling Waiver Decision, Robert B. Fitzpatrick, Dec. 14, 2012, http://robertfitzpatrick.blogspot.com/2012_12_01_archive.html

2. Debevoise & Plimpton, LLP, Client Update: Work Emails to Spouses May Not Be Protected By Marital Privilege, Dec. 14, 2013, http://www.debevoise.com/files/Publication/61db6878-5ff3-4061-8597-2907a3c9606d/Presentation/PublicationAttachment/ecb91f36-a2bf-47d2-8773-30807fac64af/Work%20Emails%20to%20Spouses%20May%20Not%20be%20Protected%20by%20Marital%20Privilege.pdf

3. Kevin G. Walsh, Use of Work Computer Results in Waiver of Marital Communication Privilege, E-Discovery Law Alert, Feb. 21, 2013, http://www.ediscoverylawalert.com/2013/02/articles/corporate-information-records/use-of-work-computer-results-in-waiver-of-marital-communication-privilege/ (noting that the Hamilton case is contrary to the Stengart holding, in that the former says that employee's legal privileges can be waived when on they are on work computers and have been sufficiently notified of the employer's computer monitoring policy)

B. *City of Ontario v. Quon, 130 S. Ct. 2619; 177 L. Ed. 2d 216; 2010 U.S. LEXIS 4972 (June 17, 2010).*

The Supreme Court reversed a Ninth Circuit decision that a police officer had a reasonable expectation of privacy in text messages sent to his wife using a city-owned pager, holding as follows:

The Court assumed without deciding that there was a Fourth Amendment expectation of privacy in the employee's text messages, but found that the employer's search of the text messages was reasonable under the Fourth Amendment because it was work-related.

The Court distinguished the facts of *Quon* from those of *Stengart v. Loving Care Agency, Inc.*, 208 N.J. Super. 53; 504 A.2d 1207; 1986 N.J. Super. LEXIS 1163 (N.J. Super. Ct. App. Div. 2009), finding that the city's audit of the "employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been."

The Court further limited its holding, stating as follows: "The Court 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… Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices… A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds."

For additional materials related to this case, see the following:

1. For briefs, analysis, and the case below, see: http://www.scotusblog.com/case-files/cases/city-of-ontario-v-quon/.

2. Ariel Cudkowizc, Kent Sinclair and Erik Weibust, *Technology and Privacy in the Workplace: Monitoring Employee Communications After the Supreme Court's* Quon *Decision*, 54 B.B.J. 29 (2010).

3. Carolyn Coda, *The Battle Between Privacy and Policy in* Quon v. City of Ontario*: Employee Privacy Rights and the Operational Realities of the Workplace on Display t the Supreme Court*, 19 CommLaw Conspectus 211, 2010.

4. Michael Hrdlicka, *The-Times-They-Are-A-Changin' or Technology Issue Avoidance* City of Ontario*,* Cal v. Quon*, 130 S. Ct. 2619 (2010)*, 15 J. Tech. L. & Pol'y 275, December, 2010.

5. Hon. Jay C. Gandhi & Panteha Abdollahi, *Workplace Privacy: The Confidentiality of Text Messages and the Attorney-Client Privilege*, Ass'n of Bus. Trial Lawyers, Spring 2010, http://www.abtl.org/report/oc/abtlocvol12no1.pdf.

6. Adam Santucci, *Supreme Court Issues Highly Anticipated* City of Ontario v. Quon *Decision*, Pennsylvania Labor & Employment Blog, June 22, 2010, *available at*: http://www.palaborandemploymentblog.com/2010/06/articles/public-employers-1/supreme-court-issues-highly-anticipated-city-of-ontario-v-quon-decision/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+PennsylvaniaLaborAndEmploymentBlog+%28Pennsylvania+Labor+and+Employment+Blog%29.

7. Roy Ginsburg*,* City of Ontario v. Quon*, The Supreme Court Weighs In On Employee Privacy Expectations*, Quirky Questions?, June 22, 2010, *available at*: http://quirkyemploymentquestions.com/privacy-rights/city-of-ontario-v-quon-the-supreme-court-weighs-in-on-employee-privacy-expectations/.

8. Ethan Ackerman, *No Warth in this Quon* – Ontario v. Quon, Technology & Marketing Law Blog, June 20, 2010, *available at*: http://blog.ericgoldman.org/archives/2010/06/no_wrath_in_thi.htm.

C. *Stengart v. Loving Care Agency, Inc., 201 N.J. 300; 990 A.2d 650; 2010 N.J. LEXIS 241 (N.J. 2010).*

A plaintiff employee sued the defendant for discrimination. The trial level court held that emails between the employee and her attorney on an employee-owned computer were not privileged, and denied the employee's request to disqualify the employer's counsel. On Appeal to the New Jersey Superior Court, the ruling was reversed, and counsel was found to have violated N.J. R. Prof. Conduct 4.4(b). On an appeal to the New Jersey Supreme Court, brought by the employer, the Court affirmed the ruling of the New Jersey Superior Court, and held that the policies behind attorney-client privilege substantially outweighed the employer's interest in enforcement of its unilaterally imposed workplace regulation, authorizing it to rummage through and retain an employee's emails to her attorney on an employer-provided computer.

For additional materials related to this case, see the following:

1. Ehling v. Monmouth-Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012)

2. In re Royce Homes, LP, 2011 Bankr. LEXIS 909 (Bankr. S.D. Tex. Mar. 11, 2011).

3. Holmes v. Petrovich Development Co., LLC, 191 Cal. App. 4th 1047, 119 Cal. Rptr. 3d 878, 2011 Cal. App. LEXIS 33, 111 Fair Empl. Prac. Cas. (BNA) 424 (Cal. App. 3d Dist. 2011) (finding that, when an employee used an employer's computer to email her attorney, she waived attorney-client privilege).

4. Parnes v. Parnes, 80 A.D.3d 948, 915 N.Y.S.2d 345, 2011 N.Y. App. Div. LEXIS 156, 2011 NY Slip Op 136 (N.Y. App. Div. 3d Dep't 2011).

