

Clear
Law
Institute

Departing Employees and Data Breaches: Policies, Procedures, and Practical Advice

Presented by:
Paul Starkman, Robert Fitz Patrick, & Jennifer Trulock
October 6, 2017

Clear Law Institute | 4601 N. Fairfax Dr., Ste 1200 | Arlington | VA | 22203

www.clearlawinstitute.com

Questions?

Please call us at 703-372-0550 or email us at
info@clearlawinstitute.com

All-Access Membership Program

Join thousands of professionals who access our hundreds of courses each year



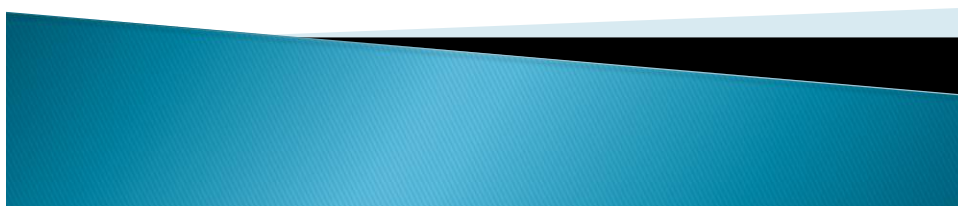
- Earn continuing education credit (CLE, CPE, SHRM, HRCI, etc.) in all states at no additional cost
- Access courses on a computer, tablet, or smartphone
- Access more than 75 live webinars each month
- Access more than 750 on-demand courses

Register within 7 days after the webinar using promo code “7member” to receive a \$200 discount off the \$799 base price.

Learn more and register here:
<http://clearlawinstitute.com/member>

Departing Employees & Data Security after the DTSA

Policies, Procedures, and Practical Advice



Presenters

- ▶ Paul E. Starkman
Clark Hill PLC
Chicago, IL
- ▶ Robert B. Fitzpatrick
Law Offices of Robert Fitzpatrick, PLLC
Washington, D.C.
- ▶ Jennifer M. Trulock
Baker Botts L.L.P.
Dallas, TX



2

Understanding the Rising Tide of Insider Data Breaches

PES
/RF

▶ Statistics

- 43% of all data breaches involve insiders
- 50% of departing employees took corporate data and did not think it was wrong
- 70% of theft occurs within employee's last 30 days

▶ Examples

- *Alphabet (Google) v. Waymo (Uber)* (trial on insider theft of driver-less car technology) (Oct. 2017)
- Equifax CEO “retires” after data breach involving 143 million Americans (Sept. 2017)
- Citibank ex-employee sentenced for shutting down 90% of company’s internet access in North America (July 2016)

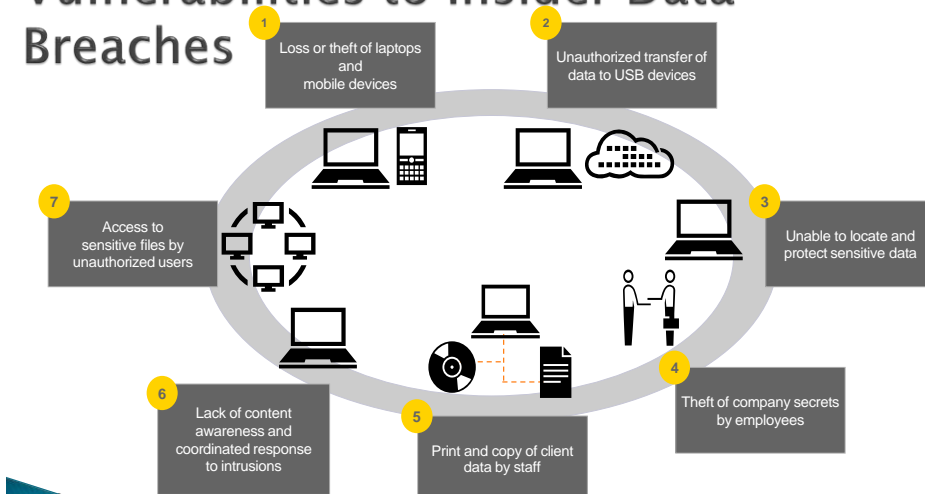
No one is immune.



3

Understanding Technological Vulnerabilities to Insider Data Breaches

JT



4

How to Prevent Breaches by Departing Employees

RF

- ▶ Policies
- ▶ Agreements
- ▶ Detection
- ▶ Technology

Good employees are key.



5

Policies to Prevent Departing Employee Data Breaches

PES

- ▶ Policies banning workplace recordings
 - Cameras and smartphones in the workplace
- ▶ Document Retention/Data Storage Policies
 - Data Landscaping (where is the data?)
- ▶ Monitoring computer usage policies
 - Notice/consent/privacy
- ▶ IT Policies/Social Media Policies

6

Policies to Prevent Departing Employee Data Breaches

RF

- ▶ Confidentiality/Non-Disclosure
 - Limit access to sensitive information
 - Home or off-site data access?
 - Misuse of corporate computers
 - Unauthorized applications
 - Passwords
 - Login/logout bypass
 - Port control:
- ▶ Devices
 - Bring your own device (BYOD) policies
 - No flash drives or electronic storage devices



7

Using Offer Letters to Prevent Data Breaches When Employees Leave

JT

- ▶ Representations and warranties
 - Do not bring former employers' data
 - Do not use or disclose to our employees
- ▶ Candidate must understand obligations before hire
- ▶ Prohibited disclosures agreement

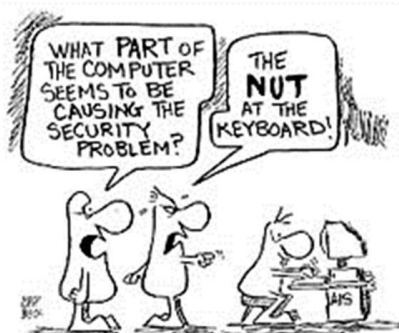


8

Technology to Prevent Data Breaches by Departing Employees

PES

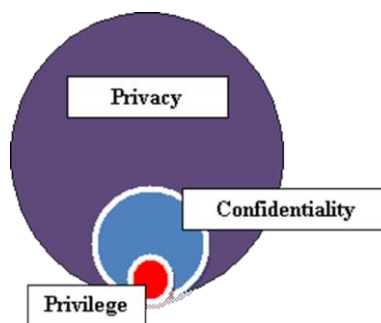
- ▶ Device management software
- ▶ Segregating information on devices
- ▶ Encryption and passwords
- ▶ Key-stroke monitoring
- ▶ Thumb drive detection
- ▶ Remote locking and
- ▶ Computer forensics



Agreements to Prevent Insider Data Breaches

RF

- ▶ Confidentiality and NDAs
 - Definition
 - Reasonable effort to keep confidential
 - DTSA Notice
- ▶ Define CI
 - Be specific
 - Trade secrets v. CI
 - Consider state law

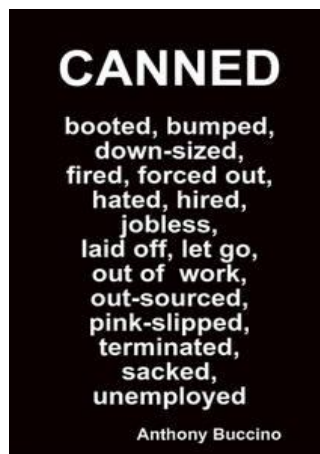


10

JT

Insider Data Breach Prevention and Response – Exit Interview

- ▶ Exit Interviews:
 - Remind employees of continuing obligations
 - Signed copies of contracts
 - Involve IT
 - Look for **Red Flags**



11

JT

Coordinating Response

- ▶ Internal Resources
 - In-house legal counsel
 - IT
 - Risk Management
 - Business Leaders
- ▶ Insurance
 - Where to get it?
 - What should it cover?
 - Loopholes
 - Notification
- ▶ External Resources
 - Outside legal counsel
 - Computer forensic consultant
 - Third-party vendors (ex. cloud storage provider)

Responding to Insider Breaches – Preservation

PES

- ▶ The duty to preserve
 - Triggers
 - Litigation holds
 - Spoliation
 - Cloud-based data
 - E-discovery



13

Legal Issues from Insider Breaches

RF/
JT/
PES

- ▶ Ethical considerations
 - Employee-attorney communications on company computers
- ▶ Self-help
 - Is employer over-zealous investigation violate Stored Communications Act?
 - Does employee data theft to support claims = protected activity?
 - *Verdrager v. Mintz Levin* (MA 2016) (yes)
- ▶ Defend Trade Secrets Act
 - Immunity for disclosure of trade secrets
 - No immunity for misappropriation of data

14

Return of Documents by Departing Employees

RF

- ▶ What do you mean by “return”?
 - Copies
 - Physical media
 - Electronic media
- ▶ Have a protocol
- ▶ Certification of return



15

Consider Actions Short of Litigation

JT

- ▶ Reminder letter from employer
 - Remind employees of obligations
 - Include *signed* copies of agreements
- ▶ Cease and desist letter
 - When to use
 - Dangers
 - To whom
- ▶ Ultimatum letters and “anticipatory” lawsuits



16

Statutory Claims Against Departed Employees for Data Breaches

- ▶ Statutory
 - DTSA – federal trade secret misappropriation
- ▶ Actual Damages
 - Lost profits
 - Unjust enrichment
 - Royalties
 - Exemplary damages
 - Attorneys' fees
- ▶ Ex Parte Seizure
 - DTSA only
- ▶ Injunctions
- ▶ Other Statutory Claims
 - CFAA
 - Stored Communications Act
 - Uniform Trade Secrets Act



PES

Claims Against Breaching Employee's New Employer

- ▶ Common Law
 - Tortious interference
 - Aiding/abetting breach of fiduciary duty
 - Conspiracy
 - Fiduciary Duties
 - Conversion/Theft/Misappropriation
- ▶ Contractual
 - Restrictive Covenants
 - Non-Disparagement
 - Confidentiality

RF



18

Civil Claim Considerations

- ▶ Is Lawsuit Worth the Risk
- ▶ Does It Meet Employer's Goals
- ▶ Will It Be Easy to Prove?

- ▶ DTSA – Action Items
 - Notice of Immunity
 - Policies
 - Contracts
 - Reps/warranties from new hires



19

Criminal Actions for Insider Data Breaches

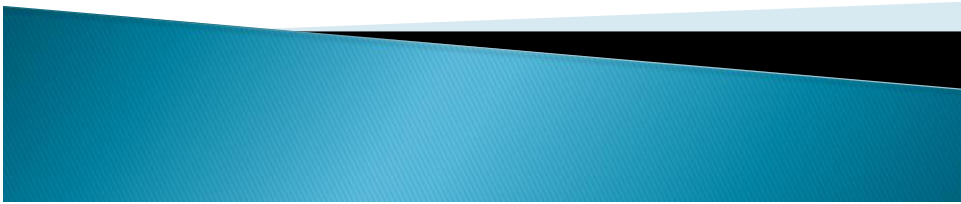
- ▶ Is Criminal Action Available?
 - Theft
 - Computer fraud
 - Criminal CFAA

- ▶ Is Criminal Action Worth the Risk?
 - No indictment
 - Dismissal
 - Malicious prosecution



20

Questions?



Data Breaches: Trends

With Robert B. Fitzpatrick

Introduction

- FBI has said "you are going to be hacked"
- Data breaches are very prevalent.

Exposure

- Brand Damage
- Loss of competitive advantage
- Loss of customers and business
 - Target breach cost target 42% of net profit in the quarter following its data breach.
- Erosion of shareholder value
- Fines and civil penalties
 - heavily enforced
- Civil litigation

Civil Litigation

- This is an area plaintiff
- In last quarter of 2013, Target faced 40 lawsuits arising out of the data breach.
- There are hundreds of data breach lawsuits around the country.
- Costs can be substantial in the short and long term.

Threats

- External
 - Outside hackers
- Internal
 - A large threat
 - Leaks
 - Employees and former employees

Data Retention

- In a symantec study, 50% of employees retain confidential corporate data, half of those said they would use it in their new jobs.

Internal Risks

- Negligence
- Malicious breach
- Data retention/theft

Types of Data Breaches

- Consumer facing
 - sensitive information about consumers is leaked.
 - vendors are a risk factor
- Employee facing
 - sensitive information about employees is leaked.

Morgan Stanley

- Wealth management employee took data of 350,000 clients

Community health systems

- Chinese hackers got 4.5 million records

Home Depot

- 56 million credit/debit card numbers

AT&T

- Two employees accessed customer records for 2.5 weeks.

IRS

- IRS employees took home on a thumb drive PII of 20,000 employees and contractors.

Advance Medical Group

- 4 laptops contained health information on 4 million patients.
- These were password protected, but not encrypted.

Veteran's Admin

- 26.5 million records regarding veterans, spouses, active duty military personnel
- Target
 - 61 million dollars spent in 4th quarter 2013 - net income decreased 46 percent compared to 2012.

- Bryan Krebs has scooped many of the data breaches. [GET ADDRESS]
- Privacyrights.org

Data Security

- Top concern for companies.

Best Practices: Data Security Assessment

- Data Security Assessment
 - What information is retained?
 - by the company?
 - By its vendors?
 - Where is it maintained?
 - Cloud provider?
 - Personal devices?
 - What measures are taken to protect it?

Best Practices: Hire a Hacker

- You can retain hackers - "security consultants" to test you information security by attacking it.

Best Practices: Oversight

- Need to assign clear responsibility for cyber-security oversight tasks.

Culture

- Need to build a culture of privacy.
- Privacy should inform design and development decisions.

Best Practices: Incident Response

- Have a plan in place.
 - Train on the plan.
 - Be able to institute it promptly.
- Have a team in place.
 - Clearly identify responsibilities.
 - Train them in crisis response in "real life" scenarios.
- Need a single person in charge of the team.

Best Practices: Response

- What notifications need to be made?
 - To insurance?
 - To government bodies?
 - To customers?
 - To employees?
- Damage control and public relations
- Many statutes require that notice be timely.

Best Practices: Public Relations

- Engage a firm promptly.
- Emphasize
 - swift response
 - breach has been contained
 - offer free credit/identity monitoring
- Establish a 24/7 hotline
- Be prepared to advise effected individuals on how to protect themselves.

Best Practices: Security Measures

- Electronic
 - Passwords
 - Encryption
 - Anti-Virus
- Physical
 - Locked cabinets
 - shredders
- Human
 - Require prompt reporting of losses
 - Protocol in place with training

Data Minimization

- Data is a liability, not an asset.
- Keep as little as possible.
- Only retain data you need to do business.
- Steps:
 - account for all data
 - "Silo" and protect data
 - Limit access to data

Telecommuting

- Encouraged by the government and many private companies.
- Poses risks for data security
 - difficult to regulate home environment
 - data may end up stored on personal devices
- Clear policies and monitoring are needed.

Evaluate IT Assets

- Consider hiring third party to evaluate your IT department.
- Identify risks and gaps in controls.
- Develop a data loss prevention plan to address weaknesses.
 - These are sometimes required by state law.

Agreements

- Have all employees sign a confidentiality agreement.
 - Provide them with separate consideration.
- Require return of company employees.
- Require consent to monitoring of use of personal devices.
- Have employees agree that they will not bring or divulge prior employer trade secrets to your organizations.

Written Information Security Program (WISP)

- CT, MD, Mass., Tex all require one.

Trade Secrets

- Inventory them.
- Treat them as secret! - this is the first test.

BYOD Policies

- Very popular a few years ago.
- Employees use personal devices for work.
- Ends up with sensitive information on employee devices.

BYOD Policies

- Need:
 - Monitoring of devices
 - Mobile Device Management software;
 - Consent to remotely wipe the device
- Some states limit installation of "kill switches" on personal devices.
- Strong passwords
- Consider encryption - and know that it is required in some industries.

Insurance

- Your General Corporate Liability policy may well not cover outside data breaches.
- [CITE NEW YORK CASE]. XXX
- Stand-alone data breach/"cyber risk"/"cyber liability" insurance is available.
 - Investigations
 - credit monitoring
 - lawsuit defense
 - payment of judgments
- You may need to require encryption.

Review Your Insurance

- Have your policy reviewed by an attorney.
- They can have loopholes and outs for insurers - make sure you have the coverage you need.

Social Media Policy

- Have the right to discipline employees for conduct which is prohibited by other policies.
- Add social media to confidential/proprietary information which may not be shared on social media.

Social Media Monitoring

- Very risky area.
- Risks include:
 - Stored Communications Act;
 - National Labor Relations Board/Section 7 of NLRA;
- Pretexting is prohibited

NLRB & Social Media

- NLRB requires language in policies that NLRA rights are not limited.
- *Flex Fleck Logistics v. NLRB*, 4th Cir 746 F.3d 205 [CITE XXX]

Timely Notification

- Critical.
- If intrusion is ongoing, you may wish to let them continue in hopes of catching them.
- Regulatory agencies respect this type of delay.

State Laws

- Virginia - If there is a breach, must notify consumers without "unreasonable delay".
 - If more than 1,000 customers have been compromised, must tell VA attorney general, all consumer reporting agencies which maintain files on consumers.
- When you provide public notice, there is a **good chance you will be sued.**

Federal Agencies

- DHS - the "High Tech Act" - a breach notification rule involving healthcare organizations.
- SEC - Security risk is a top disclosure priority for the SEC. Guidance was issued in 2011, comment letters disseminated to regulated companies.
- FCC - Involved heavily.
- CFTC
- NLRB

Limit Exposure

- Track data flows.
 - who is accessing data?
 - Is the access consistent with work assignments?
 - Flag unusually large downloads.
- Need ability to wipe or freeze data.
- Limit access.

Purging Old Mobile Devices

- Cell phones and laptops have short shelf lives.
- If devices is not properly wiped before it is sold or transferred, there is risk of breach.
- NY Transportation Department:
 - Information on 15,000 individuals was found inside refurbished drive that was being sold.
 - The reseller contacted city, no breach.

Look For Warning Signs

- Individual has expressed hostility.
- Individual is unhappy.
- Individual has poor performance evaluations or poor sales.

Mobile Phone Recordings

- Require employees to leave phones outside of rooms where there are confidential/trade secret information being discussed.
- Illinois Supreme Court found "two party consent" to be unconstitutionally overbroad.
- The legislature is attempting to write a new statute.

Prohibitions of Recordings

- Be sensitive to the NLRB which may see an overly broad anti-recording policy as violating Section 7 of the NLRA.
- See *Jones v. St. Jude Med.*, 504 Fed. Appx. 473 [CITE XXX]

Exit Interviews

- Incentivize exit interviews for departing employees.
 - make it a condition of severance pay
- Incentivize return of data and documents.
- Unwillingness to attend exit interview may be a red flag.

After Departure

- Remind employees of their obligations.
- Remind employees not to allow individuals to use their password to access the Company's systems.
- In extreme cases, require co-workers to change passwords.
- Change/update badge security systems so former employee cannot access the building.
- Return of documents should be a condition to any separation agreement.

Image Laptops

- Where there is good reason, have forensic specialist image departing employee's laptop and examine it for recent activity.
- Properly preserve evidence against the possibility of litigation.

Serious Breaches

- Present to district attorney or other appropriate authority for prosecution.
 - Federal Economic Espionage Act.
 - Computer Fraud & Abuse Act
- In *State v. Saverda*, 81 A.3d 693 [CITE XXX] employee who copied documents for use in whistleblower case was criminally prosecuted. Now before NJ Supreme Court.

Litigation

- Recent study identified 86 causes of action which have been used by plaintiffs in these actions
- Principal defense is the issue of standing.
- SCOTUS in *Clapper v. USA* held that a fear of government interception of communications did not confer standing. XXX [CITE]

Current Claims

- Plaintiffs most recently bring claims under state consumer protection statutes, which often do not require proof of damages.
- This may allow plaintiffs to evade the standing issue.

Data Breach Litigation

- Read the 97 page opinion in S.D. Cal *Sony Gaming Networks & Cust. Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 [CITE XXX]

Regulatory Activity

- The FTC has brought over forty actions arguing that negligent data breach policies constitute a deceptive trade practice under the federal statute.
- The only company to challenge them was Windham Hotels. That case is *Windham Worldwide Corp. v. FTC.*

Departing Employees: Practical Legal Guidance

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave., N.W.
Suite 230

Washington, D.C. 20009
(202) 588-5300
(202) 588-5023 (fax)

fitzpatrick.law@verizon.net

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

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	1
II. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYEE	1
a. Initial Contact With The Employee.....	1
1. Never communicate with an attorney using your employer’s e-mail system, accounts, or devices	1
2. “Document Theft” – Unauthorized Removal/Copying/ Access of Employer Documents .	4
3. Preservation Obligations.....	5
b. The Representation Agreement.....	6
c. Return of Property.....	6
1. Return of Employer Property	6
2. Return of Employee Property.....	7
d. Key Documents	7
1. All Agreements and Policies	7
2. Performance Improvement Plan	8
3. Restrictive Covenants	9
e. Post-Employment Considerations	12
1. Social Media	12
2. Unemployment Compensation	14
f. Emotional Distress	17
III. CONSIDERATIONS FOR COUNSEL FOR THE EMPLOYER	18
a. Privacy and Privilege	18
1. Overview of Privilege	18
2. For More Related Cases, See the Following:.....	18
b. How does the company interpret its monitoring policy?.....	25
c. To what does the employer monitoring policy apply?	25
d. Emerging Issue: Photocopiers Storing Confidential Information.....	27
e. Ensure Your Trade Secrets Are “Trade Secrets”	28
f. Authorized vs. Unauthorized Access.....	28
g. Control of Social Media Accounts	29
1. The Stored Communications Act	29

2.	Failure to Consider Social Media During Drafting Can Unintentionally Limit the Reach of Restrictive Covenants.....	30
3.	Courts Look to Substance Over Form – Properly Drafted Non-Solicitation Agreements Can Reach “Passive” Solicitations.....	31
4.	Unexplored Boundaries.....	32
5.	Going Forward	33
h.	Develop Policies for Mobile Computing and Work Shifting.....	34
i.	Create Document Return Policies.....	34
j.	Provide for Forfeiture and Clawbacks.....	34
k.	Keep Agreements Jurisdiction-Specific.....	35
l.	Keep Agreements Up-to-Date.....	35
IV. ARTICLES AND OTHER SOURCES:.....		35

Practical Tips for Counsel for a Departing Employee

By Robert B. Fitzpatrick¹, 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

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.

not only to work provided e-mail accounts, but also to personal e-mail accounts which the employee 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); *Kelleber 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. “Document Theft” – Unauthorized Removal/Copying/Access of Employer Documents

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 state².

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 otherwise 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

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.

“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).

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 (fiduciary 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 by 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 Brunswick 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 plaintiff's 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. Kirschenbeiter & 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 *indicta* 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. See *Betts 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 Cudkowicz, 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 to 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 Wrath 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 Cudkowicz, 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*, Ephemeral Law, April 14, 2010, available at: <http://ephemeralaw.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*, Law Office Space, April 29, 2010, available at: http://www.lawofficespace.com/2010/04/employee-email-privacy-stengarts.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+LawOfficeSpace+%28LawOffice+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%2Fkfgates+%28Electronic+Discovery+Law%29.
19. Jack Pringle, *NJ Supreme Court Opinion Addresses Corporate 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 Sacramento 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.gtleb.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 Spotlight 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 otherwise 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. The Stored Communications Act

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. Failure to Consider Social Media During Drafting Can Unintentionally Limit the Reach of Restrictive Covenants

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. Cabill*, 924 F. Supp. 2d 1281 (E.D. Okla. 2013). In *Cabill* 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](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.

Departing Employees:

Two Sample Computer Forensics Protocols

by

Robert B. Fitzpatrick, Esq.
Fitzpatrick Law Group

1666 Connecticut Ave., N.W.
Suite 230

Washington, D.C. 20009

(202) 588-5300

(202) 588-5023 (fax)

rfitzpatrick.law@verizon.net

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

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.

COMPUTER FORENSICS PROTOCOL

This Computer Forensics Protocol is hereby entered into on this ____ day of _____, 2012, by and between _____ (“Plaintiff”), _____, (“Defendant”) (collectively the “Parties”).

WHEREAS Plaintiff’s counsel, Robert B. Fitzpatrick, PLLC (hereafter “Plaintiff’s Counsel”), is currently in possession of (1) a Blackberry; (2) the SIM card for that Blackberry; (3) a Nokia cellular telephone; and (4) a mini-SD data card contained in the aforesaid Nokia cellular telephone (collectively the “Defendant-Issued Devices”); and

WHEREAS Plaintiff and/or Plaintiff’s Counsel is also currently in possession of certain electronic devices which are Plaintiff’s own personal property (collectively the “Plaintiff Devices”); and

WHEREAS the Defendant-Issued Devices and the Plaintiff Devices collectively contain electronic data, (1) some of which may be relevant to one or more disputes between the Parties, including but not limited to the claim(s) asserted by Defendant against Plaintiff, and the claim(s) asserted by Plaintiff against Defendant (hereafter the “Disputes”); (2) some of which is Plaintiff’s personal and private data (for example, private financial and medical data and spousal and other family communications) (hereafter the “Private Data”); and (3) some of which is privileged attorney-client communications between Plaintiff and his Counsel and/or the privileged attorney work product of Plaintiff’s Counsel (hereafter the “Privileged Data”) (all of the aforementioned data is hereafter collectively referred to as the “Data Set”); and

WHEREAS the Parties are interested in coming to an agreement (hereafter a “Computer Protocol”) whereby Plaintiff can return the Defendant-Issued Devices and/or Data Set to Defendant in a manner which (1) maintains adequate protections for the Privileged Data and Private Data; and (2) can be effectuated in as efficient, expeditious, and cost-effective a manner as possible; and

WHEREAS the Parties’ respective counsel have conferred with one another for several months now in an attempt to reach an agreement on such a Computer Protocol, but have to date been unable to reach such an agreement;

THE PARTIES HEREBY AGREE that as soon as is feasible, and in any event by no later than the ____ day of _____, _____, the Parties’ respective counsel, as well as the Parties’ respective forensic computer experts, agree to confer telephonically, in order to attempt in good faith to discuss and agree upon reasonable and mutually acceptable terms for a Computer Protocol. The Parties furthermore commit, in good faith, to use their best efforts to finally agree upon and reduce to writing as quickly as possible such a Computer Protocol and to comply therewith.

In an effort to facilitate such a discussion, Plaintiff’s counsel has attached hereto a proposed outline for how such a reasonable Computer Protocol might be accomplished.

[Plaintiff]

Date

[Defendant(s)]

Date

PROPOSED OUTLINE FOR COMPUTER FORENSICS PROTOCOL

- (1) As regards the Defendant-Issued Blackberry and its SIM card, _____, a computer forensics firm which Plaintiff retained, created on _____ an IPD file in connection with the data on the Blackberry. Plaintiff would, at his own expense, retain a computer forensics expert such as _____ to search the data in that IPD file, in an effort to segregate the data which is responsive to very specific criteria – that criteria being calculated to identify and segregate the data in the IPD file which constitutes attorney-client privileged communications between Plaintiff and his counsel, private spousal and other family communications between Plaintiff and his spouse and/or family, and private financial and medical data. Plaintiff and Defendant would agree to specific criteria by which such data would be segregated. This data would be returned to Plaintiff on a “clean” electronic storage device purchased for this purpose. The balance of the data in the IPD file would be transmitted to Defendant in a format to be agreed upon by the Parties. Plaintiff’s computer forensics expert would maintain an unaltered and unedited “complete” version of the IPD file. As soon as any and all Disputes between the Parties have come to a full, final, and non-appealable resolution – that is, after any and all Disputes have been fully and finally and forever resolved (hereafter, the “Dispute Resolution”), upon request by Defendant, Plaintiff’s computer forensics expert would destroy any such IPD file in his possession.

As it would be impossible to return the Blackberry and/or its SIM card itself to Defendant without giving Defendant access to the data which has been segregated according to the above process, and as a full and complete IPD of that data would be maintained in any event, the Blackberry and its SIM card would be returned to factory settings, the data removed therefrom, and the Blackberry and SIM card themselves would be returned to Defendant.

- (2) As regards the Defendant-Issued Nokia cell phone, while neither Plaintiff nor his counsel are in possession of the SIM card which was used in the Nokia while Plaintiff was employed with Defendant, the Nokia does contain a Mini-SD data card. While it is believed that there is no privileged or private data on either the Nokia or its data card, the review by Plaintiff’s computer forensics expert of the data thereon (subject to the same criteria as that set forth in paragraph # 1 above) would be for the purpose of ensuring that that is the case. If so, the Nokia and its data card would be returned to Defendant in its unaltered state. If there is any such privileged or private data, the Nokia and its data card would be handled in a similar process to that set forth in paragraph # 1 above.
- (3) As for the Plaintiff Devices, as Defendant contends that those devices contain data which is Defendant’s property, Plaintiff would certify under oath that he will not use any Defendant-related data on the Plaintiff Devices for any reason other than in connection with the Disputes between the Parties.

At the time of Dispute Resolution as defined above:

- (a) Plaintiff shall create an inventory of only those non-Defendant-related documents on the Plaintiff Devices which he wishes to keep (for example, medical records, income tax returns, etc.);
- (b) Plaintiff would send said inventory to Defendant, and Defendant would indicate whether it objects to Plaintiff keeping any such documents;
- (c) If there is any disagreement on the above inventory, the Parties agree to confer and use best efforts to reach a reasonable resolution of such a dispute, and in the event

that the Parties deem it necessary, the Parties shall appoint a neutral third party to aid in the resolution of any such dispute;

(d) Once the Parties have agreed on the aforesaid inventory, the inventoried documents shall be transferred to a new electronic device (for example, a “clean” flash drive or external hard drive), and Plaintiff shall then destroy all of the Plaintiff devices. In connection with any personal computer, destruction shall mean only destruction of the hard drive, and shall not preclude the purchase of a new “clean” hard drive to install and use in the same computer.

(4) As for Plaintiff’s Yahoo and Gmail webmail accounts, as Defendant contends that those email accounts contain data which is Defendant’s property, Plaintiff would certify under oath that he will not use any Defendant-related emails in those accounts for any reason other than in connection with the Disputes between the Parties.

At the time of Dispute Resolution as defined above:

(a) Plaintiff shall create an inventory of only those non-Defendant-related emails in the aforesaid accounts which he wishes to keep (for example, medical records, income tax returns, personal emails etc.);

(b) Plaintiff would send said inventory to Defendant, and Defendant would indicate whether it objects to Plaintiff keeping any such emails;

(c) If there is any disagreement on the above inventory, the Parties agree to confer and use best efforts to reach a reasonable resolution of such a dispute, and in the event that the Parties deem it necessary, the Parties shall appoint a neutral third party to aid in the resolution of any such dispute;

(d) Once the Parties have agreed on the aforesaid inventory, any and all data contained in the aforementioned email accounts shall be deleted, and removed from any and all “trash” folders, save only those emails contained in the aforesaid inventory.

(e) In the event that the Parties deem it necessary, the Parties shall appoint a neutral third party to verify compliance with part (4)(d) above.

COMPUTER FORENSICS PROTOCOL

This Computer Forensics Protocol is hereby entered into on this ____ day of _____, 2015, by and between [the Company] (“Company”), and [the Employee] (“Employee”) (collectively the “Parties”).

WHEREAS Employee is currently in possession of (1) a [Smartphone] (the “Smartphone”); (2) a Laptop computer (the “Laptop”); and (3) several external flash data storage devices (the “Flash Drives” and, collectively with the Laptop and the Smartphone, the “Personal Devices”); and

WHEREAS the Personal Devices are Employee’s own personal property; and

WHEREAS the Personal Devices may contain electronic data, (1) some of which may be the property of the Company (the “Company Property”); and (2) some of which is Plaintiff’s personal and private data (for example, private financial and medical data and spousal and other family communications) (hereafter the “Private Data”); and (3) some of which is privileged attorney-client communications between Plaintiff and his Counsel and/or the privileged attorney work product of Plaintiff’s Counsel (hereafter the “Privileged Data”) (all of the aforementioned data is hereafter collectively referred to as the “Data Set”); and

WHEREAS the Parties are interested in coming to an agreement (hereafter a “Computer Protocol”) whereby Employee can return the Company Property to the Company in a manner which (1) maintains adequate protections for the Privileged Data and Private Data; and (2) can be effectuated in as efficient, expeditious, and cost-effective a manner as possible;

WHEREAS as part of ongoing settlement negotiations protected under Rule 408 of the Federal Rules of Evidence, the Parties’ respective counsel have conferred with one another in an attempt to reach an agreement on such a Computer Protocol; and

WHEREAS, as part of those same ongoing settlement negotiations under Rule 408 of the Federal Rules of Evidence, the Parties desire to enter into a Computer Forensics Protocol.

THE PARTIES HEREBY AGREE to the following Computer Forensics Protocol

I. ACQUISITION OF DATA

- 1) On [Date] Employee will provide the Personal Devices, and login information necessary to access those devices, to [Forensic Expert] (the “Forensic Expert”) at their location at [address].
- 2) The Personal Devices, and all other information provided to the Forensic Expert, including this protocol and all other communications between the Forensic Expert and Employee or Employee’s Counsel, shall be subject to the Confidentiality Agreement attached hereto as **Exhibit A** and shall further be considered to be communications made as part of ongoing settlement discussions protected under Rule 408 and shall be neither discoverable nor admissible in any future proceeding.
- 3) After providing the Personal Devices to the Forensic Expert, the Employee shall, under the supervision of the Forensics Expert, access certain private documents stored on the Smartphone (the “Sensitive Documents”) and review those documents with the Forensic Expert.
- 4) If the Forensics Expert agrees that a Sensitive Document is not Company Property then that document shall be deleted.
- 5) If the Forensics Expert disagrees as to whether any particular Sensitive Document is Company Property, then the document shall not be deleted.
- 6) At the conclusion of this process, the Forensics Expert shall transmit an e-mail communication to the Parties stating as follows “The deletion of Sensitive Documents from the Smartphone has been completed. I certify that the document(s) deleted were not Company Property.”
- 7) The Parties agree that the Forensics Expert shall not, under any circumstances, be called upon to testify, report, or provide any additional information whatsoever regarding the content of the Sensitive Documents or any discussion(s) had with, or information received from, Employee during the review and deletion of the Sensitive Documents. The Parties agree that this

restriction is in the mutual interest of both Parties, and mutually waive any issues, evidentiary or otherwise, which may arise from or relate to, in any manner, this restriction.

- 8) Following the deletion of Sensitive Documents from the Smartphone, the Forensics Expert shall create a forensic image the Personal Devices (collectively, the “Images”).
- 9) The Images shall be stored securely by the Forensics Expert in accordance with their normal business practices.
- 10) The Images, and their entire content, shall, as described above, be subject to the Confidentiality Agreement attached hereto as **Exhibit A**. The Parties hereby mutually agree to the terms of the Confidentiality agreement.

II. REMOVAL OF PRIVATE DATA, PRIVILEGED DATA, AND COMPANY PROPERTY

- 11) Prior to the creation of the Images, Employee shall work with the Forensic Expert to copy certain Private Data from the Personal Devices to an external storage device.
- 12) After Employee has removed the Private Data which he desires to retain from the Personal Devices, the Forensic Expert shall permanently delete, destroy, and remove beyond all possibility of recovery all information contained on those devices. At this time, Employee shall identify, and the Forensic Expert shall delete, all backups in the custody or control of the Employee for the Personal Devices. Employee shall provide login credentials as needed to effectuate this deletion.
- 13) The Parties mutually agree that they jointly request the permanent and irrevocable deletion of data described in Paragraph 12, above. The Parties mutually agree that the irrevocable deletion of data described in Paragraph 12, above, is in the interest of both Parties, and both Parties mutually waive any issues, evidentiary or otherwise, which may arise from or relate to, in any manner, the destruction of said information.

- 14) Any information provided by Employee to the Forensic Expert during this process shall constitute information provided in the course of ongoing settlement discussions protected under Rule 408 and shall be neither discoverable nor admissible in any future proceeding.
- 15) After the Personal Devices are wiped by the Forensics Expert, as described in Paragraph 12, above, they shall be returned to the Employee.

III. FORENSIC ANALYSIS OF THE IMAGES

- 16) The Forensics Expert shall conduct a forensic investigation of the Images.
- 17) The investigation shall constitute part of the course of ongoing settlement discussions protected under Rule 408 and shall be neither discoverable nor admissible in any future proceeding.
- 18) This investigation shall cover the time period between, and including, January 1, 2015 and the date on which the Personal Devices were provided to the Forensics Expert (the “Timeframe”)
- 19) The sole purpose of the investigation shall be to identify Company Property which was removed from the Personal Devices during the Timeframe.
- 20) This shall be accomplished by identifying all documents with the following attributes:
 - a. Any document which was printed during the Timeframe;
 - b. Any document which was uploaded to an online account during the Timeframe;
 - c. Any document which was transferred from a Personal Device to any other Device during the Timeframe; and
 - d. Any document created during the Timeframe.
- 21) The Images shall also be forensically examined to ensure that all backup accounts or devices are identified. Such backup accounts and devices, if not already destroyed pursuant to Paragraph 12, above, shall be deleted as described in the paragraph.

- 22) Documents contained in slack and unallocated space (i.e. deleted documents) shall be included in this process, however the Forensic Expert shall exclude from this search the Sensitive Documents deleted by Employee as provided by Paragraph 4, above.
- 23) Following the identification of these documents (the “Located Documents”), the Forensic Expert shall search the Located Documents for the following keywords:
- a. [LIST]
- 24) Copies of the Located Documents which are determined to contain one or more of the above keywords (the “Identified Documents”) will be transmitted to Employee’s counsel via e-mail at [e-mail].
- 25) The Forensic Expert shall prepare a list of the file names of the Identified Documents and shall transmit that list to the Parties.
- 26) The Parties shall jointly determine which, if any, of the Identified Documents are to be produced for further inspection.
- 27) If, upon inspection, any of the Identified Documents are determined to be Company Property (the “Returned Documents”), said document(s) shall be returned to the Company, and shall be the subject of further investigation as described below.

IV. FURTHER INVESTIGATION

- 28) A copy of the Returned Documents shall be provided to the Forensics Expert.
- 29) Upon receipt of the Returned Documents, the Forensics Expert shall examine the Returned Documents to determine whether each Returned Document was printed, uploaded, or transferred during the Timeframe.
- a. Transferred Documents

- 30) The Forensic Expert shall promptly provide to Employee and the Company a list of all Returned Documents which were transferred to a device not included in the investigation during the Timeframe.
- 31) If the device(s) is/are in employee's custody or control, then Employee shall promptly provide the device(s) to the Forensic Expert for examination following the protocol set forth above.
- 32) If the device(s) is/are not in employee's custody or control, then Employee shall cooperate with the Company in an attempt to obtain that device for examination following the protocol set forth above.

b. Printed Documents

- 33) The Forensic Expert shall promptly provide to Employee and the Company a list of all Returned Documents which were printed during the Timeframe.
- 34) Employee shall promptly provide the hard copy(ies) of the Returned Documents so created, if Employee has not already done so.

c. Uploaded Documents

- 35) The Forensic Expert shall promptly provide to Employee and the Company a list of all Returned Documents which were uploaded during the Timeframe.
- 36) Employee shall promptly provide the Forensic Expert with the login credential(s) necessary to access any account(s) over which Employee has custody or control to which Returned Documents were uploaded. Employee shall cooperate with Company to attempt to obtain login credential(s) necessary to access any account(s) over which Employee does not have custody or control.
- 37) Any information provided by Employee to the Forensic Expert during this process shall constitute information provided in the course of ongoing settlement discussions protected under Rule 408 and shall be neither discoverable nor admissible in any future proceeding.

- 38) The Forensic Expert shall access the Cloud Accounts and forensically examine them to determine whether the copy(ies) of the Returned Documents uploaded to that account were further disseminated.
- 39) If the Forensic Expert determines that the Returned Documents were not further disseminated, then they shall be permanently deleted from the Cloud Accounts.
- 40) If the Forensic Expert determines that the Returned Documents were further disseminated, then they shall be permanently deleted from the Cloud Accounts, and the account(s) or device(s) to which they were disseminated shall be examined as described above.
- 41) In either event, no further documents shall be produced to the Company aside from a report of the Forensic Expert detailing his or her findings, and the actions taken.

V. CONCLUSION OF INVESTIGATION & FURTHER PROCEEDINGS

- 42) Following the conclusion of the investigation, the Parties jointly agree and affirmatively request that the Forensic Expert take steps necessary to ensure that the Images shall not be further accessed by the Forensic Expert or any other entity without Employee's express, written authorization.
- 43) The Images shall be maintained by the Forensic Expert, at the sole cost and expense of Company, until such time as the Parties enter into a joint, written agreement providing for the destruction of the Images.
- 44) Company agrees that it shall not request access to the Images for any purpose and that, should it make such a request, Forensic Expert and Employee shall not comply with such a request.
- 45) Company and Employee agree and jointly recognize and affirm that Employee's consent to the forensic investigation described in this protocol shall not constitute assent to any further examination of the Images whatsoever.

- 46) Company and Employee further agree and jointly recognize and affirm that the fact of Employee's consent to the forensic investigation shall be confidential and shall not be admissible into evidence.
- 47) Should the Company initiate legal proceedings against Employee, or any third party, and seek discovery of documents or Electronically Stored Information which may be contained in the Images, then such discovery shall be served directly on employee, not the Forensics Expert.
- 48) Should Employee receive discovery or other form of compulsory process from Company seeking, in whole or in part, the information contained on one or more of the Images, then Employee shall work directly with the Forensic Expert to locate documents responsive to the Company's discovery requests. Employee shall review the documents so identified and produce those relevant to the Company's request(s).
- 49) The services of the Forensic Expert shall be paid by Company based on bills prepared by the Forensic Expert and redacted by the Employee to remove the content of confidential communications covered by this Agreement or the Confidentiality Agreement, attached hereto as **Exhibit A**.
- 50) The Confidentiality Agreement, attached hereto as **Exhibit A**, shall remain in full force and effect following the conclusion of the investigation.
- 51) The Parties mutually agree that Forensic Expert shall be governed by, and shall adhere to, the terms of the Confidentiality Agreement.
- 52) The Parties further mutually agree that, to the extent that, at any later point in time, discovery is sought from Employee of documents or electronically stored information ("ESI") which may be contained in the Images, that the Images

[EMPLOYEE]

Date

[NAME]

On Behalf of [COMPANY]

Date

Data Breaches: Form to Potential Clients

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave., N.W.
Suite 230

Washington, D.C. 20009

(202) 588-5300

(202) 588-5023 (fax)

fitzpatrick.law@verizon.net

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

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.

Below are guidelines which we ask that you adhere to during the course of our [discussions regarding possible] representation of you in this matter. These guidelines are intended to protect you against some of the perils which exist in 21st century employment disputes. Poor handling of evidence and employer property can give rise to claims which employers have learned to vigorously pursue and exploit. That said, please do not be alarmed by any of the guidelines below, but please do **inform us immediately** if you feel that you may already have run afoul of our recommendations so that we can take prompt action to address any problems.

- (1) It is important that you keep all communications between yourself and any attorney private. You should not share those communications with **anyone** who is not an attorney considering representing you.
- (2) You should only use personal accounts and devices to contact an attorney. You should not contact an attorney using a work-provided account (such as a work e-mail account). You should also not contact an attorney using a personal account from a work-provided device (such as accessing a personal e-mail account on a work-provided computer). Employers have ways of monitoring communications on devices and accounts that they control, and failure to follow this instruction can allow an employer to access your communications with us.
- (3) You must preserve all information which may be relevant to your matter in any way. This includes both hard-copy documents and electronically stored information such as e-mails, text messages, social media posts, photographs, call logs, and other information. **Do not destroy, delete, alter, or misplace relevant information.** If you are not sure whether something is relevant, or if you are not sure how to keep evidence safe, **contact us immediately.**
- (4) Do not take employer property without first consulting an attorney. This includes documents, files, contacts, and other information and property, whether it is physical or electronic. While most employees end up in possession of various employer files and property during the course of employment, consciously taking something after termination, in anticipation of termination, or to use against your employer during legal proceedings can lead to **substantial, sometimes criminal, penalties.**
- (5) If you have already taken your employer's property **do not deliver or transmit that property to our firm.** Instead, please **contact us immediately** so that we can more fully discuss the property in your possession and how we can best minimize any potential exposure which you may have.
- (6) Regardless of how you obtained them **do not deliver or transmit to our firm** the following types of documents:
 - a. Documents which are marked "confidential" , "trade secret" , "classified" , "secret" or similar words or phrases.

- b. Documents which are marked “privileged” .
 - c. Documents which contain communications with any attorney employed or retained by any other party;
 - d. Documents which contain medical information, health information, financial information, account numbers, social security numbers, or similar private information about any other individual(s).
- (7) We cannot review any documents which you deliver or transmit to us until you confirm, in writing, that you have reviewed those documents as described above.

Employee's Counsel's First Communications With New Client

by Robert B. Fitzpatrick

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 THESE MATERIALS.

Robert B. Fitzpatrick

- ▶ **Robert Brian Fitzpatrick** is the principal in the boutique law firm of Robert B. Fitzpatrick PLLC in Washington, D.C., which represents clients in employment law matters in the federal and state courts of the District of Columbia, Maryland and Virginia. Mr. Fitzpatrick has concentrated his practice in employment law disputes for over forty years. He has been a member of the D.C. Bar since 1968. He is the father of three, and grandfather of three



3

Fact Gathering

- ▶ Advise new client not to disclose to you any attorney–client privileged communications

MC

4

Document Gathering

- ▶ Be extraordinarily careful to authorize client to only transmit to you documents that s/he has properly obtained
- ▶ If your firm's size permits, have a "taint" team review documents.



MC

5

Client's Goals

- ▶ Focus on what the client's goals are, that is, what the client seeks to achieve



MC

6

Manage Expectations

- ▶ Share with client statistics regarding W/L rates at EEOC and summary judgment data.



MC

7

Proposed Settlement/Severance Agreement

- ▶ Many clients come in the door with a proposed settlement/separation agreement. Some merely want your review for “legal sufficiency,” and some want you to negotiate better terms.
- ▶ Most such proposals have a 21-day consideration period driven by the OWBPA.
- ▶ Reach out to the other side, immediately, to initiate a dialogue.



MC

8

Taxes

- ▶ Be certain to disclaim competence in tax law but be certain to advise client *typically*, most moneys obtained in settlement or judgment in employment cases are taxable.
- ▶ Send client IRS publications.
- ▶ Advise client to consult with tax counsel or CPA.



MC

9

Homonyms

- ▶ Discuss the difference between “principle” and “principal”.



MC

10

Statutes of Limitations

- ▶ Focus carefully on statutes of limitation with a disclaimer that it is early in the fact gathering process and additional facts may be unearthed that affect statutes of limitations.
- ▶ Be certain to discuss the time limit to file with EEOC, or to contact an EEO counselor in a federal sector case.

MC

11

Tolling Agreement

- ▶ Your best protection, short of filing, against a claim that you “blew” a statute of limitations, is to enter into a written tolling agreement with the defense.
- ▶ While the courts respect such agreements, there is substantial variance among federal, state, and local administrative agencies. DOL’s OSHA continues to decline to respect tolling agreements in SOX matters.

MC

12

Representation Agreement

- ▶ Representation agreement
- ▶ Be certain to have a *written* representation agreement that has all material terms.



MC

13

Costs

- ▶ Be certain that the representation agreement for litigation addresses whether the client is responsible to advance costs or whether the firm agrees to advance costs.



MC

14

Risks of Losing

- ▶ While typically the defense's attorneys' fees are not a risk that your client to which your client is exposed, the defense costs are. Not only can the bill of costs be quite substantial, some courts are allocating some of the electronic discovery costs to plaintiffs.



MC

15

Potential Counterclaims

- ▶ Is the defense threatening to sue your client? Or, does your fact-gathering reveal a potential counterclaim?
- ▶ Typically, counsel does not address, in the representation agreement, whether the scope of representation does or does not encompass counterclaims. Failure to do so, in many jurisdictions, means that counsel is working for free to defend the client against the counterclaim.



MC

16

A Release

- ▶ Be certain to determine whether or not the client has already signed a release of claims.



MC

17

Unemployment Compensation

- ▶ Many clients want to know if they are eligible for unemployment, and whether they should apply.
- ▶ Determine also whether the client also has already filed and the status of the matter.
- ▶ In your first substantive communication with the defense, determine whether it intends to oppose such a claim.



N

18

Hostage

- ▶ Prevent becoming a hostage to an irrational, irascible contingency client.
- ▶ If your bar permits, have representation agreement provide that client is responsible for full fees, at your stated hourly rate, if the client:
 - Makes a material misrepresentation of fact upon which you rely to undertake the representation; or
 - The client terminates the relationship with your firm without good cause.

MC

19

EEOC and Deferral Agency

- ▶ Explain the intake and investigative process at EEOC local office and local deferral agency.

MC

20

Newspaper Clipping

- ▶ Beware the client who regales you with stories from the media of jury verdicts and settlements in extraordinary amounts.



MC

21

Background Checks

- ▶ Remind the client that a court filing is readily accessible in a background check by a future employer.



MC

22

ADR/Mediation

- ▶ Explain ADR options available and share links to articles that explain mediation.
- ▶ If and when ADR becomes an available option, share links.



MC

23

Mitigation

- ▶ Emphasize that client has a duty to seek new employment and explain that you want periodic reports regarding the client's efforts and documentation of all such efforts.
- ▶ Highly recommend that you provide the client with a form/a template for the information that you want client to routinely record.
- ▶ Recordkeeping has become more difficult because so many applications are now online and cannot be printed.
- ▶ Be certain to have the client record all pertinent information about online applications.