5. Forward v. Foschi, 27 Misc. 3d 1224A, 911 N.Y.S.2d 392, 2010 N.Y. Misc. LEXIS 1066, 2010 NY Slip Op 50876U (2010).

6. Corey Ciocchetti, The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring, 48 Am. Bus. L.J. 285 (2011).

7. Constance E. Bagley, Law as a Source of Strategic Advantage: What's Law Got to Do With It?: Integrating Law and Strategy, 47 Am. Bus. L.J. 587 (2010).

8. Ariel Cudkowizc, Kent Sinclair and Erik Weibust, Technology and Privacy in the Workplace: Monitoring Employee Communications After the Supreme Court's Quon Decision, 54 B.B.J. 29 (2010).

9. Carolyn Elefant, The "Power" of Social Media: Legal Issues & Best Practices for Utilities Engaging in Social Media, 32 Energy L. J. 1 (2011).

10. Bennett Borden, Monica McCarroll, Brian Vick and Lauren Wheeling, Four Years Later: How the 2006 Amendments to the Federal Rules Have Reshaped the E-Discovery Landscape and are Revitalizing the Civil Justice System, 17 Rich. J. L. & Tech. 10 (2011).

11. Cicero H. Brabham, Jr., Curiouser and Curiouser: Are Employers the Modern Day Alice in Wonderland? Closing the Ambiguity in Federal Privacy Law as Employers Cyber-Snoop Beyond the Workplace, 62 Rutgers L. Rev. 993 (2010).

12. Gregory C. Sisk and Nicholas Halbur, A Ticking Time Bomb? University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings, 2010 Utah L. Rev. 1277 (2010).

13. Tanya Forsheit, Privacy, Privilege, and the Cloud, Oh My: Taking LovingCare to Heart, Info. L. Grp., Apr. 3, 2010, http://www.infolawgroup.com/2010/04/articles/attorney-client-privilege/privacy-privilege-and-the-cloud-oh-my-taking-lovingcare-to-heart/

14. William Morriss, *Personal Email on Company Computers*, Ephemerallaw, April 14, 2010, *available at*: http://ephemerallaw.blogspot.com/2010/04/personal-emails-on-company-computers.html.

15. Michael Rinne*, Marina Stengart v. Loving Care Agency, Inc.*, Sacramento Bankruptcy Lawyer Blog, May 6, 2010, *available at*: http://www.sacramentobankruptcylawyerblog.com/2010/05/marina-stengart-v-loving-care.html.

16. Philip K. Miles, III, *Employee Email Privacy: Stengart's Chicken and Egg*, Lawffice Space, April 29, 2010, *available at*: http://www.lawfficespace.com/2010/04/employee-email-privacy-stengarts.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+LawfficeSpace+%28Lawffice+Space%29.

17. Fernanco Pinguelo, *New Jersey and Stengart: Perfect Together?*, E-Lessons Learned, February 15, 2010, *available at* : http://ellblog.com/?p=1925#more-1925.

18. *Court Rules Communications With Attorney Using Work Computer Are Protected as Privileged*, Electronic Discovery Law, April 2, 2010, *available at*: http://www.ediscoverylaw.com/2010/04/articles/case-summaries/court-rules-communications-with-attorney-using-work-computer-are-protected-as-privileged/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ediscoverylaw%2Fklgates+%28Electronic+Discovery+Law%29.

19. Jack Pringle, *NJ Supreme Court Opinion Addresses Corpoarte Electronic Communications Policies*, Ellis Lawhorne, April 14, 2010, *available at*: http://www.scbusinesslawblog.com/2010/04/companies-should-electronic.html.

D. *Holmes v. Petrovich Development Co., 191 Cal. App. 4th 1047; 2011 Cal. App. LEXIS 33 (Cal. Ct. App. January 13, 2011).*

A plaintiff employee brought suit for hostile work environment sexual harassment, breach of the right to privacy, intentional infliction of emotional distress, retaliation, and constructive discharge. The Superior Court of Sacrament County granted the employer's motion for summary judgment on the hostile work environment sexual harassment, retaliation, and constructive discharge claims, and a jury returned a verdict for the employer on the remaining claims. The employee appealed. In an opinion by Judge Chang, the Court found as follows:

Emails from the plaintiff to her attorney were not protected by the attorney-client privilege because they were sent from the employer's computer using her employer's company email account after the employee was expressly advised that such emails were not private, and were accessible by the employer. Because the plaintiff's privacy and intentional infliction of emotional distress claims were based on the employer's alleged violation of the attorney-client privilege, they could not stand.

The hostile work environment claim was appropriate for dismissal because the plaintiff failed to show that the environment was objectively offensive.

The plaintiff's retaliation claim could not stand because the plaintiff failed to demonstrate that she suffered an adverse employment action. The plaintiff's salary, benefits and work hours were not reduced, and she was not terminated.

Finally, there was no evidence from which a reasonable trier of fact could conclude that the defendant "intentionally created or knowingly permitted working conditions that were so intolerable or aggravated at the time of [plaintiff's] resignation that a reasonable employer would realize that a

reasonable person in [her] position would be compelled to resign." Thus the constructive discharge claim was properly dismissed.

For additional materials related to this case, see the following:

1. *Taylor v. Waddell & Reed, Inc.*, 2011 U.S. Dist. LEXIS 54109 (S.D. Cal. May 20, 2011).

2. *A Ticking Time Bomb? University Data Privacy Policies and Attorney-Client Confidentiality in Law School Settings*, 2010 Utah L. Rev. 1277 (2010).

3. *Julie Gilman Veronese v. LucasFilm*, 2011 CA App. Ct. Briefs 29535, 2011 CA App. Ct. Briefs LEXIS 2619 (Cal. App. 1st Dist. May 3, 2011).

4. *Ramaiya v. Pac. Coast Care Ctr.*, 2010 CA App. Ct. Briefs 35769, 2011 CA App. Ct. Briefs LEXIS 907 (Cal. App. 6th Dist. Feb. 16, 2011).

5. Shappard Mullin, *"Belongs to the Company" Means Exactly That*, Labor & Employment Law Blog, January 18, 2011, *available at*: http://www.laboremploymentlawblog.com/computer-and-internet-use-belongs-to-the-company-means-exactly-that.html.

6. Ashwin Trehan, *Employees' Private Email Accounts Not Necessarily Off-Limits to Employers*, Nat'l Developments in Labor & Employment Law Blog, January 27, 2011, *available at*: http://www.gtleblog.com/2011/01/articles/privacy/employees-private-email-accounts-not-necessarily-offlimits-to-employers/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+GtLeBlog+%28GT+LE+Blog%29.

7. Dana Schultz, *Handbook Defeats Employee Claim of Attorney-Client Privilege*, The High-Touch Legal Services Blog, January 26, 2011, *available at*: http://danashultz.com/blog/2011/01/26/handbook-defeats-employee-claim-of-attorney-client-confidentiality/.

8. Ashley Kasarjian, *The Spotlinght on Employee Privacy*, Employment and the Law, January 24, 2011, *available at*: http://employmentandthelaw.com/2011/01/24/the-spotlight-on-employee-privacy/.

9. Lauren Moak, *Work Email and the Attorney-Client Privilege Do Not Mix*, The Delaware Employment Law Blog, January 23, 2011, *available at*: http://www.delawareemploymentlawblog.com/2011/01/work_email_and_the_attorneycli.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+delawareemploymentlawblog%2FUagR+%28Delaware+Employment+Law+Blog%29.

10. Donna Bader, *Another Important Appellate Decision Regarding the Privacy of Emails*, An Appeal to Reason, January 28, 2011, *available at*: http://donnabader.com/?p=556.

E. *In re Asia Global Crossing, Ltd., 322 B.R. 247; 2005 Bankr. LEXIS 415 (Bankr. S.D.N.Y. 2005)*

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. 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? 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.

F. *Curto v. Med. World Commc'ns, Inc., 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y. 2006)*

An employer had a broad policy, recognized by the employee several times, that materials on her company-issued laptop and in her company email could be monitored at any time. Before being fired, the employee communicated with her attorney in her personal email account on her company-issued laptop, and then deletes all of the emails. Once the lawsuit began, the company's forensic team uncovered and produced these personal emails, prompting the employee to argue that the emails were protected by attorney-client privilege.

The lower court analyzed the case using the four-factor *Asia Global Crossing* test mentioned above, and concluded that, under that test, the emails would not be privileged. But the court then asked a new question: what if the employer did not enforce its own, broad policy regarding email monitoring, such that the employee retained a reasonable expectation of privacy even on company-issued devices? The case then moved to the U.S. District Court for the Eastern District of New York, which examined the case in light of this new 'enforcement' question. The court ultimately concluded that, because the company had only actually monitored employees' computer use on four occasions, all outside of Curto's home state, Curto maintained a reasonable expectation that her computer use would not be monitored, and hence that her emails to her attorney were privileged.

Contrast *Curto* with *In re Royce Homes, LP*, 2011 Bankr. LEXIS 909 (Bankr. S.D. Tex. Mar. 11, 2011).

In *Royce Homes*, the trustee for a bankrupt home-builder wanted access to employee emails to determine whether any fraudulent conveyances were made prior to the bankruptcy filing. The employee argued that the emails, on a hard drive given to a paralegal to conduct a privilege review, were protected by attorney-client privilege. *Id.* at 719-720.

The court applied the *Asia Global Crossing* four-factor test and concluded that the policy was sufficiently broad, and the employee sufficiently on notice, that attorney-client privilege had been waived. In contrast to *Curto*, the court stated that, "whether the [company] actually reads an employee's emails is irrelevant." *Id.* at 736.

b. How does the company interpret its monitoring policy?

United States v. Hatfield, No. 06-cr-0550, 2009 U.S. Dist. LEXIS 106269 (E.D.N.Y. Nov. 13, 2009). In a white-collar fraud case, the government produced defendant's personal emails to his attorney,

obtained through defendant's former company pursuant to their computer monitoring policy. The defendant argued that the emails were protected by attorney-client and joint defense privileges and the attorney work-product doctrine. *Id.* at *3.

The court examined the facts using the Asia Global Crossing four-part test mentioned above. In applying the four-factor test, the court found a 2-2 tie. It then added a fifth factor, questioning how the company interpreted its own policy. *Id.* at *4. The court found that the company conducted privilege reviews on employee computers and email accounts, an activity that would be unnecessary if the company interpreted its policy to waive all employee privileges. Because the company's as-interpreted policy did not waive employees' legal privileges, and in this case a privilege review had found the defendant's communications to be privileged, the court concluded that this additional "interpretation" prong of the test tipped the balance, and protected the defendant's communications with his attorney.

c. To what does the employer monitoring policy apply?

United States v. Nagle, 2010 U.S. Dist. LEXIS 104711 (M.D. Pa. Sept. 30, 2010). In *Nagle*, an employer had a policy clearly stating that Internet and email communications are "NOT private," but the policy did not mention materials stored on company hard drives. The defendant's co-worker stored a document on the hard drive of his work computer containing a chronology of the events leading up to the filing of criminal charges against the defendant. The document was not stored anywhere on the Internet, nor in the co-worker's email, and the co-worker testified that he had prepared the document after his attorney instructed him to do so. The co-worker argued that the document was protected by attorney-client privilege.

The court analyzed the case using the *Asia Global Crossing* four-part test. It found that although the employer had a policy on email and Internet monitoring, it had no "systematized method" for doing so. Furthermore, the court remarked that neither the policy nor its supposed administration applied to a computer hard drive. These facts led the court to conclude that the co-worker possessed an objectively reasonable expectation of privacy in keeping the file on the hard drive.