MC

24

Confidentiality

- ▶ Implore your clients to not discuss, with others, what you and your client have discussed, or otherwise the attorney–client privilege is imperiled.
- ▶ Explain to your client that they are not to speak to the media or write anything online about the matter.



MC

25

Arbitration

- ▶ Be careful to be on the lookout for an arbitration clause, which could be in a job application, a handbook, or a separate stand-alone document.



MC

26

Choice of Law & Forum

- ▶ Check whether any document provides for a choice of law or forum.
- ▶ After *Atlantic Marine*, the choice of forum clause is nearly sacrosanct.



MC

27

Shortening of Limitations Period

- ▶ Be on the lookout for those employers who, in a writing, have attempted to shorten the statute of limitations applicable to employment claims.



MC

28

Bankruptcy

- ▶ Inquire whether the client is, or contemplates being in, a bankruptcy proceeding or, if in one, the client did list this matter.



MC

29

Mental Health Providers

- ▶ If the client is, or recently has been, in some form of therapy, obtain a HIPAA-compliant authorization to obtain records and to be authorized to communicate with therapist.



MC

30

Preservation

- ▶ Discuss, and document that you did, preservation obligations of the client, including social media and text messages.



MC

31

Social Media

- ▶ It may be wise, sometimes, to insist that, before you commit to the case, you need access to all of the client's social media documents.
- ▶ Explore whether client has documents, including ESI, that arguably s/he ought not to have and whether, and how, they might be returned to employer.



MC

32

Client Obligations to Employer

- ▶ Determine whether the client has signed a non-compete agreement or a confidentiality agreement, or a non-disclosure agreement (an NDA), or a “work for hire” agreement, or a non-solicitation agreement.



MC

33

Employment Agreement

- ▶ Determine whether there is a written employment agreement (EA). Many clients think the offer letter is an EA.



MC

34

Employee Handbook

- ▶ Determine whether there is an employee manual/handbook – that is, a document with company policies and procedures.
- ▶ If client does not have it, be certain to explore whether client can legitimately obtain it.



MC

35

Collateral Damage

- ▶ Explain your aversion to collateral damage, that is, for example, having an incumbent employee surreptitiously provide documents to your client, thus risking being “outed” in discovery.



MC

36

Lines of Communication

- ▶ Be certain to explain to client that communicating with you, using the employer's e-mail system, potentially compromises attorney-client privilege.



MC

37

X▶ **X**

MC

38

X

▶ X



MC

39

X

▶ X



MC

40

X

▶ X



MC

41

X

▶ X



MC

42

X

▶ X



MC

43

X

▶ X



MC

44

X

▶ X

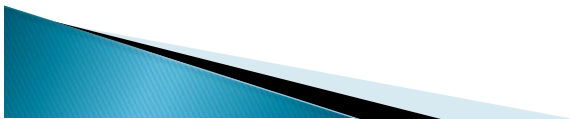


MC

45

X

▶ X



MC

46

X

▶ X



MC

47

X

▶ X



MC

48

X

▶ X



MC

49

X

▶ X



MC

50

X

▶ X



MC

51

X

▶ X



MC

52

X

▶ X



MC

53

X

▶ X



MC

54

X

▶ X



MC

55

X

▶ X



MC

56

X

▶ X



MC

57

X

▶ X



MC

58

X

▶ X



MC

59

X

▶ X



MC

60

X

▶ X

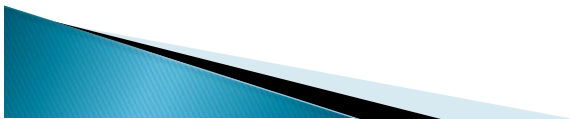


MC

61

X

▶ X



MC

62

X

▶ X



MC

63

X

▶ X



MC

64

X

▶ X



MC

65

X

▶ X



MC

66

X

▶ X



MC

67

X

▶ X



MC

68

X

▶ X



MC

69

X

▶ X



MC

70

X

▶ X



MC

71

X

▶ X



MC

72

X

▶ X



MC

73

X

▶ X



MC

74

X

▶ X



MC

75

X

▶ X



MC

76

X

▶ X

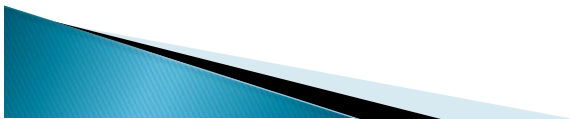


MC

77

X

▶ X



MC

78

X

▶ X



MC

79

X

▶ X



MC

80

X

▶ X



MC

81

X

▶ X



MC

82

X

▶ X



MC

83

X

▶ X



MC

84

X

▶ X



MC

85

X

▶ X



MC

86

X

▶ X



MC

87

X

▶ X



MC

88

X

▶ X



MC

89

X

▶ X



MC

90

X

▶ X



MC

91

X

▶ X



MC

92

X

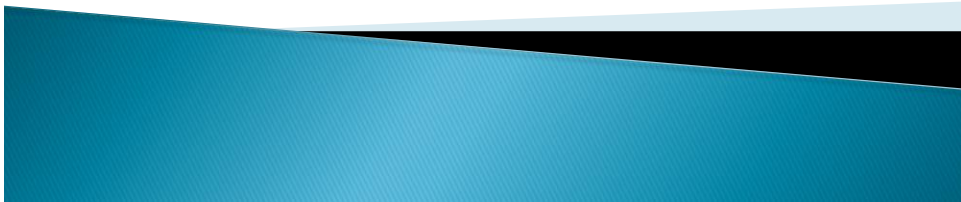
▶ X



MC

93

Cutting Edge Developments in Non-Competes and Trade Secrets for 2016



Drafting – Mandatory Forum Selection Clause

- ▶ *Torres v. SOH Distrib. Co.*, No. 3:10-cv-179, 2010 U.S. Dist. LEXIS 47448 (E.D. Va. May 13, 2010)
 - The clause stated that one “shall file any suit...only in federal or state court” in Pennsylvania, and court found it to be mandatory.



Drafting – Arbitrate Non-Compete Issues

- ▶ *Nitro-Lift Techs., LLC v. Howard*, 133 S. Ct. 500 (2012)
 - It was reserved for the arbitrator to decide whether a non-competes agreement violated applicable state law.



Drafting – Assignment

- ▶ *Guy Carpenter & Co. v. John B. Collins & Assocs.*, Civ. No. 05-1623, 2006 U.S. Dist. LEXIS 61765, 2006 WL 2502232 (D. Minn. Aug. 29, 2006)
- ▶ *Ascencea, L.L.C. v. Zisook*, Civ. No. 08-5339, 2011 U.S. Dist. LEXIS 36786, 2011 WL 1323017 (D.N.J. April 5, 2011)



Drafting – Assignment

- ▶ *Stuart C. Irby v. Tipton*, 796 F.3d 918 (8th Cir. 2015)



Litigation – Declaratory Judgment Action

- ▶ *McKenna v. PSS World Med., Inc.*, Civ. No. 09–0367, 2009 U.S. Dist. LEXIS 58292, 2009 WL 2007116 (W.D. Pa. July 9, 2009)
- ▶ *Lapolla Indus. v. Hess*, 750 S.E.2d 467 (Ga. App. 2013)



Enforcement – Signatories Missing

- ▶ *United States Risk Mgmt., L.L.C. v. Day*, 73 So. 3d 1100 (4th Cir. 2011).
- ▶ *Workflow Solutions v. Lewis*, 77 Va. Cir. 334, 2008 Va. Cir. LEXIS 186 (Va. Cir. Ct. 2008).
- ▶ *New Hanover Rent-A-Car, Inc. v. Martinez*, 525 S.E. 2d 487 (N.C. App. 2000).
- ▶ *Cameron Int'l Corp. v. Guillory*, 445 S.W.3d 840 (Tex. App. 2014)



Enforcement – Signed

- ▶ *EndoSurg Med., Inc. v. EndoMaster Med., Inc.*, 71 F. Supp. 3d 525 (D. Md. 2014)



Enforcement – Break in Service

- ▶ *Nightingale Home Healthcare, Inc. v. Helmuth*, 15 N.E.3d 1080 (Ind. App. 2014)
- ▶ *Truong, LLC v. Tran*, No. A-5752-11T1, 2014 N.J. Super. Unpub. LEXIS 64, 2013 WL 85368 (N.J. Super. Jan. 9, 2013)



Enforcement – Material Changes

- ▶ *Rent-A-PC, Inc. v. March*, Civ. No. 13-10978-GAO, 2013 U.S. Dist. LEXIS 74535, 2013 WL 2394982 (D. Mass. May 28, 2013)



Enforcement – Unilateral Material Breach

- ▶ *Smith–Schariff Paper Co., Inc. v. Blum*, 813 S.W. 2d 27 (Mo. Ct. App. 1991)



Enforcement – Electronic Signature

- ▶ *Neuson v. Macy's Dept. Stores, Inc.*, 160 Wn. App. 786, 249 P.3d 1054 (Wash. App. 2011)
- ▶ *People v. Hernandez*, 31 Misc. 3d 208 (N.Y. City Ct. 2011)
- ▶ *Adams v. Super. Ct.*, No. G042012, 2010 Cal. App. Unpub. LEXIS 1236, 2010 WL 602515 (Call. App. 4th Div. Feb. 22, 2010)
- ▶ *Labajo v. Best Buy Stores*, 478 F. Supp. 2d 523 (S.D.N.Y. 2007)



Enforcement – Wet Ink Signature

- ▶ *Campbell v. Gen'l Dynamics Gov't Sys., Corp.*, 407 F.3d 546 (1st Cir. 2005)



Enforcement – Consideration

- ▶ *Am. Well Corp. v. Osbourn*, Civ. No. 15-12265, 2015 U.S. Dist. LEXIS 160914 (D. Mass. Dec. 1, 2015)
- ▶ *Socko v. Mid-Atl. Sys. Of CPA, Inc.*, 126 A.3d 1266 (Pa. 2015)
- ▶ *Charles T. Creech, Inc. v. Brown*, 433 S.W.3d 345 (Ky. 2014)
 - Continued employment, standing alone, is insufficient consideration.
- ▶ *Runzheimer Int'l, Ltd. v. Friedlen*, App. No. 2013AP1392, 2014 Wisc. App. LEXIS 342, 2014 WL 1465157 (Wisc. App. April 15, 2014)
 - *Continued at-will employment constitutes sufficient consideration*



Statutes – Defend Trade Secrets Act

- ▶ H.R. 3326, S. 1890
- ▶ Voted out of Judiciary Committee with substitute amendment on Jan. 28, 2016
 - <https://www.congress.gov/bill/114th-congress/senate-bill/1890/actions>
- ▶ Text (as amended)
 - <https://www.congress.gov/bill/114th-congress/senate-bill/1890/text>
- ▶ No action in House since introduction.



Enforcement – Preliminary Injunction

- ▶ *Economic Research Serv., Inc. v. Resolution Economics, LLC*, No. 1:15-cv-1282, 2015 U.S. Dist. LEXIS 143274 (D.D.C. Oct. 21, 2015)
- ▶ *Burleigh v. Ctr. Pt. Contractors, Inc.*, 474 S.W.3d 887 (Ark. App. 2015)
- ▶ *Evans v. Generic Solution Engineering, LLC*, 178 So. 3d 114 (Fla. App. 5th Dist. 2015);
- ▶ *Great Lakes Home Health Servs, Inc. v. Crissman*, No. 15-cv-11053 (E.D. Mich. Nov. 2, 2015)



Enforcement – Preliminary Injunction

- ▶ *TransUnion Risk & Alternative Data Solutions, Inc. v. MacLachlan*, 625 Fed. Appx. 403 (11th Cir. 2015)
 - Rule 65, under *Erie*, trumps Florida statute precluding consideration of potential hardship.



Enforcement – TRO

- ▶ *Nicklas Assocs., Inc. v. Zimet*, No. GJH-14-3777, 2014 U.S. Dist. LEXIS 170071 (D. Md. Dec. 9, 2014)



Enforcement – Cease & Desist Letters

- ▶ *Bonds v. Philips Electronic N. Am.*, No. 2:12-cv-10371, 2014 U.S. Dist. LEXIS 6845, 2014 WL 222730 (E.D. Mich. Jan. 21, 2014)
- ▶ *Boudreaux v. OS Rest. Servs, L.L.C.*, No. 14-1169, 2015 U.S. Dist. LEXIS 8090 (E.D. La. Jan. 23, 2015)



Enforcement – Selective Enforcement

- ▶ *Custom Hardware Eng'g & Consulting, Inc. v. Dowell*, 918 F. Supp. 2d 916 (E.D. Mo. 2013)
- ▶ *Kohl's Dept. Stores, Inc. v. Schalk*, No. 2015-cv-001465 (Wis. Cir. Ct. Aug. 11, 2015) (unpub.)
- ▶ *Estee Lauder Cos., Inc. v. Batra*, 430 F. Supp. 2d 158 (S.D.N.Y. 2006)



Statutes – New State Laws

- ▶ **Alabama** – Code Section 8-1-1 (Eff. July 1, 2016)
- ▶ New Mexico – New law, effective July 1, 2015, limits non-compete clauses for doctors.
- ▶ **Arkansas** – New law permits blue-penciling of non-compete agreements
- ▶ **Wisconsin** – S.B. 69 (Trade Secrets and Unfair Competition Law) modifies enforceability of certain types of restrictive covenants.
<https://docs.legis.wisconsin.gov/2015/related/proposals/sb69>
- ▶ **Hawaii** – Effective July 1, 2015 Hawaii banned non-compete and non-solicit agreements with technology workers.




Statutes – Computer Fraud and Abuse Act


- ▶ *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015)
- ▶ *Tech. Sys., Inc. v. Pyles*, No. 13-1359, 2015 U.S. App. LEXIS 20004 (4th Cir. 2015) (unpub.)




Statutes – Proposed Federal Legislation

- ▶ Mobility and Opportunity For Vulnerable Employees Act (“MOVE” Act)
 - S. 1504
 - <https://www.congress.gov/bill/114th-congress/senate-bill/1504>
 - ▶ Limiting the Ability to Demand Detrimental Employment Restrictions Act (“LADDER” Act)
 - H.R. 2873
 - <https://www.congress.gov/bill/114th-congress/house-bill/2873>
 - ▶ Freedom for Workers to Seek Opportunity Act
 - H.R. 4254
 - <https://www.congress.gov/bill/114th-congress/house-bill/4254>
- 


Statutes – State Computer Crime Statutes

- ▶ National Conf. of State Legislatures, *Computer Crime Statutes* (June 12, 2015) (available at: <http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx>) (accessed Feb. 16, 2016)
 - ▶ Ark. Code Ann. § § 5-41-101 to 107
 - Civil cause of action for damages, including lost profits.
- 

Statutes – Preemption

- ▶ *Jenkins v. APS Ins., LLC*, 431 S.W.3d 356 (Ark. App. Div. One 2013)
 - Conversion of trade secrets claim preempted by state Trade Secrets Act.
 - ▶ *Halperin v. Uber Techs., Inc.*, No. 15-cv-02401, 2015 U.S. Dist. LEXIS 99195 (N.D. Cal. July 29, 2015)
 - ▶ *Lifeline Food Co. v. Gilman Cheese Corp.*, No. 5:15-cv-00034, 2015 U.S. Dist. LEXIS 64155 (N.D. Cal. May 15, 2015)
 - ▶ *Orca Communs. Unlimited, LLC v. Noder*, 337 P.3d 545 (Ariz. 2014)
 - ▶ *KF Jacobsen & Co. v. Gaylor*, 947 F. Supp. 2d 1120 (D. Ore. 2013)
- 

Statutes – Preemption

- ▶ *Stolle Machinery Co., LLC v. RAM Precision Indus.*, 605 Fed. Appx. 473 (6th Cir. 2015)
 - ▶ Julie Piper, *Comment: I Have A Secret?: Applying the Uniform Trade Secrets Act to Confidential Information That Does Not Rise to the Level of Trade Secret Status*, 12 Marq. Intell. Prop. L. Rev. 359 (Summer 2008) (available at: <http://scholarship.law.marquette.edu/iplr/vol12/iss2/4/>) (accessed Feb. 16, 2016)
- 

Enforcement – Choice of Law

- ▶ *Ascension Ins. Holdings, LLC v. Underwood*, C.A. No. 9897–VCG, 2015 Del. Ch. LEXIS 19 (Del. Ch. Ct. Jan. 28, 2015)
 - The ability to self-order is the sine qua non of free markets; without the ability to hold and dispose of property, and to agree to be bound contractually, no functional market could exist. Nonetheless, most if not all jurisdictions have determined as a matter of public policy that some contractual obligations are so pernicious that they must be removed from the self-ordering realm. To protect those policy interests, and for reasons of comity, states embracing the Restatement approach recognize that necessary to the right of a jurisdiction to limit contractual ordering for its citizens is a limitation on the ability of contracting parties to choose the law of a foreign jurisdiction which does not impose that limitation, and which itself has little or no interest in the enforcement of the contract at hand.



Enforcement – Choice of Law

- ▶ *Atl. Diving Supply, Inc. v. Moses*, No. 2:14–cv–380, 2014 U.S. Dist. LEXIS 105364, 2014 WL 3783343 (E.D. Va. July 31, 2014)
- ▶ *Edwards Moving & Rigging, Inc. v. W.O. Grubb Steel Erection, Inc.*, No. 3:12–cv–146, 2012 U.S. Dist. LEXIS 56818 (E.D. Va. April 23, 2012)



Enforcement – Choice of Law

- ▶ *Brown & Brown, Inc. v. Johnson*, 34 N.E. 3d 35 (N.Y. 2015)
 - N.Y. Court of Appeals refused to enforce Florida Choice-of-Law clause.
- ▶ *Cardonia v. Prosperity Bank*, 805 F.3d 573 (5th Cir. 2015)



Common Law – Fiduciary Duties & Duty of Loyalty

- ▶ *Stuart C. Irby Co., Inc. v. Tipton*, 796 F.3d 918 (8th Cir. 2015)
 - Solicited employees before he quit.
- ▶ *Ritlabs, SRL v. Ritlabs, Inc.*, No. 1:12-cv-215, 2012 U.S. Dist. LEXIS 171232, 2012 WL 6021328 (E.D. Va. Nov. 30, 2012)
- ▶ *Kaye v. Rosefelde*, 121 A.3d 862 (N.J. 2013)
- ▶ *TalentBurst, Inc. v. Collabera, Inc.*, 567 F. Supp. 2d 261 (D. Mass. 2008)
- ▶ *Contract Assocs. V. Atalay*, No. 1:14-cv-882, 2015 U.S. Dist. LEXIS 48129 (E.D. Va. April 10, 2015)
- ▶ *Tech. Sys., Inc. v. Pyles*, No. 13-1359, 2015 U.S. App. LEXIS 20004 (4th Cir. 2015) (unpub.)



Interpretation – Blue Penciling

- ▶ *AssuredPartners, Inc. v. Schmitt*, Nos. 1–14–1863, 1–14–2242, 2015 Ill. App. LEXIS 813 (Ill. App. 1st Dist. Oct. 26, 2015)
- ▶ *Clark’s Sales & Serv. v. John D. Smith & Ferguson Enters.*, 4 N.E.3d 772 (Ind. App. 2014)



Interpretation – Overbreadth

- ▶ *Distrib. Serv., Inc. v. Rusty J. Stevenson & Rugby IPD Corp.*, 16 F. Supp. 3d 964 (S.D. Ind. 2014)
- ▶ *NanoMech, Inc. v. Suresh*, 777 F.3d 1020 (8th Cir. 2015).



Enforcement – Timing of Signing

- ▶ *Dawson v. Ameritox, Ltd.*, 571 Fed. Appx. 875 (11th Cir. 2014)
- ▶ *Charles T. Creech, Inc. v. Brown*, 433 S.W.3d 345 (Ky. 2014)



Enforcement – Independent Contractors

- ▶ *Swinney v. Amcomm Telecomms., Inc.*, 30 F. Supp. 3d 629 (E.D. Mich. 2014)



Special Applications – Attorneys

- ▶ *In re: Karl N. Truman*, 7 N.E. 3d 260 (Ind. 2014)
- ▶ D.C. Bar Legal Ethics Opinion No. 368 (Feb. 2015) – <https://www.dcbar.org/bar-resources/legal-ethics/opinions/Ethics-Opinion-368.cfm>




Special Applications – Physicians


- ▶ *Pinnacle Healthcare, LLC v. Sheets*, 17 N.E. 3d 947 (Ind. App. 2014)




Enforcement – Forum Selection Clauses

- ▶ *AAMCO Transmissions, Inc. v. Romano*, 42 F. Supp. 3d 700 (E.D. Pa. 2014)
 - ▶ *Hartstein v. Rembrandt IP Solutions*, No. 12-2270, 2012 U.S. Dist. LEXIS 105984, 2012 WL 3075084 (N.D. Cal. July 30, 2012)
 - ▶ *Hosick v. Catalyst IT Servs, Inc.*, No. 3:15-cv-01100-SI, 2015 U.S. Dist. LEXIS 150281 (D. Or. Nov. 5, 2015)
 - ▶ *Marcotte v. Micros Sys.*, No. C 14-01372, 2014 U.S. Dist. LEXIS 128054 (N.D. Cal. Sept. 11, 2014).
- 


Interpretation – Social Media

- ▶ *Invidia, LLC v. DiFonzo*, 30 Mass. L. Rep. 390 (Mass. Super. 2012)
 - Facebook
 - ▶ *KNF&T Staffing, Inc. v. Muller*, 31 Mass. L. Rep. 561 (Mass. Super. 2013)
 - LinkedIn
 - ▶ *Cellular Accessories for Less, Inc. v. Trinitas, LLC*, No. 12-06736, 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014)
 - Ownership of Social Media Account
- 

Interpretation – Social Media

- ▶ *Corporate Technologies, Inc. v. Hartnett*, 731 F.3d 6 (1st Cir. 2013)
 - Email
 - ▶ *BTS, USA, Inc. v. Executive Perspectives, LLC*, No. X10-CV-116010685, 2014 Conn. Super. LEXIS 2644 (Conn. Super. Oct. 16, 2014)
 - LinkedIn
 - ▶ *Pre-Paid Legal Servs. v. Cahill*, 786 F.3d 1287 (10th Cir. 2015)
 - Facebook
- 

Interpretation – Social Media

- ▶ *Enhanced Network Solutions Group, Inc. v. Hypersonic Techs. Corp.*, 951 N.E.2d 265 (Ind. App. 2011)
 - ▶ *Amway Global v. Woodward*, 744 F. Supp. 2d 657 (E.D. Mich. 2010)
 - ▶ *Eagle v. Morgan*, No. 11-4303, 2013 U.S. Dist. LEXIS 34220 (E.D. Pa. March 12, 2013)
 - Ownership of LinkedIn Account
- 

Special Applications – Headhunters and Staffing Agencies

- ▶ *Kforce Inc. v. Beacon Hill Staffing Group LLC*, No. 4:14-cv-1880, 2015 U.S. Dist. LEXIS 1861 (E.D. Mo. Jan. 8, 2015)



Enforcement – Reimbursement of Training Costs

- ▶ *USS-Posco Indus. v. Case*, Nos. A140457, A142145, 2016 Cal. App. LEXIS 49 (Cal. App. 1st Dist., Div. One Jan. 26, 2016)



Tips – Strategy

- ▶ Scott Holt, *Strategy – Pros and Cons of Suing the Ex-Employee’s New Employer*, Delaware Non-Compete Law Blog (July 11, 2012) (available at: <http://www.delawarenoncompetelawblog.com/2012/07/pros-and-cons-of-suing-the-ex.html>) (accessed Feb. 16, 2016).



Tips – Drafting

- ▶ Scott Holt, *What Should Be In Your Noncompete Agreement*, Delaware Non-Compete Law Blog (Feb. 9, 2016) (available at: <http://www.delawarenoncompetelawblog.com/2016/02/what-should-be-in-your-noncompete-agreement.html>) (accessed Feb. 16, 2016)



Trade Secrets – Defense of Independent Development

- ▶ *Moore v. Kulicke & Soffa Indus.*, 318 F.3d 561 (3d Cir. 2003)



Trade Secrets – Defense of Reverse Engineering

- ▶ *Midland-Ross Corp. v. Sunbeam Equip. Corp.*, 316 F. Supp. 171 (W.D. Pa. 1970)
- ▶ *Aqua Connect, Inc. v. Code Rebel, LLC*, No. CV 11-5764, 2011 U.S. Dist. LEXIS 124086, 2011 WL 5075421 (C.D. Cal. Oct. 25, 2011)
- ▶ *Out of the Box Devs., LLC v. LogicBit Corp.*, 2012 NCBC 53, 2012 NCBC LEXIS 55 (N.C. Super. Oct. 30, 2012)



Trade Secrets – Defense of Reverse Engineering

- ▶ Texas Uniform Trade Secrets Act, § 134A.001, defines reverse engineering
 - "Reverse engineering" means the process of studying, analyzing, or disassembling a product or device to discover its design, structure, construction, or source code provided that the product or device was acquired lawfully or from a person having the legal right to convey it.
 - § 134A.002(5)



Enforcement – Termination Without Cause

- ▶ *Jorgensen v. United Commons Group, Ltd. P'ship*, No. 8:10-cv-00429, 2011 U.S. Dist. LEXIS 95426, 2011 WL 3821533 (D. Md. Aug. 25, 2011)



Enforcement – Asset & Stock Purchase

- ▶ *Amerigas Propane, LP v. Coffey*, No. 13-cvs-11778, 2014 NCBC 4, 2014 NCBC LEXIS 4, 2014 WL 580174 (N.C. Super. Feb. 11, 2014)

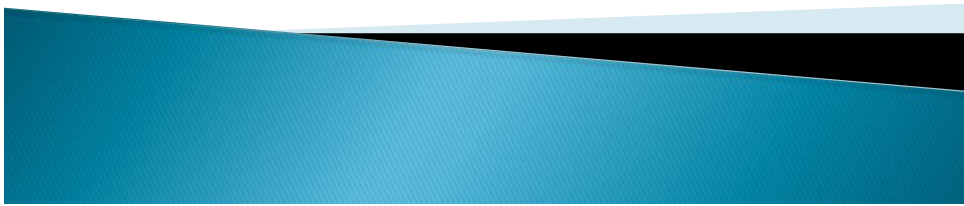


Enforcement – Absence of Unique Professional Skills

- ▶ *Genex Coop., Inc. v. Contreras*, No. 2:13-cv-03008, 2014 U.S. Dist. LEXIS 141417 (E.D. Wash. Oct. 3, 2014)



Questions?