Goldstein v. Colborne Acquisition Co., LLC, 873 F. Supp. 2d 932 (N.D. Ill. 2012).

Dombrowski v. Governor Mifflin Sch. Dist., No. 11-1278, 2012 U.S. Dist. LEXIS 90674 (E.D. Pa. June 29, 2012) (finding that, because the employer school district met the four *Asia Global Crossing* criteria outlined above, the employee, a school teacher claiming Title VII retaliation and harassment, did not have a "sufficient, reasonable expectation of privacy" in emails on her work computer).

DeGeer v. Gillis, No. 09-cv-6974, 2010 U.S. Dist. LEXIS 97457 (N.D. Ill. Sept. 17, 2010). In a breach of contract action between a consultant and his three former partners, the consultant was asked to produce communications to his lawyer that he withheld when he turned in his hard drive to the company. Neither party discussed the factor tests or the facts that apply to them, so the court examined the issue on its own, using the five-factor test from *Hatfield*.

The court applied similar reasoning as in Hatfield. The existence of a privilege review led the court to conclude that the company believed that some employee communications, even on work email, were privileged, and that their policy did not constitute a waiver of all privilege. The court held that most of the consultant's emails were protected by attorney-client privilege under the *Hatfield* test.

Sims v. Lakeside Sch., 2007 U.S. Dist. LEXIS 69568 (W.D. Wash. Sept. 20, 2007) (finding that, despite employer's clear disclosure of its email monitoring policy, public policy required that the plaintiff's attorney-client and marital communications emails remain privileged).

United States v. Etkin, No. 07-cr-913 (KMK), 2008 U.S. Dist. LEXIS 12834 (S.D.N.Y. Feb. 19, 2008) (holding, under the Fourth Amendment reasonable expectation of privacy standard, that an employee's emails to his wife at work were not privileged where the employee acknowledged the employer's email monitoring policy each time he logged on to his work computer).

TransOcean Capital, Inc. v. Fortin, 21 Mass. L. Rep. 597; 2006 Mass. Super. LEXIS 504; 2006 WL 3246401 (Mass. Super. Oct. 20, 2006) (Where the evidence was clear that an employer did not notify employees of a policy prohibiting personal email use, the Massachusetts Superior Court concluded that an employee's emails sent from the office computer to his lawyer remained privileged).

Kaufmann v. SunGard Inv. Sys., 2006 WL 1307882, 2006 U.S. Dist. LEXIS 28149 (D.N.J. May 10, 2006). The court affirmed a magistrate judge's order granting the defendant's motion seeking to discover email communications between one plaintiff and counsel, most of which had been copied and/or deleted from a company laptop. The plaintiff had not segregated her communications with counsel on the laptop before she sold the company (which owned the laptop) to the defendants. As such, the court affirmed the magistrate's decision that she had failed to take reasonable measures to withhold the emails from the defendant or ensure their confidentiality, and that disclosure of the pre-closing email communications constituted a deliberate waiver of the privilege. Moreover, the acquisition agreement indicated that email communications should have been transferred with other information. In addition, the plaintiff had used SunGard's network knowing that SunGard's company policy declared company property all information and email on its computer systems. According to company policy, all emails were subject to monitoring, and SunGard reserved the right to monitor emails. Consequently, the plaintiff had no reasonable expectation of privacy in the emails.

Nat'l Econ. Research Assocs. v. Evans, 24 Mass. L. Rep. 436 (Mass. Super. Ct. 2008). In this breach of non-solicitation agreement case, a Massachusetts court held that while the employer's computer monitoring policy clearly made an expectation of privacy on company email accounts unreasonable, the policy did not stretch so far as to negate a reasonable expectation of privacy in personal emails, even on company computers. The court noted that a reasonable person would not know that forensic software can recover screen shots of an employee's personal emails on a work computer, and reasoned that, if no protections existed for employees in these circumstances, business travelers using only work computers would not be able to have privileged conversations with their attorneys without bringing two separate computers on trips. Further, the court held that the employee's extensive – but ultimately unsuccessful – attempts to delete all attorney-client communications from

his work computer demonstrated that he had taken adequate steps to retain the attorney-client privilege.

People v. Jiang, 131 Cal. App. 4th 1027; 2005 Cal. App. LEXIS 1281 (Cal. App. 4th Dist. 2005). The trial court found that password-protected documents placed on the defendant's employer-owned laptop and segregated into a folder named "Attorney" were not protected by the attorney-client privilege because the defendant had no reasonable expectation of privacy in documents on an employer-issued laptop. The prosecutor printed the contents of a CD produced by the defendant's employer in response to a subpoena, and represented to the court and opposing counsel that the printed contents contained everything on the CD. A couple months later, however, the prosecutor discovered the password-protected files and obtained the password from the defendant's employer. The defendant, it turned out, had been communicating with counsel through his wife and other family members using his work laptop. On appeal, the court decided that because the defendant's work agreement with his employer did not preclude personal use of the computer or make any reference to copying or disclosure by the employer, and because the defendant had made "substantial efforts" to prevent others from viewing the documents, the defendant's expectation of privacy in those documents was reasonable.

Haynes v. Office of Atty. Gen. Phill Kline, 298 F.Supp.2d 1154 (D. Kan. 2003) (former assistant attorney general was entitled to preliminary injunctive enjoining a state Attorney General's Office from accessing personal files and e-mail communications stored on his work computer following his termination; plaintiff had a subjective expectation of privacy in the personal files stored on his work computer, and this expectation was objectively reasonable under the Fourth Amendment; although a computer use policy was displayed daily on his computer stating that there was no expectation of privacy in the computer system, he was told he could put personal information in a private file so no one could access it).

d. Emerging Issue: Photocopiers Storing Confidential Information

Photocopiers, particularly new models, may be storing confidential records on internal hard drives that users generally cannot access, but the drives could be removed and copied. Because copiers are storing data, it is critical that copiers be disposed of properly at the end of their life cycle, and that confidential data is protected or destroyed. For more information, *see* the following:

- Armen Keteyian, *Digital Photocopiers Loaded With Secrets*, CBS News (Apr. 15, 2010), http://www.cbsnews.com/stories/2010/04/19/eveningnews/main6412439.shtml.
- Steve Bruce, *Copy Machine May Be Storing Your Confidential Records*, HR Daily Advisor (Dec. 6, 2010), http://hrdailyadvisor.blr.com/archive/2010/12/06/HR_Policies_Procedures_Records_Recordkeeping_DOL_IRS_Crackdown.aspx.

e. Ensure Your Trade Secrets Are "Trade Secrets"

There is no one, uniform, definition of the type of information which can constitute a trade secret. For example, under the California Uniform Trade Secrets Act, Cal. Civ. Code § § 3426 *et seq.* a trade secret is defined as:

> [I]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) I the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Cal. Civ. Code § 3426.1(d). While this definition is broad, it is not enough that a piece of information be labeled a trade secret. *See Thompson v. Impaxx, Inc.*, 113 Cal. App. 4th 1425 (Cal. Ct. App. 2003). Regardless of how it is labeled – or its precise form – almost any information can be a trade secret so long as it meets the pertinent test, including:

- Customer Lists: *Am. Family Mut. Ins. Co. v. Roth*, 485 F.3d 930 (7th Cir. 2007); *Liveware Publ'g, Inc. v. Best Software, Inc.*, 252 F. Supp. 2d 74 (D. Del. 2003); *Lamorte Burns & Co. v. Walters*, 167 N.J. 285 (N.J. 2001); *Ivy Mar. Co. v. C.R. Seasons, Ltd.*, 907 F. Supp. 547 (E.D.N.Y. 1995).

- Marketing, Sales, and Pricing Data and Analysis: *Union Carbide Corp. v. UGI Corp.*, 731 F.2d 1186 (5th Cir. 1984); *Johnson Controls, Inc. v. A.P.T. Critical Sys.*, 323 F. Supp. 2d 525 (S.D.N.Y. 2004); *Ikon Office Solutions, Inc. v. Am. Office Prods., Inc.*, 178 F. Supp. 2d 1154 (D. Or. 2001).

- Drawings or Product Specifications: *Taco Cabana Int'l, Inc. v. Two Pesos, Inc.*, 932 F.2d 1113 (5th Cir. 1991); *Ctr. for Auto Safety v. Nat'l Highway Traffic Safety Admin.*, 93 F. Supp. 2d 1 (D.D.C. 2000).

- Chemical Formulae: *Kewanee Oil Co. v. Bicorn Corp.*, 416 U.S. 470 (1974); *Ctr. for Auto Safety v. Nat'l Highway traffic Safety Admin.*, 93 F. Supp. 2d 1 (D.D.C. 2000); *Wright Chem. Corp. v. Johnson*, 563 F. Supp. 501 (M.D. La. 1983).

f. Authorized vs. Unauthorized Access

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA") provides employers with a potent tool to pursue current or former employees for, among other things, the misappropriation of data. The CFAA prohibits "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss" as well as conduct where an employee "exceeds authorized access." *See* 18 U.S.C. § § 1030(a)(5)(C), 1030(a)(2), 1030(a)(4). While primarily a criminal statute, the CFAA also creates a private right of action in entities which suffer damage as a result of behavior which violates the CFAA.

The crux of the issue for claims under the CFAA is often whether an employee has exceeded their "authorized access" in copying, reviewing, or deleting certain computer files. There is a large, growing, and often conflicting body of cases interpreting this provision. In *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012), the Ninth Circuit, which has been among the most active Circuit Courts on this issue, weighed in with an *en banc* opinion interpreting this language. In *Nosal* the Court held that the language "exceeds authorized access" in the CFAA is "limited to violations of restrictions on *access* to information, and not restrictions on its *use*." *Id.* at 864 (emphasis in original). This holding means that, for example, if an employee was authorized to *access* a company's trade secret information, then the fact that the employee accessed that information for the improper purpose of misappropriating said information will not render the *access* in excess of the employee's authorization under the CFAA.

In *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012), the Fourth Circuit interpreted the CFAA in a similar fashion. In *WEC*, a welding company sued a former employee, his assistant, and a competitor after the employee, just before resigning, downloaded company information and used it in a competitor's sales presentation. The Fourth Circuit reasoned that the employees were authorized to access the information the employee prohibited use does not constituted "unauthorized access" under CFAA.

As noted above, the circuits are deeply split as to how to interpret this element. The First, Fifth, Seventh, and Eleventh Circuits have adopted a broad interpretation of the CFAA under which an employee can be found to have "exceeded" her authorization, or to have lacked authorization, to access files if she intended to make use of those files which were against the employer's interests or which were prohibited by employer policies. *See U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010) (accessing data employee was otherwise authorized to access but for a prohibited purpose was a violation); *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010) (accessing information employee was otherwised authorized to access for the purpose of committing fraud was a violation); *Int'l Airport Ctrs. L.L.C. v. Citrin*, 440 F.3d 318 (7th Cir. 2006) (deleting information from a company-issued laptop after termination, and therefore after employee's authorization to use the laptop had been revoked, was a violation); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (using a program to "scrape" a large quantity of information from a website which the individual was otherwise authorized to access was a violation). The Fourth and Ninth Circuits have adopted a narrow interpretation. *See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (Cert. dismissed Jan. 2, 2013) (downloading proprietary employer information before resigning for the purpose of competing with employer not a violation); *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (same).

g. Control of Social Media Accounts

1. <u>The Stored Communications Act</u>

Some courts have held that employer access to employee social media accounts falls afoul of the Stored Communications Act. In *Borchers v. Franciscan Tertiary Province of the Sacred Heart, Inc.*, 962 N.E.2d 29 (Ill. App. 2012), the court found that an employer had violated the Stored Communications Act by looking at an employee's personal e-mail. The court reached this holding even though the employee accessed the e-mail account from her work computer, and the account could be accessed without entering a username or password. Similarly, in *Shefts v. Petrakis*, No. 10-cv-1104, 2011 U.S. Dist. LEXIS 136538 (C.D. Ill. Nov. 29, 2011), the court found that employee e-mails stored on the employer's servers were in "electronic storage" under the Stored Communications Act and it was a violation for the employer to access them without authorization.