With Friends Like These...: Non-Solicitation Agreements and Social Media

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave., N.W.
Suite 230

Washington, D.C. 20009

(202) 588-5300

(202) 588-5023 (fax)

fitzpatrick.law@verizon.net

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

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 THESE MATERIALS.

With Friends Like These: Non-Solicitation Agreements and Social Media

by Robert B. Fitzpatrick

As social media further permeates our work culture, courts are in the difficult position of drawing lines between what constitutes an impermissible behavior online and what does not. In the context of non-solicitation agreements, two recent cases demonstrate the lines beginning to emerge, oftentimes with little clarity or justification, around online behavior related to the workplace.

I. Failure to Consider Social Media During Drafting Can Unintentionally Limit the Reach of Restrictive Covenants

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.

II. 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.

III. 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](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/>.

IV. Going Forward

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.

Protecting Corporate Assets from Departing Employees

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Avenue, N.W.
Suite 230
Washington, D.C. 20009
(202) 588-5300
(202) 588-5023 (fax)
fitzpatrick.law@verizon.net (e-mail)
<http://www.robertbfitzpatrick.com> (website)

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 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.

Practical Tips to Handle Departing Employees Pre and Post Termination

Robert B. Fitzpatrick, PLLC

3

“One Piece at a Time” Johnny Cash

- Well, I left Kentucky back in '49
An' went to Detroit workin' on a 'sembly line
The first year they had me puttin' wheels on cadillacs

Every day I'd watch them beauties roll by
And sometimes I'd hang my head and cry
'Cause I always wanted me one that was long and
black.

One day I devised myself a plan
That should be the envy of most any man
I'd sneak it out of there in a lunchbox in my hand
Now gettin' caught meant gettin' fired
But I figured I'd have it all by the time I retired
I'd have me a car worth at least a hundred grand.

[CHORUS]
I'd get it one piece at a time
And it wouldn't cost me a dime
You'll know it's me when I come through your town
I'm gonna ride around in style
I'm gonna drive everybody wild
'Cause I'll have the only one there is a round.

So the very next day when I punched in
With my big lunchbox and with help from my friends

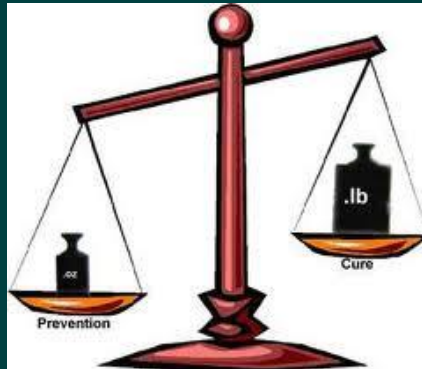
- I left that day with a lunch box full of gears
Now, I never considered myself a thief
GM wouldn't miss just one little piece
Especially if I strung it out over several years.



Robert B. Fitzpatrick, PLLC

4

Preventative Measures



Robert B. Fitzpatrick, PLLC

5

Using Restrictive Covenants: Keep Agreements Jurisdiction-Specific

Some State Laws

Regarding Non-Competes

- California (Cal. Bus. & Prof. Code § 16600): Many non-competes are unenforceable
- Nevada (NRS 613.200): Potential Criminal Penalties
- Connecticut bill (H.B. 6658, 2013 Leg. Sess. (Conn. 2013)): Notification & Review Period



By 605 © <http://stephen60.wordpress.com>

Robert B. Fitzpatrick, PLLC

6

Using Restrictive Covenants: Keep Agreements Jurisdiction-Specific

Some State Computer- Abuse Statutes

- Maryland - Md. Code Ann. Crim. Law § 7-302 (Lexis 2013)
- California - Cal. Penal Code § 502 (Deering 2013)
- Delaware - 11 Del. C. § 931 (Lexis 2013)



Robert B. Fitzpatrick, PLLC

7

Using Restrictive Covenants: Keep Agreements Up-to-Date

- Changes to the employee's job can void non-competes:
 - Promotions
 - Updated Compensation
 - Job Transfers



Robert B. Fitzpatrick, PLLC

8

Using Restrictive Covenants: Keep Agreements Up-to-Date

- Changes to the employer can void non-competes:
 - New Entity
 - Change in Control
 - Location Change
 - *Grace Hunt IT Solutions, LLC v. SIS Software, LLC, et al.*, 29 Mass. L. Rep. 460 (2012)
- Sometimes this can be addressed via contract:
 - *TEKSystems, Inc. v. Fletcher*, Civ. No. 10-11452011 U.S. Dist. LEXIS 22227 (D. Md. Mar. 2, 2011)

Robert B. Fitzpatrick, PLLC

9

Using Restrictive Covenants: Scope of Job Restrictions

- Excessive restrictions on work employee can perform in the future are unenforceable:
 - Work/responsibilities actually performed for employer
 - Unique, specialized skills



Robert B. Fitzpatrick, PLLC

10

Using Restrictive Covenants: Geographic Scope

- Geographic region
 - Reasonably necessary for the protection of the employer
 - Limited to regions where employer does business
 - Limited to regions where employer has customers

Robert B. Fitzpatrick, PLLC

11

Using Restrictive Covenants: Duration

- Duration should be reasonable to protect employer's interests.
- Two approaches:
 - Time needed to hire & train replacement
 - Duration of departing employee's "competitive edge"

Robert B. Fitzpatrick, PLLC

12

Using Restrictive Covenants: Non-Solicit Agreements

- Non-solicits are often viewed more favorably by courts than non-competes
- They will still be struck down if overbroad
 - *Newport Capital Group, LLC v. Loehwing*, Civ. No. 11-2755, 2013 U.S. Dist. LEXIS 44479 (D.N.J. Mar. 28, 2013) (Overbroad definition of a “prospective customer”)



Robert B. Fitzpatrick, PLLC

13

Using Restrictive Covenants: 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)

Robert B. Fitzpatrick, PLLC

14

Using Restrictive Covenants: Provide for Forfeiture and Clawbacks

- Clawbacks
 - Recovery of paid or unpaid compensation permitted if employee breaches fiduciary duty
 - *Janssens v. Freedom Med., Inc.*, Civ. No. 10-2042, 2011 U.S. Dist. LEXIS 46670 (D. Md. April 29, 2011)

Policies

- Develop policies to address problem areas:
 - Computer Use
 - Network authorization
 - Passwords
 - Remote Access/Remote Computing
 - System Administrators
 - Federal Contractors

Limit Access: Ensure the Secrecy of Confidential Information



- Uniform Trade Secrets Act:
 - Information is not generally known; and
 - “is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

Robert B. Fitzpatrick, PLLC

17

Limit Access: Ensure the Secrecy of Confidential Information

- To enforce, secrets must be identified with “reasonable particularity”
- Bottom line: make good use of passwords and policies to prohibit employee access to files without authorization

Robert B. Fitzpatrick, PLLC

18

Limit Access: Limit Authorization to Access Important Company Information

- The Computer Fraud & Abuse Act (“CFAA”)
 - Accessing a computer without authorization
 - Exceeding authorized access
 - Requires a showing of damage or loss

Robert B. Fitzpatrick, PLLC

19

Limit Access: Limit Authorization to Access Important Company Information

- Fourth and Ninth Circuits have a narrow definition of “unauthorized access”.
 - *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012)
 - *WEC Carolina Energy Solutions, LLC v. Miller et al.*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S.Ct. 831 (2013)

Robert B. Fitzpatrick, PLLC

20

Limit Access: Limit Authorization to Access Important Company Information

- The First and Third Circuits have a broad definition of “unauthorized access”:
 - *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001)
 - *U.S. v. Tolliver*, 451 Fed. Appx. 97 (3d Cir. 2011)

Robert B. Fitzpatrick, PLLC

21

Limit Access: Passwords

- Effective Password Management:
 - Have a written policy
 - Don't write passwords down
 - Store passwords digitally in a secure location

Robert B. Fitzpatrick, PLLC

22

Limit Access: Passwords

P@\$WORD

(Do Not Use This!)

- Hallmarks of a strong password:
 - Use letters (upper and lower case), numbers, and symbols
 - Do not use dictionary words
 - Eight or more characters long
 - Change passwords regularly (every 2-3 months)
 - Never write your password down or save it on your computer

Robert B. Fitzpatrick, PLLC

23

Limit Access: Passwords

- How to remember strong passwords:
 - Use the first letter of each word of a long phrase interspersed with symbols and numbers
 - Use a long phrase as your password. Windows can support up to 127 character passwords. A sufficiently long phrase is a strong password even if it contains dictionary words (e.g. “This is My 3rd New password this Year!”)

Robert B. Fitzpatrick, PLLC

24

Limit Access: Passwords

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN

Tr0ub4dor &3

CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION

(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON ERRORS)

~28 BITS OF ENTROPY

$2^{28} = 3$ DAYS AT 1000 GUESSES/SEC

(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE: YES. CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD

correct horse battery staple

FOUR RANDOM COMMON WORDS

~44 BITS OF ENTROPY

$2^{44} = 550$ YEARS AT 1000 GUESSES/SEC

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE. CORRECT.

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

Robert B. Fitzpatrick, PLLC

Courtesy: xkod.com/936/

25

Limit Access: HMV – An Object Lesson



- “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>

Robert B. Fitzpatrick, PLLC

26

Limit Access: Social Media

- Carefully define ownership and scope of use of social media accounts:
 - *PhoneDog v. Kravitz*, Civ. No. 11-03474, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011)
 - *Eagle v. Morgan*, Civ. No. 11-4303, 2011 U.S. Dist. LEXIS 147247 (E.D. Pa. Dec. 22, 2011)
- Address social media usage issues in a written policy

Robert B. Fitzpatrick, PLLC

27

Create Document Return Policies

- Specify the return of both hard and soft copies
- Address the “Three Cs”
 - **C**o-mingling (of personal/work docs);
 - **C**ompliance (verifying)
 - **C**ost
- Have a standard protocol



Robert B. Fitzpatrick, PLLC

28

Courtesy: mandaw.blogspot.com

Mobile Computing Bring Your Own Device

- Have a written policy!
- Problems:
 - Monitoring use of devices
 - Protecting information from loss/theft
 - Prevent employee data theft
- Solutions:
 - Require installation of monitoring software
 - Require installation of remote-wipe software
 - Use software to prevent “pod slurping”

Robert B. Fitzpatrick, PLLC

29

Mobile Computing Bring Your Own Device

- Hacked phones can be used as listening and recording devices
- Prohibit employees from carrying smart phones and other devices with recorders into important business meetings



Image: Stefan Rousseau/PA Wire

Robert B. Fitzpatrick, PLLC

30

Mobile Computing “Workshifting”

- Mobile computing and work shifting heighten ability of employees to obtain and hide employer documents
 - “Cloud” Computing
 - Personal hardware
- Employment contracts should address these topics



Courtesy: wombletradesecrets.blogspot.com

Robert B. Fitzpatrick, PLLC

31

Protecting Good Will

- Clear & Consistent expectations regarding employee and ex-employee communications
 - Confidentiality
 - Non-disparagement
 - Social Media
- Review NLRB Reports on Social Media Usage
 - <http://www.nlr.gov/node/5078>



32

Robert B. Fitzpatrick, PLLC

Courtesy: www.stoelivesworldofemployment.com

Employee Training

- Train IT staff on basic tasks:
 - Imaging devices
 - Preservation
 - Data recovery
- Chain of Custody (Procedures & Forms)
- Involve IT in terminations

Robert B. Fitzpatrick, PLLC

33

Managing Termination



Robert B. Fitzpatrick, PLLC

34

Termination Checklist

- Disable access to digital systems, devices, & accounts
- Retrieve access cards, keys, and badges
- Advise security that the employee is not to be permitted on the premises

Robert B. Fitzpatrick, PLLC

35

Termination Checklist

- Secure the employee's laptop, desktop, and Company-issued devices
- Secure the employee's office/cubicle
- Arrange for the employee to remove personal possessions, under careful supervision, with **as little embarrassment as possible**



Do Not Do This

Telegraph Media, 2013

Robert B. Fitzpatrick, PLLC

36

Exit Interview

- Incentivize departing employees to participate in exit interviews
- Have a well thought out checklist:
 - Return of documents
 - Return of other property
 - Discuss employee's continuing obligations
 - Retrieval of employee's property from his/her office

Robert B. Fitzpatrick, PLLC

37

Exit Interview

- Key employee obligations:
 - Statutory (CFAA, Trade Secrets)
 - Contractual (Restrictive Covenants, Non-Disparagement, Confidentiality)
 - Common Law (Fiduciary Duties)
 - Consequences (Clawback)

Robert B. Fitzpatrick, PLLC

38

Exit Interview

- Involve an IT professional in planning and executing this meeting
- If the exit interview or employee behavior evinces “red flags”, consider preemptively conducting a forensic examination of the employee’s electronic device(s)

Robert B. Fitzpatrick, PLLC

39

Forensic Examinations

- Look for signs of:
 - USB Connections
 - Printer Usage
 - Scanned Documents
 - E-mailed documents
 - Read/reviewed documents
 - Uploaded documents
 - Phone records
 - Access to personal accounts over the internet
- Handle this examination with care to avoid privileged and private information
- This investigation may be instrumental in discovering evidence of document theft, collusion with new employer, and/or collusion with other employees



Robert B. Fitzpatrick, PLLC

40

First Communication With Departing Employee's Attorney

- Remind the attorney of his/her client's obligations
 - Contractual (e.g. Return of documents, return of property, non-compete obligations, etc.)
 - Statutory (e.g. the CFAA, state computer use statutes, state Trade Secrets statutes, etc.)
 - Common Law (e.g. fiduciary duties)

First Communication With Departing Employee's Attorney

- Signal willingness to negotiate a reasonable protocol regarding the return of documents
- Discuss how personal information can be segregated from company owned information

First Communication With Departing Employee's Attorney

- Remind the attorney of his/her client's preservation obligations
- Identify the devices and/or information to be preserved (e.g. personal laptop, text messages, audio/video recordings, e-mail, web browser history, etc.)

Robert B. Fitzpatrick, PLLC

43

Navigating the Ethical Minefield

- Notify employees that the Company can access all information stored on its servers
- Nevertheless, avoid accessing:
 - Attorney-client privileged material
 - Private Medical information
 - Private financial information



Robert B. Fitzpatrick, PLLC

Navigating the Ethical Minefield

- Ethical implications of encouraging, aiding, and/or abetting document theft
- Ethical issues if counsel takes possession of stolen documents

Robert B. Fitzpatrick, PLLC

45

Indemnification Clauses

- Review indemnification obligations carefully prior to termination
- Determine if the Company is arguably required to advance fees and costs to a departing executive in the event that the Company asserts claims against that executive, either under contract or under law (e.g. § 18-108 of the Delaware Limited Liability Company Act)
- If so, can the Company contractually or legally exclude such claims from its indemnification obligations

Robert B. Fitzpatrick, PLLC

46

Additional Resources

- Dan Blake, Five Mistakes to Avoid in Drafting Non-Compete and Non-Solicitation Agreements, EPLI Risk, May 22, 2013, <http://eplirisk.com/five-mistakes-to-avoid-in-drafting-non-compete-agreements/>
- Harry Jones, Recent Study Reveals Troubling Amount of Employee Misuse and Theft of Company Data, Unfair Competition & Trade Secrets Counsel, Mar. 19, 2013, <http://www.unfaircompetitiontradesecretsandtradejournal.com/conversion/recent-study-reveals-troubling-amount-of-employee-misuse-and-theft-of-company-data/>
- Kenneth J. Vanko, When a Restriction on Soliciting “Prospective” Customers is Unreasonable (and How to Fix It), Legal Developments in Non-Competition Agreements, Apr. 25, 2013, <http://www.non-competes.com/2013/04/when-restriction-on-soliciting.html>
- Ron Williams, Protecting Your Crown Jewels: Preventing Against and Responding to Intellectual Property Theft, Smart Business, June 1, 2011, <http://www.sbnonline.com/2011/06/protecting-your-crown-jewels-preventing-against-and-responding-to-intellectual-property-theft/>

Exit Interviews of Departing Employees:

Checklists for Employers and Employees

by

Robert B. Fitzpatrick, Esq.
Fitzpatrick Law Group
1666 Connecticut Ave., N.W.
Suite 230
Washington, D.C. 20009
(202) 588-5300 (phone)
(202) 588-5023 (fax)

rfitzpatrick@robertbfitzpatrick.com

<http://www.robertbfitzpatrick.com> (website)

<http://robertbfitzpatrick.blogspot.com> (blog)

Exit Interviews of Departing Employees:

Checklists for Employers and Employees

by Robert B. Fitzpatrick

Robert B. Fitzpatrick, PLLC
1666 Connecticut Avenue, N.W., Suite 230
Washington, D.C. 20009
Telephone: (202) 588-5300
Facsimile: (202) 588-5023

E-mail: rfitzpatrick@robertbfitzpatrick.com

I. EMPLOYEE'S CHECKLIST

1. Hard Copies of Documents

- a. Have a substantial discussion with the departing employee regarding hard copies of documents that the individual has in their possession. If HR is conducting the exit interview, HR ought to consult with management of the departing employee, seeking a comprehensive list of documents or types of documents that the employee might have. Certainly, HR ought to inquire about:
 - i. Customer lists;
 - ii. Past sources of funding;
 - iii. Current customer requirements;
 - iv. Price lists;
 - v. Market studies;
 - vi. Business plans;
 - vii. Historical financial information;
 - viii. Company financial projections and budgets;
 - ix. Company historical and projected sales;
 - x. Company capital spending budgets and plans;
 - xi. All notes, summaries, and other material regarding the foregoing.

2. Soft Copies of Documents

- a. Soft copies refer to digital or electronically stored documents or information ("ESI").
- b. The departing employee may have ESI on external storage devices, may have e-mailed ESI to a personal account (either their own or those of a relative or friend), may have transferred ESI to a personal device, or may even have e-mailed documents to a third party or potential competitor.
- c. The departing employee may have brought one or more personal devices to work and, under an implicit or explicit BYOD policy, have work documents on the personal device.
- d. The departing employee should be questioned about all of the techniques which can be used to move ESI from the work site to the employee's possession.

- e. Where red flags are up or the departing employee is not fully cooperating, bring in IT to forensically examine the employee's company devices to determine what has been transferred, in particular, what has been transferred shortly prior to departure.
3. Return of Company-Issued Devices
 - a. Company-issued devices often contain personal information. If possible, you should work cooperatively with the employee to allow the employee, with appropriate supervision, to remove the personal material from the company-issued device.
 4. Documents Which the Employee May Keep.
 - a. Be open to permitting the departing employee to retain specific documents.
 - b. Provide the employee with the opportunity to articulate which specific documents s/he would like to retain.
 5. User Accounts and Passwords
 - a. Disable the departing employee's passwords and accounts immediately.
 - b. If you have noticed red flags, you might change passwords for accounts which the departing employee had access to.
 - c. You may also change the passwords of the departing employee's co-workers, as the departing employee may have learned them during the course of business.
 6. Certification
 - a. Have the departing employee certify in writing that s/he has returned all hard and soft documents, with the agreed-upon exceptions.
 7. Remind of Agreements
 - a. If the departing employee signed an NDA, a confidentiality agreement, a non-solicitation agreement, or a non-compete agreement – or any other post-employment agreement – remind the employee of that fact.
 - b. Provide the Employee with a copy, preferably a signed copy, of the agreement(s).
 8. Prospective Employers
 - a. Remind the employee of her/his duties, both under written agreements and, under the common law (e.g. fiduciary duties), in her/his dealings with a prospective employer.
 - b. If there is an agreement that the departing employee is to disclose certain restrictive covenants to a prospective employer, remind the employee of that obligation.
 9. Remote Wiping
 - a. If there is a carefully drafted agreement that management may remotely wipe company-issued, or even personal, devices, do not forget to do so.
 - b. You might consider in the exit process reminding the departing employee that you will be doing so, but that management is open to, under supervision, allowing the employee to transfer personal documents to an external device.
 10. Trade Secrets
 - a. Remind the departing employee not to transfer or communicate any trade secret, proprietary, or corporate confidential information to a new employer.
 - b. This prohibition should include customer lists.

11. LinkedIn

- a. Remind the departing employee to remove from her/his LinkedIn and other social media accounts any statement that they are employed by your company.
- b. If there is a social media agreement which prohibits them from “advertising” their new employment on LinkedIn as a method to circumvent the non-solicitation agreement, then remind them of any such obligations.

12. Social Media

- a. If there is a social media agreement, or even if there is not one, but there is a non-solicitation or non-compete agreement, then you should advise the departing employee that, in the company’s judgment, it would be a violation to send a post to former customers of your new work location.

13. Ownership of Social Media Accounts

- a. If an agreement regarding ownership of social media accounts is in place, remind the departing employee of its existence and her/his obligations thereunder.

14. Refusal to Participate

- a. If the departing employee refuses to participate in an exit interview, or is uncooperative during the exit interview, this may well be a red flag suggesting that you should have IT take a deeper dive into his/her computer activity in recent weeks.

15. Keys & Cards

- a. Obviously, get all office keys and swipe cards or other devices used to access the building.
- b. Retrieve identification badges
- c. Advise security/concierge that individual is not permitted on premises except under escort.
- d. These steps should be taken for all departing employees so that there can be no suggestion of defamation.

16. Personal Possessions

- a. This is an area where management ought to be respectful and sensitive to the interests and feelings of the departing employees.
- b. First, **do not** bar the departing employee from retrieving her/his possessions so long as that is done under supervision and what is removed from the premises by the departing employee is specifically approved by management.
- c. Allow the employee to do this at a time of day of her/his choosing. Avoid the scenario of a guard or the HR director escorting the employee out, carrying a cardboard box with personal possessions. It is a common, bitter complaint of departing employees that they feel they have been treated like a criminal in such circumstances. We have seen numerous such circumstances where management decides that it will gather the departing employee’s possessions and ship them to her/him. Invariably in those circumstances something is missing or damaged. The simplest and most effective solution is to bar access to the employee’s work area

until the employee can come back at an appropriate time of day, under supervision, to retrieve her/his possessions.

d. Respect ought to be the watchword here.

17. Mandatory or Voluntary Disclosures of Alleged Wrongdoing

a. Many employers now require employees to disclose/report wrongdoing, encouraging internal reporting and complaining.

b. At the exit interview, one ought to remind the employees of any such mandatory obligations to report alleged wrongdoing.

c. Even if the company does not have a mandatory reporting policy, the company should ask the departing employee to disclose any wrongdoing and any complaints that the employee might have.

d. If you hear any whisper during this process of a complaint, that discussion should be aggressively pursued and acted upon.

18. Reasons for Termination

a. Whomever is conducting the exit interview should be fully briefed on what, if any, reason(s) have been given to the departing employee for the termination.

b. If no reason has been given, then whomever is conducting the exit interview should indicate that she/he is unaware of the reason.

c. If the reason is conduct or performance, whatever is said to the departing employee should be 100% consistent with what management has already told the employee are the reasons for termination.

d. Whomever conducts the exit interview should avoid being drawn into a debate about the merits – or demerits – of the termination.

19. Alternative Dispute Resolution

a. Remind the departing employee of any alternative dispute resolution policies or agreements, mandatory or voluntary, to which she/he is subject.

b. If there is an agreement to shorten the statute of limitations, remind the departing employee of the agreement and the shortened deadline.

20. Posters

a. A number of courts have recently held that statutes of limitations under the FLSA and ADEA are tolled if the Company did not post the government-issued notices of rights required by those statutes.

b. In light of these developments, have the departing employee acknowledge that the Company had posted these notices.