2. <u>Failure to Consider Social Media During Drafting Can Unintentionally Limit the Reach of Restrictive Covenants</u>

In KNF&T Staffing v. Muller, No. 13-3676 (Mass. Super. Oct. 24, 2013) (available at: http://pdfserver.amlaw.com/nlj/MassSuperiorKNF&TvMullerPIOrder.pdf), the Massachusetts Superior Court ruled that a former employee's update of her LinkedIn page was not a solicitation intended to

compete with her former employer, with whom she had signed a non-competition agreement. Ms. Charlotte Muller worked for eight years at KNF&T Staffing in Boston, Massachusetts. She signed a non-compete agreement with KNF&T when she first started which prohibited her from "solicit[ing], recruit[ing], or hir[ing] away employees of the Company" or "enga[ging] in any activity involving personnel placement in the Company's Fields of Placement" within one year of her departure from the company. *Id.* at *2. The agreement defined "Fields of Placement" as the specific staffing areas in which Muller worked, which were mainly administrative and secretarial staffing. *Id.* at *3.

Within a few months after leaving KNF&T on April 12, 2013, Muller joined a new staffing firm in Boston, working exclusively in IT-focused staffing. She also updated her LinkedIn profile, including in her "Skills & Expertise" section "Internet Recruiting" as well as other general areas such as "Staffing Services" and "Recruiting". *Id.* Upon learning of this social media update and other activities, KNF&T filed a complaint as well as a motion for a temporary restraining order requiring defendant to abide by the terms of her non-compete agreement. In its motion for a temporary restraining order, which the court treated as a request for a preliminary injunction, KNF&T argued that the LinkedIn update constituted solicitation in violation of the non-compete, contending that Muller was reaching out to potential clients of KNF&T through her LinkedIn profile. Superior Court Judge Thomas Billings strongly disagreed, stating that "Muller was not and is not prohibited from soliciting or accepting any potential client for recruitment of IT professionals, or anyone else in a field in which KNF&T does not recruit." *Id.* at *7. Central to Judge Billings's reasoning was that Muller's LinkedIn profile listed staffing specialties that were either so general ("Staffing Services" and "Recruiting") or so different ("Internet Recruiting") that they did not fall under non-compete agreement's "Fields of Placement." Judge Billings denied KNF&T's motion for a preliminary injunction, holding that there was "no evidence of a past or present violation of the non-compete agreement." *Id.*

Similarly, in *Enhanced Network Solutions Group, Inc. v. Hypersonic Technologies Corp.*, 951 N.E.2d 265 (Ct. App. Ind. 2011) ("*ENS*"), the plaintiff-contractor sued defendant-subcontractor to enforce a clause of the SubContractor Agreement which prohibited the parties from soliciting each other's employees. Plaintiff alleged that defendant had violated this agreement by posting an open sales representative position on its LinkedIn web portal, which led to one of plaintiff's employees to apply for, and ultimately accept, the open position. The Indiana Court of Appeals affirmed the trial court's determination that defendant had not "solicited" plaintiff's employee. In so holding, the Court relied on several facts: 1) the terms "solicit" and "induce" were undefined and their ordinary dictionary definitions did not support plaintiff's claim that the posting constituted a "solicitation" or "inducement"; 2) the employee made the initial contact with defendant; and 3) the employee initiated all conversations regarding the position.

3. Courts Look to Substance Over Form – Properly Drafted Non-Solicitation Agreements Can Reach "Passive" Solicitations

By contrast, in *Amway Global v. Woodward*, 744 F. Supp. 2d 657 (E.D. Mich 2010), the Eastern District of Michigan affirmed an arbitrator's decision that untargeted blog and website postings had violated

the non-solicitation agreement executed by defendant. In *Amway*, plaintiff alleged that defendant 's postings on various websites, including a blog entry in which defendant announced his decision to join a competing company because "[i]f you knew what I knew, you would do what I do" , constituted solicitation in violation of defendant's contractual obligations. *Id.* at 673. In response, defendant argued that "passive, untargeted communications" could not, as a matter of law, constitute actionable solicitation. In affirming the arbitration decision to the contrary, the Court opined that "common sense dictates that it is the *substance* of the message conveyed, and not the medium through which it is transmitted, that determines whether a communication qualifies as solicitation." *Id.* at 674. In so holding, the Court noted that other courts to confront this issue had reached similar conclusions, most notably the Ninth Circuit in *United States v. Pirello*, 355 F.3d 728 (9th Cir. 2001), which rejected the dissent's argument that "passive placement" of information on the internet could not qualify as solicitation because it did not entail "one-on-one importuning" and was not "directed at specific individuals." *Pirello*, 355 F.3d at 733 (Berzon, J., dissenting); *See also Domino's Pizza PMC v. Caribbean Rhino, Inc.*, 453 F. Supp. 2d 998 (E.D. Mich. 2006) (finding that activities including posts on internet websites to constitute prohibited solicitation); *United States v. Zein*, No. 09-20237, 2009 U.S. Dist. LEXIS 115814 at *2 (E.D. Mich. Dec. 11, 2009) (holding in a criminal matter that a Craigslist advertisement "certainly qualifies as a plan to solicit by the internet.").

The First Circuit had occasion to address solicitation in the context of electronic communications in the case of *Corp. Technologies v. Harnett*, No. 12-12385, 2013 U.S. Dist. LEXIS 63598, 35 I.E.R. Cas. (BNA) 863 (1st Cir. May 3, 2013). In that case, Harnett had signed a non-compete and non-solicitation agreement with Corporate Technologies, and a decade later left the company and joined a competitor. Shortly after he joined the competitor, Harnett sent a blast email with an update on his new position to dozens of potential clients, of which approximately 40 percent were clients of Corporate Technologies. *Id.* at *4. Numerous Corporate Technologies clients replied to the email, and some completed sales with Harnett. Soon after, Corporate Technologies filed a motion for preliminary injunction against Harnett, arguing that Harnett violated the non-solicitation agreement through his email.

In the subsequent court filings, Harnett argued that it was the Corporate Technologies clients that had contacted and completed sales with him, and thus he had not solicited their business in violation of the agreement. The First Circuit disagreed, calling this attempt to shift the initial contact from Harnett to the clients a "linguistic trick." *Id.* at *7. The court declined to create an initial contact test, stating instead that the party making the initial contact is "just one factor in drawing the line between solicitation and acceptance." *Id.* at 10. Reasoning that Harnett's blast email was a" targeted mailing" to customers of Corporate Technologies, the court held that Harnett violated the non-solicitation agreement and granted the Corporate Technologies' motion for a preliminary injunction. *Id.* at 10.

4. Unexplored Boundaries

It is clear from the above that courts are still struggling to find a path through the ever-evolving thicket of means available to employees and businesses to promote themselves. The underlying question in many of these cases appears to center around whether the court, under the particular

facts of the case, inferred that defendant *intended* to solicit the recipients of his or her communications. This can be well illustrated by comparing the facts of *ENS* with those in *Harnett*, both discussed above. In *ENS*, a job opening was posted on a LinkedIn website, and as a result was transmitted to one (or more) of plaintiff's employees in violation of defendant's non-solicitation agreement, while in *Harnett* defendant transmitted an "e-mail blast" to potential clients, approximately 40 percent of whom defendant was prohibited from soliciting.

Indeed, "intent" seems to have been the basis for the decision of the Eastern District of Oklahoma in *Pre-Paid Legal Servs., Inc. v. Cahill*, 924 F. Supp. 2d 1281 (E.D. Okla. 2013). In *Cahill* plaintiff alleged that defendant's practice of posting information to his Facebook account, which was viewable by plaintiff's "friends", including his former employees, constituted actionable solicitation. The Court disagreed, explaining that "[t]here was no evidence that Defendant's Facebook posts have resulted in the departure of a single [employee of plaintiff, nor was there any evidence that Defendant is targeting [plaintiff's employees] by posting directly on their walls or through private messaging. *Id.*; *See also* Jon Hyman, "Does Social Media Change the Meaning of 'Solicitation?'", Ohio Employer's Law Blog (Feb. 25, 2013) (available at: http://www.ohioemployerlawblog.com/2013/02/does-social-media-change-definition.html).

Of course, the question remains as to what level of contact, intentional or not, is needed to make out an actionable claim of solicitation. Unfortunately, several cases which may have provided an answer to this question have settled without reaching the merits. Nevertheless, these cases serve to illustrate the threat perceived by some employers in the growing use of social media.

In *Graziano v. NESCO Serv. Co.*, No. 1:09-cv-2661, 2011 U.S. Dist. LEXIS 33497 (N.D. Ohio March 4, 2011), after being terminated by defendant, an employment staffing agency, plaintiff created an account on LinkedIn, and used that account to contact several former co-workers. While the opinion is unclear, it appears that plaintiff did little more than request a "link" with his former colleagues. In response, defendant notified plaintiff that he should "cease all use of the LinkedIn website", as such conduct allegedly violated the terms of the non-solicit clause contained in plaintiff's severance agreement. When plaintiff refused to comply, defendant ceased the severance payments provided for in the severance agreement. The case settled before a determination could be made as to whether Graziano's conduct constituted a violation of his non-solicitation obligations. *See also* Erik B. von Zeipel, "When Does LinkedIn Activity Violate Non-Solicitation Agreements?", Trading Secrets (Nov. 4, 2013) (available at: http://www.tradesecretslaw.com/2013/11/articles/trade-secrets/when-does-linkedin-activity-violate-non-solicitation-agreements/).

Similarly, in *TEKsystems, Inc. v. Hammernick*, No. 0:10-cv-00819 (D. Minn. March 16, 2010) (Complaint) (available at: http://op.bna.com/pen.nsf/id/jmer-86fq5g/$File/linkedin-hammernick.pdf) (accessed Dec. 13, 2013). In *TEKsystems*, the plaintiff alleged that defendant had violated his non-solicitation obligations by "connecting" with contacts through social media websites. In the non-solicitation agreement defendant had agreed not to, whether directly or indirectly, "[a]pproach, contact, solicit, or induce any individual" to perform certain prohibited acts. *Id.* at par. 27(B). While other contacts were alleged by plaintiff, the focus of its complaint is on the fact that defendant had "connected" with at least sixteen of its employees through LinkedIn. This

case also settled before a determination could be made as to whether defendant's conduct constituted a violation of his non-solicitation obligations. See Zeipel at http://www.tradesecretslaw.com/2013/11/articles/trade-secrets/when-does-linkedin-activity-violate-non-solicitation-agreements/.

5. Going Forward

> "The lesson for any business is clear: If you're facing an uncomfortable collision with loyal employees, lock down your social media accounts. The anonymous worker indicated in another series of tweets … that HMV's feeds were set up by an intern years ago and likely not secured." Jared Keller, "HMV Employee Commandeers Corporate Twitter Account in Response to Layoffs," BusinessWeek, Jan. 31, 2013, http://www.businessweek.com/articles/2013-01-31/hmv-employees-commandeer-corporate-twitter-account-in-response-to-layoffs.

In response to these court decisions, there are several steps practitioners for both employers and employees might take in advising their clients.

1. Employers should advise his or her client to address social media within the terms of the restrictive covenant to be certain that even "passive" solicitation falls within the terms of the covenant. As with any other restrictive covenant, the terms should be narrowly drawn to protect the employer's legitimate business interests.