II. EMPLOYEE'S CHECKLIST

1. Copies of All Agreements

1. Departing employee should obtain a fully executed, if it exists, copy of all agreements which s/he has entered into with her/his employer, including non-compete agreements, confidentiality agreements, non-disclosure agreements, etc. There may not be an agreement that is fully executed. Sometimes the employer, for a variety of

reasons (sometimes because it does not have a fully executed non-compete agreement) will seek to have the departing employee “reaffirm” the supposed non-compete agreement. Before signing, one might ask to see a copy of the supposed former fully executed agreement.

2. Shortened Statutes of Limitations

1. given the fact that many employers are having employees sign agreements shortening the statute of limitations applicable to employment-related claims, the departing employee should be certain to inquire, at exit interview, or earlier, about whether any such agreement exists. These agreements can be contained in the application for employment which the individual signed.

3. Arbitration

1. Employee should determine, before departure, whether there is any "agreement" requiring that the employee submit any claim to mandatory, binding, arbitration.

4. Many employers now have such agreements. They are sometimes stand-alone documents, sometimes in other contracts, and sometimes in employee handbooks or certain benefit documents.

5. Benefit Documents

1. The departing employee should gather all benefit plans that effect the employee, including stock option plans, restricted stock plans, the 401k, any pension plans, the STD and LTD plans, etc.

6. Employee Handbook/Manual

1. Where permissible, the employee should copy the employee handbook/manual/personnel policy(ies). For voluminous documents the employee should, at a minimum, copy all language disclaiming contractual intent and referencing at-will employment. The employee should also be certain to copy those portions of the document which relate to the employee's specific circumstances.
2. Employee, if proper, should download a copy of the employee handbook or manual in its entirety. Employee's counsel will be interested, among other things, in any disclaimers of contractual agreement and affirmations that the employee is at-will.
3. Employee's counsel will also be interested in any progressive disciplinary procedures contained in the manual.

7. Choice of Law

1. Employee should be careful to gather any document that makes a reference to what choice of law applies to controversies with the employer.

8. Choice of Forum

1. Employee should do same regarding any documents which make reference to a choice of forum where disputes with the employer must be filed.

9. Disclosure of Inappropriate Conduct

1. Employee should be careful to determine whether there is any written policy requiring that the employee disclose any wrongful conduct at the employer, including government contract fraud, inappropriate conduct (e.g. sex or race harassment).

10. Surreptitious Recording

1. While some states permit an employee to secretly record, without the consent of others, conversations with the employer, our firm discourages such conduct. Having

said that, D.C. and Virginia are so-called "one party" states whereas Maryland is a two-party consent state.

11. Company Documents

1. Employees should be extremely careful regarding document/electronically stored information which employee takes with her/him upon departure or retains upon departure.

12. Communications With Lawyer

1. In communicating with a lawyer, employee ought not to communicate using the employer's e-mail system as that can arguably constitute a waiver of attorney-client privilege.
2. In communicating with an attorney using a company device and one's own e-mail account(s) sometimes doing this at work can result in the communication being on the company's server.

13. Deletion of ESI

1. Employee should not delete any electronically stored information unless specifically instructed to do so by Company management. Otherwise, even if the deletion is 100% benign, there is the risk that the company's lawyers will make a big to-do about it, and divert attention from the real issues to peripheral issues such as spoliation, the computer fraud and abuse act, and a bevy of other causes of action which company lawyers now routinely threaten employees with.

14. Social Media

1. Employees ought not to delete social media accounts or information thereon. Social media accounts are arguably fair game in discovery for employment litigation. While your lawyer will attempt to prevent the employer from, in discovery, indiscriminately accessing your social media, spoliation of that information will be looked upon with great disfavor by the court.

15. LinkedIn

1. Employee needs to be cautious about the use of their LinkedIn profile. They should immediately delete any reference which suggests that they are still employed by their former employer and, if they have a non-compete or non-solicitation agreement with the former employer they may, in some jurisdictions, need to be careful that the language they use in LinkedIn profiles do not violate any such agreement.

16. Communications With Competitors

1. Communications with your employer's competitor while still employed can create significant problems. While one is not prohibited from entertaining offers from a competitor in all circumstances, sometimes these conversations can approach, or cross, the line between competing and preparing to compete. Caution should be the watchword.

17. Return of Company Laptop

1. A significant problem for many departing employees is the reality that either their company issued digital device or personal digital device contain not only work-related documents and information but also personal documents and information, including, sometimes, financial documents, statements, tax returns, personal family documents, medical records, and other personal documents. There can be a relatively easy methodology put in place by employer/employee to assure that employee retains all documents and information without the employer accessing same, and employer having returned to it all its work documents and information without

employee retaining a copy or access to a copy. Sadly many make a mountain out of this molehill and, quite frankly, typically in that scenario, the only winners are the lawyers and the IT professionals. In short, a lot of time and money can be wasted over what is, in a high percentile of cases, nothing.

18. Access to Company Computers

1. Do not - I repeat, do NOT - access or attempt to access the Company's computer systems after your final day, even if the company has neglected to shut down your access or if some other employee's access codes are in your possession.

19. Non-Disparagement

1. If you blog, belong to a chat group, or on a board devoted to disgruntled employees, restrain yourself. Those posts may be discoverable and may not reflect well upon you in the eyes of the judge and jury. Indeed, depending on what is said and the circumstances, they may constitute defamation, disparagement, or violation of a company confidentiality agreement.

20. Acknowledgment of Receipt

1. Oftentimes, employees are asked to sign documents during the departure process which acknowledge that they have received and read the document. In most circumstances, the employee should do so so long as the employee is provided with a copy of the complete document with their signature which simply acknowledges receipt or acknowledges that they have received and read the document. Sometimes, employees ask to acknowledge that they have read "and understood" the document. If asked to acknowledge that one understands the document, the employee should generally strike the word "understood" and initial the deletion. Of course, if the document is extremely simple, you should not irritate all concerned by doing this, but for more complex legal documents, the deletion should be made.

21. Severance Plan

22. Performance Improvement Plan ("PIP")

1. Employers are taught, even though the employee is at-will, to create a paper trail leading to the employee's termination. Employee ought not totally resist a PIP, but rather create a paper trail that the PIP does not have, and ought to have, objective measures of performance and, obviously, reasonable objective measures.

23. Time Limits: EEOC

1. Employee should be aware that there is a three-hundred (300) calendar day (or, in some instances, a one-hundred eighty (180) calendar day) time limit to file a charge with EEOC, which is a precondition to suit. Employee should complete, online, the EEOC intake questionnaire and an EEOC charge, and hand-deliver or e-mail, or overnight mail to EEOC such documents.

24. Work-Sharing Agreement

25. FOIA or Subpoena for EEOC File

26. Offer Letter

27. Employment Agreement

28. Co-Workers

29. Former Co-Workers

30. Access Codes

31. Company Website

1. Employee should insist that employer immediately remove her/his name, bio, and photo from the company's website. If the Company continues to use the employee's

photo, there may be a claim under some state laws for misappropriation of one's likeness.

32. Twitter

1. Employee should be aware that there has been a spate of litigation over ownership of Twitter accounts that the employee had used to further the company's agenda.

33. Clawback/Forfeiture

1. Employee should review all documents/agreements for clawback or forfeiture clauses. Sometimes long-term incentive benefits have such provisions, and if the employee commits acts inimical to the Employer, it may attempt to claw back or exercise a forfeiture.

34. Business Expenses

1. Employee should be certain to submit, on a timely basis following accepted procedure, any and all outstanding business expenses for reimbursement.

35. Unemployment Compensation

1. In most states, gross misconduct or willful misconduct (e.g. Virginia) will disqualify the employee from receiving unemployment compensation benefits, and simple misconduct may reduce the number of eligible weeks for the employee.
2. Employee will want an agreement from the employer that it will not oppose a claim for unemployment compensation benefits. Federal law no longer makes it quite that simple.

36. Access to Personnel File

1. Some states, by statute, require, under certain circumstances, that the employer permit the employee to have access to her/his personnel file.

37. Job References

1. Employee may be able, on departure, to secure a verbal commitment that one or more representatives of employer will provide verbal and/or written positive job references. In addition, employee would want a commitment from employer that former employees in particular are free to provide a job reference to the departing employee.

38. Job Search/Mitigation

1. Employee has a duty to mitigate her/his damages. In this day and age, it is quite easy to apply online on a daily basis for scores of jobs. Employee should maintain detailed records of all efforts made to find alternative employment. Employee should seek advice if employee decides, for example, to go back to school.

39. Confidential Documents

1. Employee ought not remove confidential documents, including any that are attorney-client privileged, or health records of others, or financial records of others, or credit card information of others. There are some cases where in-house attorneys have removed documents to use in furtherance of claims against his/her employer.

40. Finding a Lawyer

41. Filing Pro-Se

42. Ghostwriting

43. Potential Client Status/Fiduciary Duties

44. Negotiating Styles

45. OWBPA Compliance

46. Initial Instructions to Potential Client

1. Do not communicate using employer's e-mail.

2. Do not transmit documents to us without our explicit permission.
3. Client's goals.
4. Damages questionnaire.
5. Mitigation instructions.
6. Ex-parte communications.
7. The defense cease and desist letter.
8. The opening demand.
9. Inventory all digital devices.
10. Preservation of text messages.
11. Clients to avoid.
12. Indemnification.

Hiring and Firing in the Digital Age

Legal and Practical Issues

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Avenue, N.W.
Suite 230
Washington, D.C. 20009
(202) 588-5300 (phone)
(202) 588-5023 (fax)
fitzpatrick.law@verizon.net (e-mail)
<http://www.robertbfitzpatrick.com> (website)

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 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.

Choose a job you love, and you will never have to work a day in your life.

- Confucius

LOVE & MARRIAGE



Resume Screening Software

- The vast majority of large employers use specialized resume screening software, often called “Applicant Tracking Systems” (“ATs”).
- ATs generally functions by screening job applications for specific words or phrases.
- Even highly qualified candidates can experience difficulty getting past ATs.



Problems With Resume Screening Software

- Discrimination
 - While giving the appearance of impartiality, ATSs may, due to the keywords selected, have a disparate impact on applicants from one or more protected categories.
 - Employers should regularly audit the output of their ATS, and should be prepared to promptly correct any deficiencies.
- Preservation
 - Employers should preserve the input to, output of, and heuristics used by, their ATS.



Pre-Employment Notices: Employer to Employee

- Some states are adopting legislation requiring employers to provide certain notices to job applicants prior to their acceptance of a position.
- Should the employer provide notice of:
 - A mandatory non-compete agreement?
 - *Oregon*: ORS 653.295
 - *New Hampshire*: RSA 275:70
 - Massachusetts, Connecticut, and Michigan have all considered similar legislation
 - Changes to its arbitration agreement?
 - Numerous courts have held that arbitration agreements which can be changed without prior notice are illusory.
 - Contractually reduced statute of limitations?



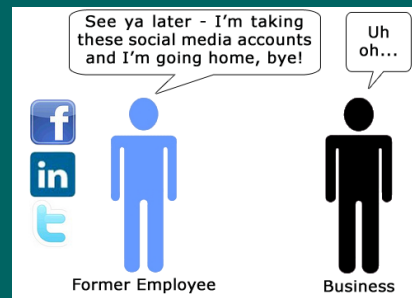
Pre-Employment Notices: Employee to Employer

- Employees should be required to disclose all continuing obligations to which they are subject:
 - Restrictive Covenants;
 - Non-disclosure agreements;
 - Intellectual property agreements;
 - Other continuing obligations.
- Employees should represent, in writing, that they will not bring documents, or use information, which contain:
 - Trade secrets;
 - Confidential or Proprietary information



Policies & Procedures

- Your onboarding process should include up-to-date policies and procedures.
- These policies should be sure to address:
 - Use of social media;
 - Ownership of employee social media accounts;
 - Use of employee-owned devices for work purposes (“Bring Your Own Device” policies)



Use of Social Media

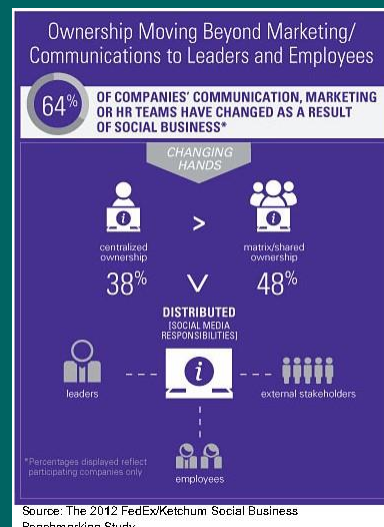
- An employer should institute guidelines governing the acceptable use of social media.
- In drafting such a policy, the employer should keep in mind the following issues:
 - Protected concerted activity under the NLRA
 - Whether, and when, post-employment use of social media constitutes prohibited competition;
 - Use of the Company's name in social media posts.



Source: Jana Hrdinova, et al., "Designing Social Media Policy for Government: Eight Essential Elements", Center for Technology in Government (May 2010)

Ownership of Social Media Accounts

- Courts are currently grappling with issues regarding ownership of social media related information.
- Employees should not generally be permitted to use personal social media accounts for business purposes
- As to Company accounts, the policy should address:
 - Ownership/return of usernames and passwords;
 - Ownership of "contacts", "followers", "links", and content.



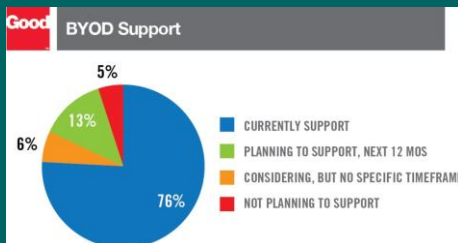
HMV – An Object Lesson



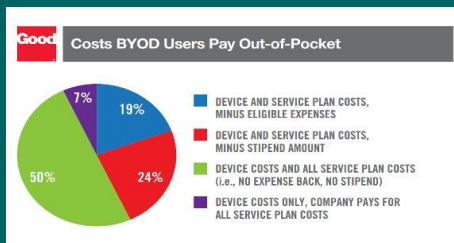
- “The lesson for any business is clear: If you’re facing an uncomfortable collision with loyal employees, lock down your social media accounts. The anonymous worker indicated in another series of tweets ... that HMV’s feeds were set up by an intern years ago and likely not secured.”
 - Jared Keller, “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>

Bring Your Own Device (“BYOD”) Policies

- Allowing employees to use their own devices for work is rapidly growing in popularity, due in part to the potential cost-savings it offers.



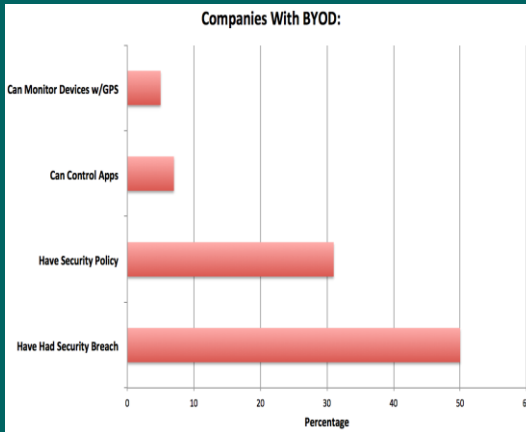
Good Technology, 2012 BYOD Data Report



Good Technology, 2012 BYOD Data Report

Many Employers are Unprepared

- This trend brings with it both legal complications and security concerns which many organizations are poorly equipped to handle.



Zenprise 2012 Security Survey

- Companies ignore security risks at their peril

Data breaches continue to have serious financial consequences

Average organizational cost per data breach

\$5.5 million

Cost per compromised record

\$194

BYOD Policies – Security

- A BYOD policy should require the employee to work with the employer to mitigate the security risks.
- Software:
 - Mobile Device Management Software
 - Anti-Virus Software
 - Full device encryption;
 - Strong passwords.
- Dangerous Apps
- High-Risk Device Permissions
- Require training!**

Top 5 enterprise mobile security concerns

- Device loss
- Application security
- Device data leakage
- Malware attacks
- Device theft

*Respondents asked to choose up to five concerns; ranking is based on a weighted calculation.

SearchSecurity.com Mobile Security Survey (2012)

BYOD Policies – Legal Challenges

Preservation

Employers must be able to search, preserve, and produce information on employee devices, including:

1. Text Messages
2. E-mail
3. Downloads
4. Browser history

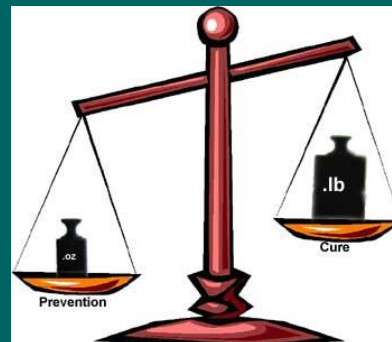
Improper Use

Employers must guard against misuse of devices by employees, including:

1. Trade Secrets laws;
2. The Computer Fraud and Abuse Act;
3. Restrictive Covenants;
4. Common law duties.

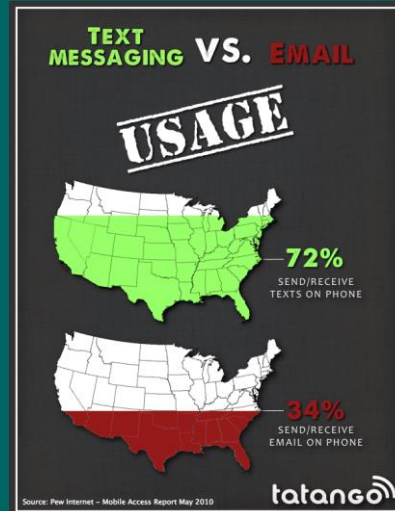
Prepare to Preserve

- The employer should maintain an up-to-date list of document repositories for key employees:
 - Company devices;
 - Employee owned devices;
 - Company server(s);
 - Portable storage media (flash drives, external hard drives, etc.)
- The employer should put in place processes governing how such data will be maintained, deleted, and preserved.



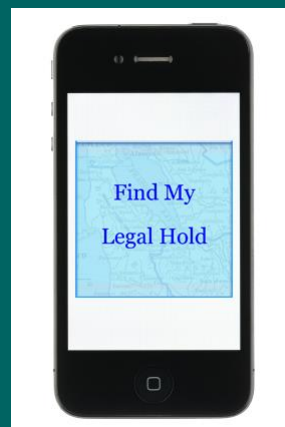
Preservation of Text Messages & Chats

- E-mail is being replaced by text messaging and online “chats” as the most frequently used form of electronic communication
- Preservation is complicated by the presence of multiple devices, programs/apps, and formats



Preservation of Text Messages & Chats: How-To

- Screenshots:
 - Pros: Inexpensive, no special training needed
 - Cons: unwieldy for long exchanges, loss of metadata, does not guard against later deletion
- Backup/Export Utilities:
 - Pros: relatively inexpensive, easier for large-scale preservation, preserves some metadata
 - Cons: may require training
- Forensic Imaging:
 - Pros: generates forensically verifiable copy, preserves all data, increases ease of search for large reviews
 - Cons: expensive, requires further processing for use



Marriage is the chief cause of divorce.
- Groucho Marx

SEPARATION & DIVORCE



Monitoring Device Usage

- The employer should clearly communicate that all electronic device usage may be monitored.
- The employer need not monitor day-to-day usage, but should begin monitoring in advance of termination, or if “red flags” are raised.
- Monitoring software should be installed on all employer devices and any devices subject to the employer’s BYOD policy.
- Don’t forget the photocopier!



Stored Communications Act

- Accessing private employee data in the cloud risks violating the Stored Communications Act.
- Activities which violate the SCA include:
 - Employer reviewing private Facebook posts
 - *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, No. 2:11-cv-03305, 2013 U.S. Dist. LEXIS 117689, 2013 WL 4436539 (D.N.J. Aug. 20, 2013)
 - Employer reviewing contents of private e-mail account linked to employer provided device
 - *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748 (N.D. Ohio 2013)



SCA – Scope & Disclosure

- An entity which holds an electronic communication can provide that information if there is “lawful consent”
- Who can consent to disclosure of a communication?
 - The originator
 - The addressee
 - The intended recipient
 - The account holder (sometimes)
- The application of the SCA is not straightforward, and is complicated by its use of badly outdated terminology.
- Obtaining consent is made complicated by the growing number of states which have passed legislation prohibiting the employer from requiring employees to provide access to these accounts.

The SCA was written for computers like this:



It is applied to computers like this:



SCA – Penalties

- Violating the Stored Communications Act carries potentially severe penalties, including:
 - Imprisonment of up to five years for a first offense;
 - Criminal fines of up to \$500,000.00 for organizations for malicious, mercenary, tortious, and/or criminal violations;
 - Damages equal to the total of the offender's profits and victim's losses; and
 - Reasonable attorneys' fees.



Job References

- Many employers have committed, either by standard policy or by contract, to providing a neutral reference.
- Nevertheless, employers should consider whether they have a duty to disclose certain facts.
- For example, was the employee:
 - Violent in the workplace?
 - A harasser?
 - A bully?
 - Terminated or accused of inappropriate or illegal conduct (e.g. fraud, child pornography)

Do you give references more like this:



Or like this:



Be Afraid: Texts, E-mails, and Privilege Waiver

- Courts are split on whether use of employer-provided devices waives privilege:
 - The Fourth Circuit, in *United States v. Hamilton*, 701 F.3d 404 (4th Cir. 2012), found the marital privilege waived.
 - The New Jersey Supreme Court, in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010) found the attorney-client privilege had not been waived.
- Justice Sotomayor, in *United States v. Jones*, 132 S. Ct. 945 (2012) opined that:
 - [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties [because] [t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.



Limit Access: Ensure the Secrecy of Confidential Information



- Uniform Trade Secrets Act:
 - Information is not generally known; and
 - “is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.”

Limit Access: Ensure the Secrecy of Confidential Information

- To enforce, secrets must be identified with “reasonable particularity”
- Bottom line: make good use of passwords and policies to prohibit employee access to files without authorization

Limit Access: Limit Authorization to Access Important Company Information

- The Computer Fraud & Abuse Act (“CFAA”)
 - Accessing a computer without authorization
 - Exceeding authorized access
 - Requires a showing of damage or loss

Limit Access: Limit Authorization to Access Important Company Information

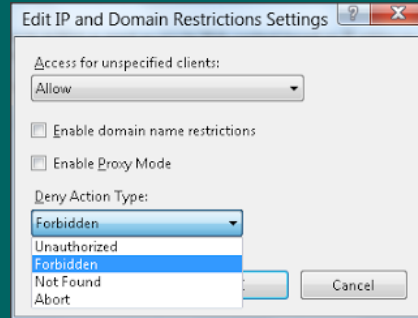
- Fourth and Ninth Circuits have a narrow definition of “unauthorized access”.
 - *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012)
 - *WEC Carolina Energy Solutions, LLC v. Miller et al.*, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S.Ct. 831 (2013)

Limit Access: Limit Authorization to Access Important Company Information

- The First and Third Circuits have a broad definition of “unauthorized access”:
 - *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001)
 - *U.S. v. Tolliver*, 451 Fed. Appx. 97 (3d Cir. 2011)

Technological Solutions

- To protect truly sensitive hardware and information, the Company should institute software based restrictions on access.
- This is especially true given the circuit split.
- All courts agree that circumventing a “code based restriction” constitutes unauthorized access.
- These can include:
 - Requiring passwords
 - Installing software which alerts the Company to the use of flash drives on its network;
 - Installing software which prohibits high-risk operations (e.g. large volume downloads, remote access)



Managing Termination



Think Through Termination

- The manner and justification provided for a termination decision should be thoroughly discussed and vetted.
- The manner and justification for termination can impact numerous legal issues, including:
 - Discrimination claims;
 - Unemployment compensation;
 - Contractual Rights:
 - Stock Options;
 - Enforceability of Restrictive Covenants.
 - Wrongful termination/Public Policy Tort.
- Remember: Once you give a reason, you are stuck with it.



Termination Checklist

- Disable access to digital systems, devices, & accounts
- Retrieve access cards, keys, and badges
- Advise security that the employee is not to be permitted on the premises
- Make sure you have ***signed*** copies of all pertinent agreements

Termination Checklist

- Secure the employee's laptop, desktop, and Company-issued devices
- Secure the employee's office/cubicle
- Arrange for the employee to remove personal possessions, under careful supervision, with as little embarrassment as possible



Telegraph Media, 2013

Exit Interview

- Incentivize departing employees to participate in exit interviews – provide consideration
- Have a well thought out checklist:
 - Return of documents
 - Return of other property
 - Discuss employee's continuing obligations
 - Retrieval of employee's property from his/her office

Exit Interview

- Remind employees of key obligations:
 - Statutory (CFAA, Trade Secrets)
 - Contractual (Restrictive Covenants, Non-Disparagement, Confidentiality)
 - Common Law (Fiduciary Duties)
 - Consequences (Clawback)

Communications Regarding Continuing Obligations

- Remind supervisors not to defame the employee or violate any contractual obligations they may have (e.g. non-disparagement)
- Prematurely or inappropriately contacting a former employee's current or potential employer can give rise to liability, including:
 - Defamation;
 - Tortious Interference;
 - False Light;
 - Breach of Contract;
 - Retaliation.



Exit Interview

- Involve an IT professional in planning and executing this meeting
- If the exit interview or employee behavior evinces “red flags”, consider preemptively conducting a forensic examination of the employee’s electronic device(s)

Severance Agreements

- Provide fresh consideration for any new obligations;
- Consider the necessity of controversial provisions;
 - Restrictive Covenants;
 - No rehire (“do not darken my doorstep”) clauses;
 - Liquidated damages;
 - Fee shifting.
- Consider Including:
 - Return of documents/property;
 - Non-disparagement;
 - Confidentiality.
- Choice of Law **AND FORUM** are *crucial* to any agreement.



Create Document Return Policies

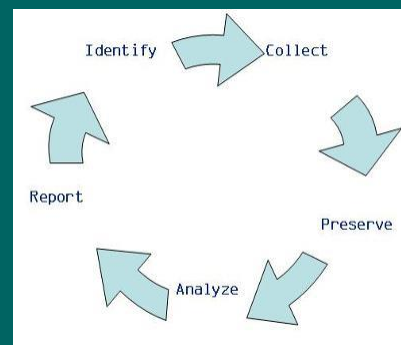
- Specify the return of both hard and soft copies
- Address the “Three Cs”
 - Co-mingling (of personal/work docs);
 - Compliance (verifying)
 - Cost
- Have a standard protocol



Courtesy: manotaw.blogspot.com

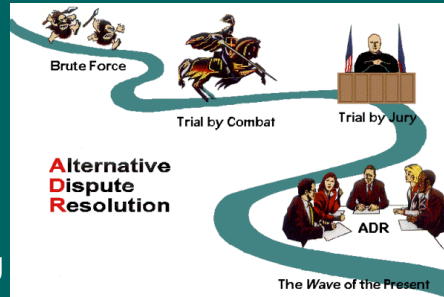
Information Technology

- Image computer before wiping, especially if there are red flags
- Quickly see what has been recently downloaded.
- If photos of the employee on the company website or other advertising products, digital or hard copy, take them down before you get a virginia you stole my likeness case



ADR Agreements

- Be familiar with any ADR agreements and procedures
- Common ADR Steps:
 - Notice of claim
 - Informal steps
 - Mediation
 - arbitration
- Know the deadlines
- Be aware of any cost-shifting
 - Fee shifting provisions?
 - Company required to pay?
- Provisions which (are likely to) apply only against the employee are a **red flag**.



Wage, Hour, and Leave

- Ensure you have processes in place to scrupulously comply with federal, state, and local wage, hour, and leave laws.
- Some states/localities require payment of accrued but unused leave
- Most state wage and hour laws have strict requirements regarding distribution of an employee's final paycheck.
- Penalties for violations can be severe relative to the consequences of the violation.



Computer Fraud and Abuse Act: Current Developments

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave., N.W.
Suite 230
Washington, D.C. 20009
(202) 588-5300
(202) 588-5023 (fax)
fitzpatrick.law@verizon.net

<http://www.robertbfitzpatrick.com> (website)
<http://robertbfitzpatrick.blogspot.com> (blog)

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 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.

COMPUTER FRAUD AND ABUSE ACT:

Current Developments

by Robert B. Fitzpatrick, Esq.*

I. Introduction

Originally designed as a criminal statute aimed at deterring and punishing hackers, particularly those who attack computers used for compelling federal interests (e.g., computers used by the federal government, large financial institutions, etc.), the Computer Fraud and Abuse Act (CFAA), “has been expanded through various amendments since its enactment in 1984.” *Int’l Airport Centers L.L.C. v. Citrin*, 2005 U.S. Dist. LEXIS 3905 (N.D. Ill. 2005), *rev’d on other grounds*, 2006 U.S. App. LEXIS 5772 (7th Cir. 2006). For example, in 1994 the Act began to allow for civil liability for certain types of violations. As amended in September 2008, the Act establishes civil liability for anyone who, among other things, “intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage...” involving “loss to 1 or more persons during any 1-year period... aggregating at least \$5,000 in value.” 18 U.S.C. § 1030(g) (incorporating 18 U.S.C. § 1030 (a)(5)(B) & (c)(4)(A)(i)(I)).

In recent years, employers have increasingly been using the CFAA to sue employees and former employees who make wrongful use of the employer’s computer systems or electronic devices, such as retaining, wrongfully accessing, or copying the employer’s computer systems or electronic documents without proper authorization. Such use of the CFAA in the employment context has been made possible in part by the broad definition of “protected computer” under the Act, which explicitly includes any computer “which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States...” 18 U.S.C. § 1030(e)(2)(B). At the time this language was originally adopted, relatively few computers fit within this statutory definition of “protected computer”, as internet connectivity was much more primitive and less commonly used than it is today. But, given the current state of technology and the courts’ expansive definition of “interstate or foreign commerce”, it is hard to conceive of an internet - connected employer-owned computer or other device which could not arguably be considered a “protected computer”.

However, as the CFAA is primarily a criminal statute, courts have held that its language should be narrowly construed in the context of civil liability. *See, e.g., Int’l Ass’n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 499 (D. Md. 2005). Thus, understanding the language of the Act and its construction by courts is of paramount importance for any party contemplating bringing a civil suit under the Act.

*This article was prepared with assistance by Ryan P. Chapline, an associate with Robert B. Fitzpatrick, PLLC. Mr. Chapline is a May 2009 graduate of George Mason University School of Law and a member of the Maryland State Bar.

II. Scope of Employee Authorization to Access Employer's Computerized Information

Since civil liability under the CFAA hinges in part upon whether the defendant accessed the protected computer in question with or without “authorization”, the scope of an employee’s or a former employee’s authorization to access his current or former work computer is often a topic of contention in employment cases brought under the Act. According to the Act, “the term ‘exceeds authorized access’ means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter...” 18 U.S.C. § 1030(e)(6). Along those lines, a circuit split has recently developed on the topic of whether the Act should be interpreted broadly or narrowly when an employer claims that an employee or former employee has acted “without authorization” or has “exceeded authorization” in accessing the employer’s computer-stored information.

The narrower and more employee-friendly view, which has garnered significant support, is illustrated by the 9th Circuit’s holding in *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), where the Court rejected the employer’s argument that an employee accesses electronic documents without “authorization” when the employee acts contrary to the employer’s interest or in breach of the employee’s fiduciary obligation of loyalty to the employer. Rather, where the employee’s actions are consistent with the access previously granted to him as an employee, the Court held that the employee acts with proper “authorization” within the meaning of the Act, regardless of whether the employee breached his or her duty of loyalty to the employer. For other decisions adopting this view, see, e.g., *Clarity Servs. v. Barney*, 2010 U.S. Dist. LEXIS 32519 (M.D. Fla. 2010); *Bell Aero. Servs. v. U.S. Aero Servs.*, 2010 U.S. Dist. LEXIS 19876 (M.D. Ala. 2010); *Bridal Expo, Inc. v. Van Florestein*, 2009 U.S. Dist. Lexis 7388 (S.D. Tex. 2009); *Lasco Foods, Inc. v. Hall & Shaw Sales, Marketing, and Consulting LLC*, 600 F. Supp. 2d 1045 (E.D. Mo. 2009); *U.S. Bioservices Corp. v. Lugo*, 595 F. Supp. 2d 1189 (D. Kan. 2009); *Condux International, Inc. v. Haugum*, 2008 U.S. Dist. LEXIS 100949 (D. Minn. 2008); *Black & Decker, Inc. v. Smith*, 568 F. Supp. 2d 929, 934-37 (W.D. Tenn. 2008); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008); *Diamond Power Int’l v. Davidson*, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007); *Brett Senior & Assocs., P.C. v. Fitzgerald*, 2007 U.S. Dist. LEXIS 50833 (E.D. Pa. 2007); *B&B Microscopes v. Armogida*, 532 F. Supp. 2d 744 (W.D. Pa. 2007); *Lockheed Martin Corp. v. Speed*, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. 2006); *International Ass’n of Machinists & Aerospace Workers v. Werner-Masuda*, 390 F. Supp. 2d 479 (D. Md. 2005).

The broader and more employer-friendly view, which has proven thus far to be the minority view, is illustrated by the 7th Circuit’s decision in *Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), where the Court held that an employee can be found to have accessed a computer “without authorization” whenever he does so in breach of his duty of loyalty to the company. For other decisions adopting this view, see, e.g., *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2007); *Guest-Tek Interactive Entm’t Inc. v. Pullen*, 665 F. Supp. 2d 42 (D. Mass. 2009); *Ervin & Smith Advertising & Pub. Relations, Inc. v. Ervin*, 2009 U.S. Dist. LEXIS 8096 (D. Neb. 2009); *Nilfisk-Advance, Inc. v. Mitchell*, 2006 U.S. Dist. LEXIS 21993 (W.D. Ark. 2006).

For a number of cases decided before this circuit split arose on the scope of “access” and “authorization” under the Act, see *United States v. Phillips*, 477 F.3d 215; 2007 U.S. App. LEXIS 1632 (5th Cir. 2007) (A user's authorization to access a protected computer is based on the expected norms of intended use or the nature of the relationship established between the computer owner and the user); *Expert Business Systems, LLC v. BI4CE, Inc. d/b/a Business Intelligence Forces*, 233 Fed. Appx. 251; 2007 U.S. App. LEXIS 11002 (4th Cir. 2007) (upholding the district court's ruling that an employer had failed to present sufficient evidence to support its claims under the CFAA, which centered in part on whether the defendants had remotely accessed the employer's computers without authorization); *Triad Consultants Inc. v. Wiggins*, 249 Fed. Appx. 38; 2007 U.S. App. LEXIS 22226 (10th Cir. 2007) (upholding district court's dismissal of corporation's claims under the CFAA, in part because the corporation alleged no facts showing that former employee / defendant accessed the information in question); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) (upholding district court's award of preliminary injunction to plaintiff, because plaintiff showed it would likely succeed on the merits of its CFAA claim, which turned largely in part on whether the defendant had “exceeded authorized access” to the plaintiff's website); *Worldspan, L.P. v. Orbitz, LLC*, 2006 U.S. Dist. LEXIS 26153 (N.D. Ill. Apr. 19, 2006) (“Moreover, it is clear from the language of the CFAA that accessing a computer ‘without authorization’ does not include ‘exceed[ing] authorized access.’ Because Worldspan has not adequately alleged that Orbitz accessed its computers “without authorization,” Count I must be dismissed”); *SecureInfo Corp. v. Telos Corp.*, 387 F. Supp. 2d 593, 209; 2005 U.S. Dist. LEXIS 21228 (E.D. Va. Sept. 9, 2005) (“Furthermore, Plaintiff's Amended Complaint does not allege facts that the defendants “exceeded authorized access” within the meaning of the statute. Mr. Berman gave the CFAA defendants access to BAI's server and to the information on the server; consequently, the CFAA defendants were “entitled to obtain” information on the server because Mr. Berman explicitly allowed them access to it. See § 1030(e)(6). Even if Mr. Berman allowed the defendants access to the BAI server and SecureInfo's materials in violation of the license agreements, under his grant of authority to the defendants, they were entitled to obtain the information on the server”) (Corporation's wholesale use of the tour company's travel codes to facilitate gathering tour company's prices from its website was abuse of proprietary information that went beyond any authorized use of appellee's website); *Business Information Systems v. Professional Governmental Research*, 2003 U.S. Dist. LEXIS 27363 (W.D. Va. Dec. 16, 2003) (“Progress's actions did not result in impairment of the availability of data, a program, a system, or information because it did not shut down BIS's server. In addition, Progress's actions did not result in an impairment to the integrity of the system because Progress's program utilized Snyder's username and password to access BIS's system on behalf of others. It was the same as if Snyder had communicated his username and password to the remote user and told him or her that they were free to use it; Progress's program just automated this process. As a result, there is no violation of the Computer Fraud and Abuse Act”); *Four Seasons Hotel & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 2003 U.S. Dist. LEXIS 8717 (S.D. Fla. May 9, 2003) (e-mail messages are considered to access every computer they pass through on their way to their intended recipients); *In re America Online, Inc. Version 5.0 Software Litigation*, 168 F.Supp.2d 1359, 1370-71 (S.D. Fla. 2001) (Citing legislative history of subsections 1030(a)(5)(B) and (C) for the proposition that these provisions “are intended to apply to outsiders who access a computer,” not to “insiders” who access individuals' computers with their

permission to do so); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (Use of search robots to harvest information from Plaintiff's database is "access" under the CFAA).

III. Proving Loss / Damage

As noted above, in order for civil liability to attach under the Act, the employer has the burden to show that the employee's unauthorized access "recklessly cause[d] damage..." involving "loss to 1 or more persons during any 1-year period... aggregating at least \$5,000 in value." 18 U.S.C. § 1030(g) (incorporating 18 U.S.C. § 1030 (a)(5)(B) & (c)(4)(A)(i)(I)). The Act specifically defines "loss" to mean "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service..."; and defines "damage" to mean "any impairment to the integrity or availability of data, a program, a system, or information..." 18 U.S.C. § 1030(e)(8) & (11).

A number of courts have strictly construed this damage/loss prerequisite and the Act's definition of cognizable "loss", and have granted summary judgment for defendant employees sued under the Act where the employer fails to introduce sufficient evidence to show \$5,000 in aggregate losses as defined under the Act. *See, e.g., Global Policy Partners, LLC v. Yessin*, 2010 U.S. Dist. LEXIS 14838 at *11 (E.D. Va. February 18, 2010) (holding that plaintiffs in CFAA cases "must show that the losses they claim were the reasonably foreseeable result of the alleged CFAA violations, and that any costs incurred as a result of the measures undertaken to restore and resecure the [computer] system were reasonably necessary in the circumstances") (*citing A.V. ex rel. Vanderhye v. iParadigms, LLC*, 562 F.3d 630, 646 (4th Cir. 2009)); *B.U.S.A. Corp. v. Ecogloves, Inc.*, 2009 U.S. Dist. LEXIS 89035 (S.D.N.Y. Sept. 28, 2009) (dismissing plaintiffs' CFAA claim, in part for failing "to marshal admissible evidence that would show that they have met the jurisdictional threshold for damages under the CFAA").

In *Global Policy Partners*, it was largely undisputed that the defendant had broken into the plaintiff's computer system and read the plaintiff's emails without authority. The "loss" claimed by the plaintiff consisted of (i) nearly \$6,500 paid to a web designer and to ISPs "in order to register, configure, and design new web sites and e-mail accounts"; (ii) \$27,500 in the plaintiff's lost billable time spent investigating and responding to the offense; and (iii) "millions of dollars" in lost revenue from failing to win a project that was the subject of the emails in question. While the court conceded that many of these claimed losses were arguably spent in "responding to and addressing an offense and costs of restoring the system to its condition prior to the offense", the court held that the damages were nevertheless not recoverable under the Act because, *inter alia*, the plaintiff failed to show that the expenditures "were a reasonably necessary response to the alleged CFAA violations". As stated by Lee E. Berlik in a blog post written about this opinion, *Proving Loss Under the Computer Fraud and Abuse Act*, Virginia Business Litigation Lawyer Blog (May 24, 2010), the decision stands for the proposition that losses from a violation of the Act are not necessarily recoverable "simply because money was spent subsequent to the violations"; and even where a violation occurs, "that would not give the plaintiff a blank check to

perform system updates that were not reasonably necessary to restore and re-secure the system”. The blog post can be accessed here:

http://www.virginiabusinesslitigationlawyer.com/2010/05/proving-loss-under-the-compute.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Virginia+Business+Litigation+Lawyer+Blog%29.

Some courts have further limited the scope of cognizable losses under the Act by holding that the Act permits recovery of lost revenue only where the violation of the statute leads to an “interruption in service” and/or some type of inoperability of the computer systems in question. See, e.g., *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 Fed. Appx. 559 (2nd Cir. 2006) (affirming dismissal of a CFAA case, holding that plaintiff failed to establish the requisite amount of loss required under the Act, partially due to the fact that while plaintiff company incurred lost profits from violation of the Act, it did not suffer an interruption in service); *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760 (N.D. Ill. 2009) (holding that the Act’s definition of damage is limited to impairment of integrity or availability of data and information, as the plain language of the statutory definition referred to situations in which data was lost or impaired because, for example, it was erased or because defendant had physically destroyed the computer equipment); *Civic Center Motors, Ltd. v. Mason Street Import Cars, Ltd.*, 387 F. Supp. 2d 378 (S.D.N.Y. 2005) (holding that because lost profits resulting from defendant’s unauthorized access did not result from computer impairment or damage, they were not compensable losses under the CFAA).

For other cases along these same lines, see also *SKF USA, Inc. v. Bjerkness*, 636 F. Supp. 2d 696 (N.D. Ill. 2009) (employer failed to state claim under the CFAA against former employees because the employer did not plead that it suffered any costs related to its computers or that it suffered any service interruptions); *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int’l Inc.*, 616 F. Supp. 2d 805 (N.D. Ill. 2009) (former employee who e-mailed customer files to herself when she left her employer was entitled to summary judgment dismissing former employer’s claim alleging violation of the CFAA because the employer suffered no damage or loss to its data, computers, or network from this conduct); *A.V. v. iParadigms*, 544 F. Supp. 2d 473 (E.D. Va. 2008) (granting summary judgment to defendant in CFAA claim, partly due to the fact that the plaintiff failed to produce any evidence of actual or economic damages resulting from the defendant’s alleged violation of the Act); *Chas. S. Winner, Inc. v. Polistina*, 2007 U.S. Dist. LEXIS 40741 (D.N.J. 2007) (dismissing for lack of federal subject matter jurisdiction because the plaintiffs failed to allege facts that show that they suffered they suffered a “loss” as defined under the Act); *L-3 Communications Westwood Corp v. Joseph Emile Robichaux, Jr. et al*, 2007 U.S. Dist. LEXIS 16789 (E.D. La. Mar. 8, 2007) (“Because L-3 has not asserted that there was damage to their computers or an interruption of service, it has not alleged a cognizable loss under the CFAA. Accordingly, L-3 has not demonstrated a likelihood of success on the merits of the CFAA claim.”); *Spangler, Jennings & Dougherty, P.C. v. Mysliwy*, 2006 U.S. Dist. LEXIS 39602 (N.D. Ind. 2006) (denying plaintiff’s motion for summary judgment on its claim under the Act, because the plaintiff failed to provide any proof that it had been damaged by the defendant’s alleged violation of the Act); *Worldspan, L.P. v. Orbitz, LLC.*, 2006 U.S. Dist. LEXIS 26153 (N.D. Ill. Apr. 19, 2006) (“Worldspan’s failure to adequately allege damage is an alternative ground for dismissal of the complaint. We need not reach Orbitz’s remaining argument.”); *Resdev, LLC v. Lot Builders Assoc., Inc.*, 2005 U.S. Dist. LEXIS 19099 (M.D. Fla.

Aug. 10, 2005) (Revenues from a trade secret were, in this case, neither a "but-for" nor a proximate consequence of "damage" and also did not fit within the grouping of "loss" in the CFAA.); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382; 2005 U.S. Dist. LEXIS 19941 (S.D.N.Y. Sep. 6, 2005) (case dismissed because Plaintiffs failed to plead losses resulting from data corruption, the cost of responding to and repairing the computer problems, and exposure to liability to customers for breach of privacy in their complaint which resulted in a failure to state proper grounds for relief under the CFAA); *Nexans v. Sark-S.A.*, 319 F. Supp. 2d 468; 2004 U.S. Dist. LEXIS 9712 (S.D.N.Y., May 27, 2004) ("Under the Computer Fraud and Abuse Act, 18 U.S.C.S. § 1030, the meaning of 'loss,' both before and after the term was defined by statute, has consistently meant a cost of investigating or remedying damage to a computer, or a cost incurred because the computer's service was interrupted."); "The 'revenue lost' which constitutes 'loss' under 18 U.S.C.S. § 1030(e)(11) appears from the plain language of the statute to be revenue lost because of an interruption of service. Revenue lost because the information was used by a defendant to unfairly compete after extraction from a computer does not appear to be the type of 'loss' contemplated by the Computer Fraud and Abuse Act, 18 U.S.C.S. § 1030."); *Pearl Invs. LLC v. Standard I/O, Inc.*, 257 F. Supp. 2d 326, 2003 U.S. Dist. LEXIS 6890 (D. Me. 2003) (magistrate judge recommends that defendants be granted summary judgment as to plaintiff's claim under the Act, as the plaintiff showed no cognizable evidence that defendant's alleged conduct damaged plaintiff's computer system in any quantifiable amount); *Tyco Int'l Inc. v. Does*, 2003 U.S. Dist. LEXIS 11800 (S.D.N.Y. 2003) (discussing compensatory damages under the Act for plaintiff's costs associated with assessing the damage to its computer system and restoring its system after plaintiff's attack); *Motorola Credit Corp. v. Uzan*, 2002 U.S. Dist. LEXIS 19632 (S.D.N.Y., Oct. 16, 2002) ("With regard to plaintiffs' "computer hacking" claims... Defendants properly note that plaintiffs' complaint fails to allege the requisite \$ 5,000 in damages required to maintain a civil action under § 1030(a)(5)(B)(i) and, accordingly, this claim must be dismissed, without prejudice."); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 524-25 (S.D.N.Y. 2001) (recognizing only costs in remedying damage as recoverable under CFAA).

Thus, in bringing a claim against an employee or former employee under the CFAA, an employer must be careful to ensure that the it has incurred, within the span of no more than one year, at least \$5,000 in losses which would qualify as losses as defined under both the Act itself and case law in the relevant jurisdiction construing such claimed losses. Along those same lines, counsel for employees sued under the Act should always consider the propriety of filing a motion to dismiss or summary judgment motion, challenging the adequacy of the employer's claim for CFAA losses.

IV. Potential Supplement to Trade Secret and Non-Compete Claims

One common context in which CFAA claims arise in the employment context is where an employer is suing an employee or former employee for unlawful use of company trade secrets or for violation of a non-compete clause, because such claims often involve allegations that the employee has made an unauthorized use of electronic data such as customer lists, proprietary company information, and the like. Furthermore, adding a CFAA claim in such cases may be attractive to an employer for a number of reasons. For one thing, where a departing employee is

actively interfering with or damaging the employer's business by the unauthorized use of electronic data, particularly where that data has been altered or damaged, "loss" arising from a CFAA violation may be somewhat easier for the employer to establish. See, e.g., *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (The CFAA is designed to encompass situations where Plaintiff's employees, while still working for plaintiff, used plaintiff's computers to send trade secrets to defendant via e-mail). Also, bringing a CFAA claim may give the employer the option of bringing its claims in federal court, in a case where federal jurisdiction may have otherwise been unavailable, due to lack of diversity between the parties and claims which otherwise would have been entirely governed by state law (such as a claim under a contractual non-compete clause).

On the other hand, a number of courts have questioned whether improper use of trade secrets or violation of a non-compete clause constitute the type of "loss" or "damage" contemplated by the CFAA. See, e.g., *Motorola, Inc. v. Lemko Corp.*, 609 F. Supp. 2d 760 (N.D. Ill. 2009) (claims for dissemination of trade secrets and confidential information to competitor were not covered by CFAA's definition of damage; rather, damage under the Act was limited to impairment of integrity or availability of data and information, as plain language of statutory definition referred to situations in which data was lost or impaired because, for example, it was erased or because defendant had physically destroyed the computer equipment); *SKF USA, Inc. v. Bjerckness*, 636 F. Supp. 2d 696 (N.D. Ill. 2009) (employer failed to state claim under the CFAA against former employees who allegedly transferred confidential information from their work computers to storage devices and took information with them when they went to work for a competitor, because the employer did not plead that it suffered any costs related to its computers or that it suffered any service interruptions); *Garelli Wong v. Nichols*, 2008 U.S. Dist. Lexis 3288 (N.D. Ill. Jan. 16, 2008) ("Though Garelli Wong would like us to believe that recent amendments to the CFAA are intended to expand the use of the CFAA to cases where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show "impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Therefore, we conclude that Garelli Wong has failed to sufficiently plead damage under the CFAA."); *Am. Family Mut. Ins. Co. v. Rickman*, 554 F. Supp. 2d 766 (N.D. Ohio 2008) (granting motion to dismiss CFAA claim because CFAA was not meant to cover disloyal employee who walked off with confidential information; rather the CFAA punished trespassers and hackers; the employer had not alleged the type of loss that came within the scope of the Act); *Lockheed Martin v Kevin Speed*, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006) (taking of trade secrets does not, by itself, fit within the grouping of "damage" or "loss"); *Civic Ctr. Motors, Ltd. v. Mason St. Imp. Cars, Ltd.*, 387 F. Supp. 2d 378, 382; 2005 U.S. Dist. LEXIS 19941 (S.D.N.Y. Sep. 6, 2005) ("In the instant case, Plaintiffs are seeking compensation for lost profits resulting from Defendant's unfair competitive edge and for their now wasted investment in the development and compilation of the database information. However, neither of these kinds of losses are the result of computer impairment or computer damage. Therefore, they are not compensable "losses" under the CFAA.").