2. Employees should be advised of the potential dangers inherent in their use of social media websites. Where possible, Employees should negotiate specific carve outs to allow reasonable use of social media to obtain non-competitive employment even if that use entails incidental contact with employees or customers of the former Employer.

h. Develop Policies for Mobile Computing and Work Shifting

- Mobile computing and work shifting heighten ability of employees to obtain and hide employer documents
  - Personal email and cloud accounts
  - Personal hardware: computers, tablets, phones
- Consider including protections against certain uses of mobile devices and cloud products in employment contracts

i. Create Document Return Policies

- Specify the return of both hard and soft copies
- More complex than it may appear:
  - Co-mingling of personal/work docs
  - Difficult to verify compliance with established policies

Expensive

j. Provide for Forfeiture and Clawbacks

- Forfeiture/Employee Choice Doctrine
  - Employee forfeits deferred compensation if employee makes "genuine and knowing voluntary choice" to violate non-compete agreement
  - *Morris v. Schroder Capital Mgmt.*, 859 N.E.2d 503 (N.Y. 2006); *Lucente v. Int'l Bus. Machines Corp.*, 310 F.3d 243 (2d Cir. 2002)
- Clawbacks
  - Recovery of paid or unpaid compensation permitted if employee breaches fiduciary duty
  - *Janssens v. Freedom Med., Inc.*, No. 10-2042, 2011 U.S. Dist. LEXIS 46670 (D. Md. April 29, 2011)

k. Keep Agreements Jurisdiction-Specific

- Be aware of state non-compete statutes
  - Statutes making non-competes unenforceable in most circumstances – California (Cal. Bus. & Prof. Code § 16600)
  - Criminal penalties for unreasonable prohibitions on employment – Nevada (NRS 613.200)
  - Legislation requiring waiting period to allow employee to seek legal review of non-compete agreements – Connecticut bill (H.B. 6658, 2013 Leg. Sess. (Conn. 2013)).
- State computer-abuse statutes
  - Access "without authorization" – Md. Code Ann. Crim. Law § 7-302 (LexisNexis 2013)
  - "Unauthorized access" – California Comprehensive Computer Data and Fraud Act (Cal. Penal Code § 502 (Deering 2013))

l. Keep Agreements Up-to-Date

- Major changes in employee status such as promotions, updated compensation, transfers, may void non-compete agreement
- Major changes in employer – new entity, location change
  - *Grace Hunt IT Solutions, LLC v. SIS Software, LLC, et al.*, 29 Mass. L. Rep. 460 (2012)

– Can attempt to solve through contractual language, but be cautious:

TEKSystems, Inc. v. Fletcher, 2011 U.S. Dist. LEXIS 22227 (D. Md. Mar. 2, 2011)

IV. ARTICLES AND OTHER SOURCES:

- Ben N. Dunlap, *Beware Inadvertent Waiver of the Attorney-Client Privilege Through Use of Employer-Provided Computers or E-mail*, LeClairRyan Accountant & Attorney Liability Newsbrief, May 21, 2013, at 1-2, *available at* http://www.leclairryan.com/files/Uploads/Documents/Acct%20Atty%20Liability%20Newsletter%2005%2013.pdf;
- *Attorney-Client Privilege and Waiver in Employee Email on Company Systems*, Seyfarth eDigital, May 2011, http://www.seyfarth.com/ dir_docs/news_item/71423fc4-f298-4f18-8649-48e861380210_documentupload.pdf;
- Louise L. Hill, *Gone but Not Forgotten: When Privacy, Policy, and Privilege Collide*, 9 Nw. J. Tech. & Intell. Prop. (2011), *available at* http://scholarlycommons.law.northwestern.edu/njtip/vol9/iss8/3
- Frank Steinberg, *Using Your Employer's E-mail: There's Legal, and Then There's Smart*, New Jersey Employment Law Blog (Jan 18, 2011); http://employment.lawfirmnewjersey.com/finding-hiring-an-employment-lawyer/using-your-employers-e-mail-theres-legal-and-then-theres-smart/.
- Toby Brown, Use Gmail – Waive Privilege?, 3 Geeks & a Law Blog, Aug. 19, 2009, http://www.geeklawblog.com/2009/08/use-gmail-waive-privilege.html
- Toby Brown, Gmail Waives Privilege – Part Deux, 3 Geeks & a Law Blog, Sept. 3, 2009, http://www.geeklawblog.com/2009/09/gmail-waives-privilege-part-deux.html
  Anthony E. Davis, *More Privilege Issues with Employee E-Mail*, Law Technology News, January 5, 2010, http://www.law.com/jsp/lawtechnologynews/PubArticleFriendlyLTN.jsp?id=1202437380338.

- Robert Ottinger, *Employees Have a Right to Privacy in E-Mail Sent from Work*, New York Employment Lawyer Blog, December 15, 2009, http://www.newyorkemploymentlawyerblog.com/2009/12/employees_have_a_right_to_priv.html.
- Tresa Baldas, *District Court Finds Personal E-Mail from Work Still Privileged, The Blog of Legal Times*, December 11, 2009, http://legaltimes.typepad.com/blt/2009/12/district-court-finds-personal-email-from-work-still-privileged.html.
- Adam C. Losey, *Dunwoody Distinguished Lecture in Law: Note: Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 Fla. L. Rev. 1179 (2008), *available at* http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1063&context=flr.
- Ruth E. Piller, *Employees Cannot Expect Privacy in E-Mail Using Employer's Computers*, American Bar Association Litigation News Online, May 2008, http://www.abanet.org/litigation/litigationnews/2008/june/0608_article_email.html.
- Debra Cassens Weiss, *Email to Lawyer Not Privileged Because of Employer Policy*, ABA Journal, October 30, 2007, http://www.abajournal.com/

news/article/
e_mail_to_lawyer_not_privileged_because_of_employer_policy/.

- Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. Rev. 323 (2012), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2129523.