For more information on CFAA claims in the context of trade secret cases, see Peter J. Toren, *CFAA Can Protect Trade Secrets*, New York Law Journal (May 24, 2010), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458635753>.

V. Upshot / Takeaway

Counsel on both sides of the employment relationship would do well to keep several things in mind when working on matters that may potentially involve liability under the CFAA. For example:

- Attorneys counseling recently terminated employees, or employees who are for any other reason departing their employer, should take care to ensure that the client does not take any actions which may potentially lead to a claim being brought against the client under the CFAA. For instance, the client should be closely advised about the dangers of erasing valuable computer files, copying or printing files which they do not have authorization to take with them, accessing email accounts or databases which they do not have the right to view, viewing or copying sensitive proprietary information such as trade secrets or customer lists, sabotaging the employer's computer equipment or systems, etc.
- Counsel for employers should consider their client's rights to bring a civil action under the CFAA when an employee or departing employee has accessed, used, copied, printed, or deleted computer files without authorization. Such claims should particularly be considered in trade secret or non-compete claims brought against employees or former employees, and/or as potential counterclaims where such employees have sued the employer – for example, in a lawsuit challenging the circumstances surrounding the employee's termination.
- One must also always keep in mind the employer's burden to show the requisite amount of "loss" as defined under the Act. Unauthorized access of company computers or systems may not be actionable under the Act where the access was innocuous or largely harmless from an economic perspective, where the loss was not reasonably incurred in response to the unauthorized access, or where the access did not cause the computers or systems to be inoperable or out of service for any significant amount of time.

VI. More Resources

For more information on CFAA claims brought in the employment context and related topics, see the following sources (keeping in mind that the most recent amendments to the CFAA went into effect in September 2008, making any articles before that date potentially outdated):

- Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561 (2010), http://www.minnesotalawreview.org/sites/default/files/Kerr_MLR_0.pdf.
- Peter J. Toren, *CFAA Can Protect Trade Secrets*, New York Law Journal (May 24, 2010), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458635753>.

- Jon Hyman, *Do You Know? 12% of Employees Knowingly Violate IT Policies*, Ohio Employer's Law Blog (March 16, 2010), <http://ohioemploymentlaw.blogspot.com/search?q=12%25+IT&x=0&y=0>.
- Dale C. Campbell and David Muradyan, *The Seventh and Ninth Circuits Split on What Constitutes "Without Authorization" Within the Meaning of the Computer Fraud and Abuse Act*, The IP Law Blog (February 19, 2010), <http://www.theiplawblog.com/archives/-webtech-the-seventh-and-ninth-circuits-split-on-what-constitutes-without-authorization-within-the-meaning-of-the-computer-fraud-and-abuse-act.html>.
- David Johnson, *Update on CFAA Circuit Split: District Courts in 8th Circuit Adopt Minority View, Permitting Claims Where Defendant Exceeds His Authority to Access Computer*, Digital Media Lawyer Blog (November 16, 2009), http://www.digitalmedialawyerblog.com/2009/11/update_on_cfaa_circuit_split_d.html.
- David Conforto, *Employees Beware: Computer Fraud & Abuse May Restrict Ability to Retain Documents*, Boston Employment Lawyer Blog (November 5, 2009), http://www.bostonemploymentlawyerblog.com/2009/11/computer_fraud_and_abuse_act_b.html.
- Amy E. Bivins, *Attorneys Advise Employers to Revisit Data Misuse Policies After Brekka Ruling*, Bureau of National Affairs Daily Labor Report (November 4, 2009), <http://www.tradesecretslaw.com/uploads/file/110409%20DailyLaborReport.pdf>.
- Kenneth J. Vanko, *Two Views of the Computer Fraud and Abuse Act (Brekka and Pullen)*, Legal Developments in Non-Competition Agreements (October 30, 2009), <http://www.non-competes.com/2009/10/two-views-of-computer-fraud-and-abuse.html>.
- Robert B. Milligan and Carolyn E. Sieve, *Establishing CFAA Violations by Former Employees*, Law 360 (October 27, 2009), <http://www.tradesecretslaw.com/uploads/file/Establishing%20CFAA%20Violations%20-%20Law%20360.pdf>.
- David Johnson, *LVRC v. Brekka: 9th Circuit Decision Creates Circuit Split on Whether CFAA Applies to an Employee Who Misuses His Authority to Access His Employer's Computer Files*, Digital Media Lawyer Blog (October 1, 2009), http://www.digitalmedialawyerblog.com/2009/10/lvrc_v_brekka_9th_circuit_dec.html.
- Lori Bauman, *Ninth Circuit Narrowly Interprets Computer Fraud and Abuse Act*, Ater Wynne LLP Northwest Business Litigation Blog (September 24, 2009), http://www.aterwynneblog.com/oregon_business_litigation/2009/09/ninth-circuit-narrowly-interprets-computer-fraud-and-abuse-act.html.

- David Johnson, *ES&H v. Allied Safety: Court Sidesteps Split in Authority over Whether CFAA Applies to an Employee Who Misuses His Authority to Access His Employer's Computer Files*, Digital Media Lawyer Blog (September 24, 2009), http://www.digitalmedialawyerblog.com/2009/09/esh_v_allied_safety_court_side_1.html.
- Amy E. Bivins, *Brekka Case Shows Need for Comprehensive Strategy to Shield Data from Insider Misuse*, Bureau of National Affairs Electronic Commerce & Law Report (September 20, 2009), <http://www.tradesecretslaw.com/uploads/file/Sieve.pdf>.
- Nick Akerman, *When Workers Steal Data to Use at New Jobs*, The National Law Journal (July 7, 2009), <http://www.law.com/jsp/article.jsp?id=1202432036948>.
- Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819 (March 2009), <http://www.michiganlawreview.org/assets/pdfs/107/5/field.pdf>.
- Richard Warner, *Symposium: The Electronic Workplace: The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 Empl. Rts. & Employ. Pol'y J. 11 (2008), <https://litigation-essentials.lexisnexis.com/webcd/app?action=DocumentDisplay&crawlid=1&crawlid=1&doctype=cite&docid=12+Empl.+Rts.+%26+Employ.+Pol%27y+J.+11&srctype=smi&srcid=3B15&key=5af00d2a6ee82f58f5d3e2de9c20b24f>.
- Shari Claire Lewis, *Can the CFAA Protect Your Firm's Data?*, New York Law Journal (July 25, 2008), <http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202423247330>.
- Brian H. Corcoran, *The Computer Fraud and Abuse Act: "Hacker Repellent" That Works Great on Ex-Employees, Too*, Cyberspace Lawyer Vol. 7, No. 1 (March 2002) at page 2, <http://www.kattenlaw.com/files/Publication/8bb06409-a2bc-4f76-b594-02d9c2c77078/Presentation/PublicationAttachment/a654e6e5-30f5-4bfb-96a0-f174d49f1c45/Technology%20Winter%202001%20PDF.pdf>.

The Defend Trade Secrets Act: The First Year

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave NW, Suite 230
Washington, D.C. 20009
(202) 588-5300

rfitzpatrick@robertbfitzpatrick.com (e-mail)
<http://www.robertbfitzpatrick.com> (website)

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 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.

Ex Parte Seizure Cases

- [OOO Brunswick Rail Mgmt. v. Sultanov](#), 2017 U.S. Dist. LEXIS 2343 (N.D. Calif. January 6, 2017)
- [Balearia Caribbean v. Calvo](#), 1:16-cv-23300 (S.D. Fla. August 5, 2016)
- [Jones Printing v. Adams Lithographing](#), 1:16-cv-00442 (E.D. Tenn. November 3, 2016)
- [Dazzle Software II v. Kinney](#), 2016 U.S. Dist. LEXIS 155993 (E.D. Mich. Aug. 22, 2016)
- [Mission Capital Advisors LLC v. Romaka](#), 16-cv-5878 (S.D. N.Y. July 29, 2016)
- [Earthbound Corp. v. MiTek USA, Inc.](#), 2016 U.S. Dist. LEXIS 110960 (W.D Wash. August 19, 2016)



Expedited Discovery

- [Trulite Glass & Aluminum Solutions, LLC v. Smith](#), 2016 U.S. Dist. LEXIS 142827 (E.D. Cal. Oct. 4, 2016)
- [Allstate Ins. Co. v. Rote](#), 2016 U.S. Dist. LEXIS 104374 (D. Or. August 7, 2016)



DTSA Coverage of Pre-Enactment Conduct

- [Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc.](#), 2016 U.S. Dist. LEXIS 130918 (S.D. N.Y. September 23, 2016)
- [Avago Techs. United States Inc. v. NanoPrecision Prods.](#), 2017 U.S. Dist. LEXIS 13484 (N.D. Calif. January 31, 2017)
- [Adams Arms, LLC v. Unified Weapons Sys.](#), 2017 U.S. Dist. LEXIS 51913 (M.D. Fla. September 27, 2016)



“Misappropriation” under the DTSA

- [HealthBanc Int'l, LLC v. Synergy Worldwide, Inc.](#), 2016 U.S. Dist. LEXIS 130417 (D. Utah September 22, 2016)
- [M.C. Dean v. City of Miami Beach](#), 199 F. Supp. 3d 1349 (S.D. Fla. Aug. 8, 2016)



Whistleblower Provision

- [Unum Grp. v. Loftus](#), 2016 U.S. Dist. LEXIS 168713 (D. Mass. December 6, 2016)



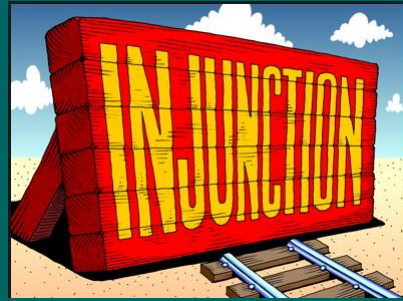
Discovery

- [Henry Schein, Inc. v. Cook](#), 191 F. Supp. 3d 1072 (N. D. Cal. June 10, 2016)



Preliminary Injunction

- *Earthbound Corp v. Mi Tek USA, Inc.*, 2016 U.S. Dist. LEXIS 110960 (W.D. Wash. Aug. 19, 2016)
- *Engility Corp v. Daniels*, 2016 U.S. Dist. LEXIS 166737 (D. Colo. Dec. 2, 2016)
- *OOO Brunswick Rail Mgmt. v. Sultanov*, 2017 U.S. Dist. LEXIS 2343 (N.D. Calif. January 6, 2017)



Questions/Comments?



Feel free to contact me at:
(202) 588-5300

rfitzpatrick@robertbfitzpatrick.com

Non-Compete Agreements and Trade Secrets Discussion Panel

Citations, References, & Materials

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave., N.W.
Suite 230
Washington, D.C. 20009
(202) 588-5300
(202) 588-5023 (fax)
fitzpatrick.law@verizon.net
<http://www.robertbfitzpatrick.com> (website)
<http://robertbfitzpatrick.blogspot.com> (blog)

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.

TABLE OF CONTENTS

I.	Assignments	1
II.	Change in Job Duties.....	6
III.	Choice of Law	11
IV.	Physicians	16
V.	Customer Lists.....	21
VI.	Inevitable Disclosure	25
VII.	Cease and Desist Letter	30
VIII.	Plead with Particularity	34
IX.	Valuation of Goodwill.....	39
X.	Computer Fraud and Abuse Act –Latest Developments	40
XI.	Preemption	45

I. Assignments

1. Business & Technology Law Group, *Maryland Trial Court Enforces Employment Covenant as Asset of Surviving Company*, Jan. 29, 2012, available at http://www.btlg.us/News_and_Press/articles/Non-compete%20assignment (last visited July 15, 2013).

a. *Nat'l Instrument Co. v. Braithwaite*, 2006 MDBT 11, 2006 Md. Cir. Ct. LEXIS 12 (Md. Cir. Ct. 2006).

2. Craig W. Trepanier & James C. MacGillis, *Non-Compete Agreements: Are They Assignable Under Minnesota Law?*, Trepanier & MacGillis, July 1, 2009, available at <http://trepanierlaw.com/whatsnew.asp?id=70520090113> (last visited July 12, 2013).

a. *Saliterman v. Finney*, 361 N.W.2d 175 (Minn. Ct. App. 1985)

3. Margaret Molly DiBianca, *Enforceability of Noncompete Agreements Post-Merger*, LexisNexis Labor & Employment Law Commentary Blog, Oct. 10, 2012, available at <http://www.lexisnexis.com/community/labor-employment-law/blogs/labor-employment-commentary/archive/2012/10/10/enforceability-of-noncompete-agreements-post-merger.aspx> (last visited June 10, 2013).

a. *Acordia of Ohio, L.L.C. v. Fishel*, 133 Ohio St. 3d 356, 978 N.E.2d 823 (Ohio 2012).

4. Thomas A. Dye, *Florida Court Upholds Assignment of Non-Compete Agreement Rights*, Carlton Fields P.A., Aug. 31, 2012, available at <http://www.carltonfields.com/florida-court--upholds-assignment-of-non-compete-agreement-rights-08-31-2012/> (last visited June 10, 2013).

a. *DePuy Orthopaedics, Inc. v. Waxman*, 95 So. 3d 928, 2012 Fla. App. LEXIS 12654 (Ct. App. Fla. 2012).

5. Richard M. Jordan, *Non-Compete Agreements After An Acquisition: Are They Enforceable?*, Findlaw, Mar. 26, 2008, available at <http://corporate.findlaw.com/business-operations/non-compete-agreements-after-an-acquisition-are-they.html> (last visited June 10, 2013).

a. *Siemens Med. Health Servs. Solutions Corp. v. Carmelengo*, 167 F. Supp. 2d 752 (E.D. Pa. 2001).

6. Patricia F. Krewson & James M. Stone, *Ohio Court Finds Non-Compete Assignment Valid, But Scores Duration*, JacksonLewis Workplace Resource Center, Jan. 28, 2009, available at <http://www.jacksonlewis.com/resources.php?NewsID=1610> (last visited June 10, 2013).

a. *Murray v. Accounting Ctr. & Tax Servs., Inc.*, 178 Ohio App.3d 432, 898 N.E.2d 89 (Ct. App. Ohio 2008)

7. Jason Cornell, *Does Florida Permit the Assignment of Non-Compete Agreements?*, South Florida Trial Practice, Feb. 6, 2013, available at <http://southfloridatrial.foxrothschild.com/employment-litigation/does-florida-permit-the-assignment-of-non-compete-agreements/> (last visited June 10, 2013).

a. *Patel v. Boers*, 68 So.3d 380, 2011 Fla. App. LEXIS 13493 (Fla. 5th DCA 2011).

8. *Assignment Clause*, Minnesota Noncompete Agreement.com, Mar. 8, 2012, available at http://minnesotanoncompeteagreement.com/Assignment_Clause.html (last visited June 11, 2013).

9. *Employee Confidentiality Agreement*, LeapLaw, available at http://www.leaplaw.com/pubsearch/preview/4063_EmployeeConfid.pdf (last visited June 11, 2013).

10. Neil Desai & David A. Skidmore, Jr., *Successors and Assigns of Noncompete Agreements in Ohio*, Frost Brown Todd, LLC, Oct. 17, 2012, available at <http://www.frostbrowntodd.com/resources-1525.html> (last visited June 11, 2013).

a. *Acordia of Ohio, L.L.C. v. Fishel*, 133 Ohio St. 3d 356, 978 N.E.2d 823 (Ohio 2012).

11. Richard Tuschman, *General Assignment Clause Is Sufficient for Enforcement of Non-Compete Agreement By Assignee*, Duane Morris Institute: The Florida Employer, Sept. 12, 2011, available at http://blogs.duanemorrisinstitute.com/thefloridaemployer/entry/general_assignment_clause_is_sufficient (last visited June 10, 2013).

a. *Patel v. Boers*, 68 So.3d 380, 2011 Fla. App. LEXIS 13493 (Fla. 5th DCA 2011).

12. Kenneth J. Vanko, *Assignment of Non-Compete Agreements in Ohio Continues To Be Fact-Specific* (Michael's Finer Meats v. Alfery), Legal Developments in Non-Competition Agreements, Jan. 19, 2009, available at <http://www.non-competes.com/2009/01/assignments-of-non-compete-agreements.html> (last visited June 10, 2013).

a. *Michael's Finer Meats v. Alfery*, 649 F. Supp. 2d 748 (S.D. Ohio 2009).

13. *Non-Compete Agreement*, OneCLE, Apr. 21, 2008, available at <http://contracts.onecle.com/type/21.shtml> (last visited June 11, 2013).

14. *Sample Business Contracts: Form of Non-Competition, Non-Disclosure, and Assignment of Inventions Agreement with iVillage, Inc.*, OneCLE, Apr. 21, 2008, available at <http://contracts.onecle.com/ivillage/evans.noncomp.shtml> (last visited June 11, 2013).

15. *As a New Employee, Is It Common to Edit Assignment or Non-compete Agreements Before Signing?*, The Workplace Beta, May 26, 2013, available at <http://workplace.stackexchange.com/questions/12004/as-a-new-employee-is-it-common-to-edit-assignment-or-non-compete-agreements-bef> (last visited June 10, 2013).

16. David Sanders, *Assignment of Employee Noncompetes in the Acquisition Context*, FoleyLardner Trade Secret / Noncompete Blog, July 31, 2009, available at <http://tradesecretnoncompete.wordpress.com/tag/assignment-merger-assets-stock-sale-purchase-non-compete/> (last visited June 10, 2013).

a. *HD Supply Facilities Maint., Ltd. v. Bymoen*, 125 Nev. 200, 210 P.3d 183 (Nev. 2009).

17. Dan Warden, *An Employer Seeking to Enforce an Assigned Non-Compete Must Demonstrate That the Non-Compete Was Assigned*, Colorado Non-Compete Law Blog, Dec. 3, 2008, available at <http://www.coloradononcompetelaw.com/2008/12/articles/assignment/an-employer-seeking-to-enforce-an-assigned-noncompete-must-demonstate-that-the-noncompete-was-assigned/> (last visited July 12, 2013).

18. Kelly L. Hamilton, *The Ohio Supreme Court Gives Teeth to Noncompete Agreements Applicable to Acquired Employees*, Ogletree Deakins, Oct. 22, 2012, available at <http://www.ogletreedeakins.com/print/publications/2012-10-22/ohio-supreme-court-gives-teeth-noncompete-agreements-applicable-acquired-emp> (last visited June 10, 2013).

a. *Acordia of Ohio, L.L.C. v. Fishel*, 133 Ohio St. 3d 356, 978 N.E.2d 823 (Ohio 2012).

19. *Employee Confidentiality Non-Compete and Invention Assignment Agreement*, Docstoc.com, available at <http://premium.docstoc.com/docs/117344764/Employee-Confidentiality-Non-Compete-and-Invention-Assignment-Agreement> (last visited June 11, 2013).

20. Stephen L. Richey, *Non-Competes and Acquisitions*, HR Magazine, Sept. 2006, available at <http://www.shrm.org/Publications/hrmagazine/EditorialContent/Pages/0906legalrends2.aspx> (last visited July 12, 2013).

21. Halifax Media Group, LLC, *Employee Non-Solicitation, Non-Compete and Confidentiality Agreement*, available at <http://poynter.org/extra/HalifaxNonCompete.pdf> (last visited June 11, 2013).

22. Alexander Duie Pyle Latta, *Tips for Pennsylvania Non-Compete Agreements*, Avvo.com, Jan. 1, 2009, available at <http://www.avvo.com/legal-guides/ugc/tips-for-pennsylvania-non-compete-agreements> (last visited July 12, 2013).

23. Lee Gesmer, *Two Recent Noncompete Cases From the Superior Court*, Mass. Law Blog, Mar. 23, 2012, available at <http://masslawblog.com/noncompete-agreements/two-recent-noncompete-cases-from-the-superior-court/> (last visited June 11, 2013).

a. *Grace Hunt IT Solutions v. SIS Software, LLC*, 29 Mass. L. Rep. 460, 2012 Mass. Super. LEXIS 40 (Mass. Super. Ct. 2012).

b. *A.R.S. Servs. v. Baker*, 29 Mass. L. Rep. 457, 2012 Mass. Super LEXIS 43 (Mass. Super. Ct. 2012).

24. Jeffrey R. Schmitt, *Employee's Non-Compete Agreement Unenforceable After Transfer to Third Party*, Danna McKittrick, P.C. Newsflash!, July 2005, available at <http://www.dannamckittrick.com/articles/wp-content/uploads/2009/05/2005-schmitt-employee-non-compete-unenforceable-after-transfer-to-3rd-party.pdf> (last visited June 11, 2013).

a. *Roeder v. Ferrell-Duncan Clinic, Inc.*, 155 S.W.3d 76, 2004 Mo. App. LEXIS 2006 (Mo.App. S.D. 2004).

25. Richard D. Tuschman, *Is a General Assignment Clause Sufficient Under Florida's Non-Compete Statute?*, HR Defense Blog, Sept. 16, 2012, available at <http://www.akerman.com/Blogs/HRDefense/post/2012/09/18/test.aspx> (last visited June 11, 2013).

a. *DePuy Orthopaedics, Inc. v. Waxman*, 95 So. 3d 928, 2012 Fla. App. LEXIS 12654 (Ct. App. Fla. 2012).

26. William M. Corrigan, Jr. & Michael B. Kass, *Non-Compete Agreements and Unfair Competition – An Updated Overview*, Armstrong Teasdale, LLP, Mar.-Apr. 2006, available at <http://www.armstrongteasdale.com/files/Uploads/Documents/Non-Compete%20Agreements%20and%20Unfair%20Competition-8878876-1.PDF> (last visited June 11, 2013).

a. *Victoria's Secret Stores v. May Dep't Stores Co.*, 157 S.W.3d 256, 2004 Mo. App. LEXIS 1973 (Mo. Ct. App. 2004).

27. Barry W. Fissel et. al, *Enforceability of Non-Compete Agreements Following a Merger: Supreme Court of Ohio Overrules Earlier Decision*, Eastman & Smith Legal Briefs, Nov. 2012, available at http://www.eastmansmith.com/documents/publications/enforce%20non%20competes%2011_12.pdf (last visited June 11, 2013).

a. *Acordia of Ohio, L.L.C. v. Fishel*, 133 Ohio St. 3d 345, 978 N.E.2d 814 (Ohio 2012).

b. *Acordia of Ohio, L.L.C. v. Fishel*, 133 Ohio St. 3d 356, 978 N.E.2d 823 (Ohio 2012).

28. *Phillips v. Corporate Express Office Prods.*, 800 So. 2d 618, 619, 2001 Fla. App. LEXIS 11496 (Fla. Dist. Ct. App. 5th Dist. 2001), available at <http://www.5dca.org/opinions/Opin2001/081301/01-864cor.op.pdf> (last visited June 11, 2013).

29. Minn. Dep't of Empl. & Econ. Dev., *Non-Competition Agreements, Non-Solicitation Agreements, and Intellectual Property Rights*, in Employer's Guide to Employment Law Issues in Minnesota, available at http://www.positivelyminnesota.com/Business/Starting_a_Business/Employers_Guide_to_Employment_Law_Issues_in_Minnesota/02_Non-Competition,_Non-Solicitation_Agreements_Intel_Property_Rights.pdf (last visited June 11, 2013).

a. *Softchoice, Inc. v. Schmidt*, 763 N.W.2d 660, 667, 2009 Minn. App. LEXIS 52 (Minn. App. 2009)

30. Robert M. Shea & Scott J. Connolly, *Enforcing Noncompetition Agreements*, Morse, Barnes-Brown & Pendleton P.C., June 2006, available at <http://www.mbbp.com/resources/employment/noncomps.html> (last visited June 11, 2013).

II. Change in Job Duties

1. Morse, Barnes-Brown & Pendleton P.C., Employment Law Group, *Material Changes May Void Employee's Non-Compete*, Morse, Barnes-Brown & Pendleton P.C., Nov. 2012, available at <http://www.mbbp.com/resources/employment/material-job-change.html> (last visited July 12, 2013).
 - a. *Grace Hunt IT Solutions v. SIS Software, LLC*, 29 Mass. L. Rep. 460, 2012 Mass. Super. LEXIS 40 (Mass. Super. Ct. 2012).
 - b. *Protege Software Servs. v. Colameta*, 30 Mass. L. Rep. 127, 2012 Mass. Super. LEXIS 190 (Mass. Super. Ct. 2012).
2. Lee Gesmer, *Noncompete Agreements – Rent-A-PC Fails to Enforce Restrictive Covenants Against Former Employees*, Mass. Law Blog, May 30, 2013, <http://masslawblog.com/noncompete-agreements/rent-a-pc-fails-to-enforce-restrictive-covenants-against-former-employees/>
 - a. *Rent-A-PC, Inc. v. March*, No. 13-10978-GAO, 2013 U.S. Dist. LEXIS 74535 (D. Mass. May 28, 2013), available at <http://pacer.mad.uscourts.gov/dc/cgi-bin/recentops.pl?filename=otoole/pdf/rent%20a%20pc%20v%20march%20pi%20order.pdf> (last visited June 11, 2013).
3. “Marsha411JD,” Response to *If Your Job Description Changes After You Have Signed a Non Compete Contract*, JustAnswer Employment Law, 2010, available at <http://www.justanswer.com/employment-law/3ivct-job-description-changes-signed-non.html> (last visited June 11, 2013).
4. Bennett & Belfort LLP, *Non-Compete Enforcement: The Defenses of Material Job Changes and Wrongful Conduct*, The B&B Docket, May 18, 2012, available at <http://www.bennettandbelfort.com/blog/?p=294> (last visited July 12, 2013).
 - a. *Grace Hunt IT Solutions v. SIS Software, LLC*, 29 Mass. L. Rep. 460, 2012 Mass. Super. LEXIS 40 (Mass. Super. Ct. 2012).
 - b. *A.R.S. Servs. v. Baker*, 29 Mass. L. Rep. 457, 2012 Mass. Super LEXIS 43 (Mass. Super. Ct. 2012).
5. Anonymous user in Kentucky, *How Would Change of Job Responsibilities Effect a Non Compete Agreement?*, Avvo.com, 2009, available at <http://www.avvo.com/legal-answers/how-would-change-of-job-responsibilities-effect-a--150848.html> (last visited June 11, 2013).
6. Jean D. Sifleet, *Understanding Non-Compete Agreements*, Job-Hunt.org, 2006, available at http://www.job-hunt.org/onlinejobsearchguide/article_noncompete_agreements.shtml (last visited June 11, 2013).

7. “PallasAthene,” *Non-Compete and Change in Roles*, Analyst Forum, Mar. 7, 2013, available at <http://www.analystforum.com/forums/careers/91318709> (last visited June 11, 2013).
8. Amy D. Cabbage, *So You Have Non-Compete Agreements in Place. Are They Still Enforceable?*, McBrayer, McGinnis, Leslie & Kirkland, PLLC, June 25, 2012, available at <http://mcbrayeremploymentlaw.com/category/non-competite-agreement/> (last visited June 11, 2013).
9. Susan Heathfield, *What is a Non-Compete Agreement?*, About.com, May 20, 2013, available at http://humanresources.about.com/od/glossaryn/qt/noncompetite_agreement.htm (last visited June 11, 2013).
10. Epke Spijkerman, *When is a Non-competite Clause No Longer Valid*, Employment Law Alliance, Nov. 11, 2011, available at <http://www.employmentlawalliance.com/firms/boekeldeneree/articles/validity-of-non-competite-clause> (last visited June 11, 2013).
11. James Briody, *Where Does Your State Stand on Non-Compete Agreements?*, JD Supra, May 30, 2013, available at <http://www.jdsupra.com/legalnews/where-does-your-state-stand-on-non-compe-05027/> (last visited June 11, 2013).
 - a. *Paramount Pest Control Company, Inc. v. Shaffer*, 282 Va. 412, 718 S.E.2d 762 (2011).
12. Maureen A. Dowd, *Non-Competition Agreements: Reasonable is Key*, Bernstein-Burkley P.C., 2013, available at <http://bernsteinlaw.com/publications-list/non-competition-agreements-reasonable-is-key/> (last visited June 11, 2013).
13. David C. Henderson & Christopher H. Lindstrom, *Eight Issues to Consider When Dealing With Non-Competition Agreements*, NEHRA HR Ctr., Aug. 25, 2008, available at <http://www.boston.com/jobs/nehra/082508.shtml> (last visited June 11, 2013).
14. Terry A. Venneberg, *Non-Compete Agreements*, Tacoma, Washington Employment Lawyer, 2013, available at <http://www.washemploymentlaw.com/employee-rights/noncompetite?agree=yes> (last visited June 11, 2013).
15. Jonathan Lister, *Are Employment Noncompetite Clauses Void Once You Change Title?*, eHow.com, available at http://www.ehow.com/info_8637414_employment-void-once-change-title.html (last visited June 11, 2013).
16. Christopher Cole, *Changes to New Hampshire Non-Compete Law*, Business Law Insights, July 5, 2012, available at <http://blog.sheehan.com/index.php/business-litigation/non-competite-law/> (last visited June 11, 2013).
 - a. H.B. 1270, 2012 Sess. (N.H. 2012), available at <http://legiscan.com/NH/bill/HB1270/2012> (last visited June 11, 2013).

17. Heidi Harvey, *Dos and Don'ts of Fair Competition for Departing Employees (and some Insights for Those Who Employ Them Now or Want to Hire Them)*, Fish & Richardson, 2008, available at <http://www.fr.com/files/uploads/Documents/Dos-and-Don%27ts-of-Fair-Competition-Heidi-Harvey.pdf> (last visited June 11, 2013).
- a. *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1995 U.S. App. LEXIS 10903 (7th Cir. 1995)
18. Cindy Rhodes Victor, *Non-Compete Agreements*, Reference for Business, 2013, available at <http://www.referenceforbusiness.com/management/Mar-No/Non-Compete-Agreements.html> (last visited June 11, 2013).
19. Knowledge@Wharton, *Got a New Job? Better Check That Non-Compete Clause*, Knowledge@Wharton, Mar. 19, 2001, available at <http://knowledge.wharton.upenn.edu/article.cfm?articleid=327> (last visited June 11, 2013).
20. Cameron Shilling, *New Hampshire's Non-Compete Law*, McLane, Graf, Raulerson & Middleton, Dec. 2012, available at <http://www.mclane.com/resources/article-detail.aspx?id=927> (last visited June 11, 2013).
- a. RSA 275:70, 2011 Leg., Reg. Sess. (N.H. 2011) (effective July 14, 2012).
21. R. Scott Oswald & Jason Zuckerman, *Strategies for Defending Against Non-Compete Litigation*, Employment Law Group, 2011, available at <http://www.employmentlawgroup.net/Articles/ROswald/DefendingNonCompete.asp> (last visited June 11, 2013).
- a. *Omniplex World Servs. Corp. v. United States Investigations Servs., Inc.*, 270 Va. 246, 249, 618 S.E.2d 340 (Va. 2005).
- b. *Simmons v. Miller*, 261 Va. 561, 581, 544 S.E.2d 666 (Va. 2001)
22. User Named "Stefanie," *How Binding Are Non-Compete Clauses in Employment Contracts?*, Yahoo! Answers Forum, Aug 8, 2009, available at <http://answers.yahoo.com/question/index?qid=20090808112424AAeHDbM> (last visited June 11, 2013).
23. Alan Sklover, *Don't Let Your Employer Ruin Your Career – How To Defeat a Noncompete Agreement*, Bottom Line Publications, June 15, 2012, available at <http://www.bottomlinepublications.com/content/article/business/dont-let-your-employer-ruin-your-careerhow-to-defeat-a-noncompete-agreement> (last visited June 11, 2013).
24. John L. Koenig, *Proposed Changes to MA Non-Compete Law*, Indigo Venture, Dec. 3, 2010, available at <http://indigoventure.com/briefs/2010/12/proposed-changes-to-ma-non-compete-law/> (last visited June 11, 2013).

a. H.B. 4607, 186th Gen. Assem., 2010 Sess. (Mass. 2010)

25. Jacquelyn Gutc, *Non-compete Agreements May Restrict Employees' Mobility, But Experts Say They Have Benefits*, WBJournal, Sept. 3, 2012, available at <http://www.wbjournal.com/article/20120903/PRINTEDITION/308309983/non-compete-agreements-may-restrict-employees-mobility-but-experts-say-they-have-benefits> (last visited June 12, 2013).

26. Tennessee Employment Law Center, *Non-Compete Agreements*, Tennessee Employment Law Center, 2010, available at http://www.tennesseeemploymentlawcenter.com/noncompete_agreements.html (last visited June 12, 2013).

27. QuickMBA, *Employment Law and Duties to One's Former Employer*, QuickMBA, 2010, available at <http://www.quickmba.com/law/empl/> (last visited June 12, 2013).

28. Anonymous User, *Is the Non-Compete Vet Still Valid If I Have Changed Roles for the Past 7 Years?*, Law Q & A, Apr. 23, 2013, available at <http://www.lawqa.com/qa/is-noncompete-vet-still-valid-if-i-have-changed-roles-for-past-7-years> (last visited June 12, 2013).

29. Vanessa Maire Griffith, *Non-compete Agreements With Employees*, PLC Toolkit, Dec. 2011, available at <http://www.velaw.com/uploadedFiles/VEsite/Resources/Non-CompeteAgreementsEmployees2012.pdf> (last visited June 12, 2013).

a. *National Business Services, Inc. v. Wright*, 2 F. Supp. 2d 701 (E.D. Penn. 1998).

b. *Whitten v. Malcolm*, 541 N.W.2d 45 (Neb. 1995).

30. William Christopher Penwell, *List of Non-Compete Cases Through June 10, 2010*, Seigel Brill, PA, June 10, 2010, available at <http://www.sbgdf.com/files/6013/4573/7675/penwell-noncompetecases.pdf> (last visited June 11, 2013).

a. *Sanitary Farm Dairies v. Wolf*, 261 Minn. 166, 112 N.W.2d 42 (Minn. 1961).

b. *Thermorama, Inc. v. Buckwold*, 267 Minn. 551, 125 N.W.2d 844 (Minn. 1964).

c. *Bennett v. Storz Broadcasting Co.*, 270 Minn. 525, 134 N.W.2d 892 (Minn. 1965).

d. *Sealock v. Petersen*, No. 06-2479, 2008 Minn. App. Unpub. LEXIS 135 (Minn. Ct. App. Feb. 5, 2008).

e. *Berg v. Miller*, No. 04-1188, 2005 Minn. App. LEXIS 398 (Minn. Ct. App. Apr. 12, 2005) (unpublished opinion).

III. Choice of Law

1. Brian E. Dickerson & Jon Secrest, *Protecting Non-Compete Agreements with Choice of Law Provisions and Swift Action*, Ohio Univ. Ctr. for Sports Admin., available at http://www.sportsad.ohio.edu/features/index.html?article_id=274 (last visited June 12, 2013).
2. Paulo B. McKeeby, *Solving the Multi-State Non-Compete Puzzle Through Choice of Law and Venue*, Corporate Counsel, Oct. 17, 2012, available at http://www.morganlewis.com/pubs/CorporateCounsel_SolvingMultiStateNonCompetePuzzle_17oct12.pdf (last visited June 17, 2012).
 - a. *Arkley v. Aon Risk Servs. Cos.*, No. 12-cv-1966, 2012 U.S. Dist. LEXIS 96330 (C.D. Cal. June 13, 2012).
3. Rose McCaffrey, *Choice of Law Provision in Non-Compete and Solicitation Agreements May Mean No Choice for Employers in Arizona*, Sherman & Howard, Jan. 3, 2012, available at <http://www.sah.com/NewsAndEvents/View/90B0B930-5056-9125-63216D793FA097A1/> (last visited June 12, 2013).
 - a. *Pathway Med. Techs., Inc. v. Nelson*, No. 11-cv-0857, 2011 U.S. Dist. LEXIS 113075 (D. Ariz. Sept. 30, 2011).
4. Tyler M. Paetkau, *Enforceability of Non-Compete and Choice-of-Law Provisions in the Modern Employment Contract*, Cal. Labor & Empl. Bulletin, Jan. 2005, available at <http://www.hartnettsmith.com/wp-content/themes/hartnettsmithpaetkau-082012/docs/Choice-of-Law-and-Modern-Employment-Contract.pdf> (last visited June 12, 2013).
 - a. *Nedlloyd Lines B.V. v. Superior Court*, 3 Cal. 4th 459, 834 P.2d 1148 (Cal. 1992).
5. Jonathan Pollard, *Non-Compete Cases and Choice of Law: A Recent Case From Missouri*, The Non-Compete Blog, Nov. 12, 2012, available at <http://thenoncompeteblog.com/2012/11/12/non-competite-cases-and-choice-of-law-a-recent-case-from-missouri/> (last visited June 12, 2013).
 - a. *TLC Vision United States Corp. v. Freeman*, No. 4:12-cv-1855, 2012 U.S. Dist. LEXIS 152592 (E.D. Mo. Oct. 24, 2012).
6. Jennifer A. Adler, *Choice of Law Issues In Non-Compete Agreements*, Robins, Kaplan, Miller & Ciresi, Apr. 1, 2008, available at <http://www.rkmc.com/publications/articles/choice-of-law-issues-in-non-competite-agreements> (last visited June 12, 2013).
 - a. *Convergys Corp. v. Keener*, 276 Ga. 808, 582 S.E.2d 84 (2003).
7. Reginald C. Johnson, *Choice of Law Provisions in Non-Compete Agreements May Be Losing*

Their Teeth, Fox Galvin Employment Law in the News, Feb. 2006, available at <http://www.foxgalvin.com/news/2006-02employment.pdf> (last visited June 12, 2013).

- a. *DCS Sanitation Mgmt. v. Castillo*, 435 F.3d 892 (8th Cir. Neb. 2006), *reh'g denied* by 2006 U.S. Ap.. LEXIS 8154 (8th Cir. Apr. 4, 2006).

8. Connie N. Bertram, *Choice of Law and Forum Selection In Non-Competition Agreements*, Cooley LLP, 2011, available at http://news.acc.com/accwm/downloads/Cooley_011113.pdf (last visited June 12, 2013).

- a. *Stonhard, Inc. v. Carolina Flooring Specialists, Inc.*, 366 S.C. 156, 621 S.E.2d 352 (S.C. 2005).

9. Deborah Crandall Saxe & George S. Howard, *Doing Business In California: The Top 10 Things You Need to Know About California Employment Law*, Jones Day, June 9, 2010, available at <http://www.jonesday.com/files/Event/b5a7c73c-7655-4c2f-a10d-7e053bbb77/Presentation/EventAttachment/d3cd9217-50c8-4814-9da8-1f5baca3b8d1/Handout.pdf> (last visited July 12, 2013).

- a. *D'Sa v. Playhut, Inc.*, 85 Cal. App. 4th 927, 933, 102 Cal. Rptr. 2d 495 (2000).
- b. *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937, 189 P.3d 285 (Cal. 2008).

10. Jason Cornell, *When Do Florida Courts Uphold Choice of Law Provisions in a Non-Compete Agreement?*, S. Florida Trial Practice, Apr. 18, 2013, available at <http://southfloridatrial.foxrothschild.com/employment-litigation/when-do-florida-courts-uphold-choice-of-law-provisions-in-a-non-compete-agreement/> (last visited July 12, 2013).

- a. *Magner International Corp v. Brett*, 960 So.2d 841, 2007 Fla. App. LEXIS 10380 (Fla. Ct. App. 4th 2007).

11. Joel W. Mohrman & Andy Cao, *Can California Law on Noncompete Agreements Affect You?*, Lorman Educ. Servs., Oct. 21, 2011, available at http://www.lorman.com/newsletter/article.php?article_id=1083&newsletter_id=233&category_id=1 (last visited June 12, 2013).

- a. *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (Cal. 2008).

12. Jason Cornell, *Florida Courts Do Not Always Recognize Choice of Law Provisions in Non-Compete Agreements*, S. Florida Trial Practice, May 2, 2013, available at <http://southfloridatrial.foxrothschild.com/employment-litigation/florida-courts-do-not-always-recognize-choice-of-law-provisions-in-non-compete-agreements/> (last visited June 12, 2013).

- a. *Punzi v. Shaker Advertising Agency, Inc.*, 601 So. 2d 599, 1992 Fla. App. LEXIS 6252 (Fla. Dist. Ct. App. 2d Dist. 1992).

13. Cooley LLP, *Noncompete Battles Across State Lines: California Employers Beware*, Cooley LLP Client Alerts, Dec. 14, 2001, available at <http://www.cooley.com/showalert.aspx?Show=57476> (last visited June 12, 2013).

- a. *Advanced Bionics Corp. v. Medtronic, Inc.*, 87 Cal.App.4th 1235, 105 Cal. Rptr. 265 (2001), rev. granted, 2001 Cal. LEXIS 3764 (June 13, 2001).
- b. *D'Sa v. Playhut, Inc.*, 85 Cal. App. 4th 927, 933, 102 Cal. Rptr. 2d 495 (2000).

14. George B. Breen, Frank C. Morris, Jr. & Casey M. Cosentino, *Non-compete Laws: Virginia*, Epstein, Becker & Green, P.C., 2011, available at http://www.ebglaw.com/files/47170_PLC-Non-compete-Laws-Virginia.pdf (last visited June 12, 2013).

- a. *Omniplex World Servs. Corp. v. US Investigations Servs.*, 270 Va. 246, 618 S.E.2d 340 (Va. 2005).
- b. *Simmons v. Miller*, 261 Va. 561, 544 S.E.2d 666 (Va. 2001).

15. Andy Arnold, *Two Bites at the Apple: Choice of Law Provisions in Non-Compete Agreements*, Beat Your Non-Compete, June 4, 2009, available at <http://www.snoncompetelawyer.com/two-bites-of-the-apple-choice-of-law-provisions-in-non-compete-agreements/> (last visited July 12, 2013).

- a. *Stonhard, Inc. v. Carolina Flooring Specialists, Inc.*, 366 S.C. 156, 621 S.E.2d 352 (S.C. 2005).

16. Douglas M. Weems, *Non-compete Laws: Kansas*, PLC Labor & Empl., 2013, available at http://www.spencerfane.com/files/Uploads/Documents/Labor%20and%20Employment/PLC-Non-compete%20Laws_Kansas.pdf (last visited July 12, 2013).

- a. *Weber v. Tillman*, 259 Kan. 457, 913 P.2d 84 (Kan. 1996)

17. Gregory Valenza, *Enforcing Non-Compete Agreements in California After Advanced Bionics v. Medtronic*, Cal. Labor & Empl. Law Bulletin, Apr. 2007, <http://www.shawvalenza.com/pubs/NonCompete.pdf> (last visited June 12, 2013).

- a. *Advanced Bionics Corp. v. Medtronic, Inc.*, 29 Cal. 4th 697, 59 P.3d 231 (Cal. 2002).

18. Vanessa Marie Griffith, *Non-Compete Agreements with Employees*, PLC Law Dep't, 2010, available at <http://www.velaw.com/uploadedFiles/VEsite/Resources/Non-competeAgreementswithEmployees%287-501-3409%29.pdf> (last visited July 12, 2013).

19. Richard Tuschman, *Employee Non-Compete Agreements: One Size Doesn't Fit All*, Forbes, Feb. 18, 2013, available at <http://www.forbes.com/sites/richardtuschman/2013/02/18/employee-non-compete-agreements-one-size-doesnt-fit-all/> (last visited June 12, 2013).

20. Scott J. Wenner & Joleen Okun, *Non-Compete Laws: District of Columbia*, Practical Law Company, 2011, available at <http://www.schnader.com/files/Publication/a13edb32-45a7-4876-b460-71867cfbac4d/Presentation/PublicationAttachment/36832938-c454-441e-88c6-79a5b3464921/Non%20compete%20laws%20in%20District%20of%20Columbia%20Q%20and%20A%20%286-504-6108%29%20%284%29.pdf> (last visited June 12, 2013).
21. Armand J. Zottola et. al, *Enforcing Non-Compete Provisions in California*, Venable LLP Labor & Empl. Law News Alert, Jan. 2012, available at <http://www.venable.com/enforcing-non-compete-provisions-in-california-01-13-2012/> (last visited June 12, 2013).
- a. *Edwards v. Arthur Andersen LLP*, 44 Cal. 4th 937 (Cal. 2008).
22. Steven M. Rubin, *Non-compete Agreements in California: More Than Meets the Eye*, Rubin Law Corporation, available at <http://www.stevenrubinlaw.com/PracticeAreas/Non-compete-Agreements-in-California.asp> (last visited June 12, 2013).
23. Dana H. Shultz, *Choice-of-Law and Non-Compete Provisions*, High-Touch Legal Services Blog, May 13, 2009, available at <http://danashultz.com/blog/2009/05/13/choice-of-law-and-non-compete-provisions/> (last visited June 12, 2013).
- a. *Application Grp. v. Hunter Grp.*, 61 Cal. App. 4th 881, 72 Cal. Rptr. 2d 73 (Cal. App. 1st Dist. 1998)
24. Duane Morris LLP, *Beware Multiple Non-Compete Agreements Given in Connection With Corporate Deals in California*, Duane Morris LLP, Sept. 14, 2012, available at http://www.duanemorris.com/alerts/beware_multiple_non-compete_agreements_given_in_connection_with_corporate_deals_california_4596.html (last visited July 15, 2013).
- a. *Fillpoint, LLC v. Maas*, 208 Cal. App. 4th 1170 (Cal. App. 4th Dist. 2012).
25. Matt Dickstein, *Franchise Non-Competition Agreements in California*, Matt Dickstein Business Attorney, 2013, available at <http://www.matt dickstein.com/Files/4Franchise/Non-Competes.htm> (last visited July 15, 2013).
26. Littler Mendelson PC, *Employers Should Include Choice-of-Law Provisions in Non-Compete Agreements*, Unfair Competition & Trade Secrets Counsel, June 21, 2011, available at <http://www.unfaircompetitiontradeseccounsel.com/covenants-not-to-compete/employers-should-include-choice-of-law-provisions-in-non-compete-agreements/> (last visited July 15, 2013).
- a. *Coface Collections N. Am. v. Newton*, 430 Fed. Appx. 162 (3d Cir. 2011).

27. Neil Klingshirn, *Choice of Law in Non-compete Cases*, My Employment Lawyer, Feb. 7, 2010, available at <http://www.myemploymentlawyer.com/wiki/Choice-of-Law-in-Non-compete-Cases.htm> (last visited July 15, 2013).

a. *S. A. Empresa De Viacao Aerea Rio Grandense v. Boeing Co.*, 641 F.2d 746 (9th Cir. 1981).

28. Lawrence H. Reece, III, *Employee Noncompetition Agreements: Recent Developments and Trends*, 88 Mass. L. Rev. 1 (2003), available at <http://www.massbar.org/publications/massachusetts-law-review/2003/v88-n1/employee-noncompetition-agreements-recent-developments> (last visited July 15, 2013).

a. *Norton Co. v. Hess*, 14 Mass. L. Rep. 162, 2001 Mass. Super. LEXIS 553 (Mass. Super. Ct. 2001).

29. Brian P. Bialas, *The Drawback of Choice-of-Law Clauses for Employers*, Massachusetts Noncompete Law, Oct. 16, 2012, available at <http://www.massachusettsnoncompetelaw.com/2012/10/the-drawback-of-choice-of-law-clauses-for-employers/> (last visited June 12, 2013).

IV. Physicians

1. Claire Bushey, *Non-Compete Clauses Pit Doctor Against Doctor*, Crain's Chicago Business, Oct. 4, 2012, available at <http://www.chicagobusiness.com/article/20121004/NEWS03/121009868/non-compete-clauses-pit-doctor-against-doctor> (last visited July 15, 2013).
2. *Virginia Physician Employment Agreements: "Non-Compete" Provisions*, Frith & Ellerman, P.C., available at <http://www.frithlawfirm.com/Articles/BusinessLitigation/ForDoctors/tabid/147/Default.aspx> (last visited July 15, 2013).
 - a. *Greenbrier Obstetrics & Gynecology, P.C. v. Leao*, No. 08-0072, 2009 Va. LEXIS 118 (Va. Jan. 9, 2009).
3. James M. Shore, *Using Physician Noncompete Agreements in Washington*, Washington Healthcare News, Dec. 2012, available at <http://www.wahcnews.com/newsletters/wa-jshore1210.pdf> (last visited July 15, 2013).
4. Jeffrey L. Cohen, *Noncompete Clause Once Again Relevant for Doctors*, *Medical Economics*, Mar. 25, 2012, available at <http://medicaleconomics.modernmedicine.com/medical-economics/news/modernmedicine/modern-medicine-now/noncompete-clause-once-again-relevant-doct> (last visited July 15, 2013).
5. Victoria Stagg Elliott, *FTC Order Could Give Physicians a Way Out of Noncompete Deals with Hospitals*, Amednews.com, available at <http://www.amednews.com/article/20120822/business/308229997/8/> (last visited July 15, 2013).
 - a. *Renown Health Doctors*, F.T.C. No. C-4366 (Nov. 30, 2012), available at <http://ftc.gov/os/caselist/1110101/121204renownhealthdo.pdf> (last visited July 15, 2013).
6. Beth Wilson, *Location, Location, Location: The Geographic Facts About Noncompete Clauses*, Amednews.com, Jan. 30, 2006, available at <http://www.amednews.com/article/20060130/profession/301309960/4/> (last visited June 11, 2013).
 - a. *Idbeis v. Wichita Surgical Specialists, P.A.*, 279 Kan. 755, 112 P.3d 81 (Kan. 2005).
7. Andy Arnold, *Physician Non-Competes Upheld by South Carolina Court of Appeals: Baugh v. Columbia Heart Clinic, P.A., Beat Your Non-Compete*, Apr. 10, 2013, available at <http://www.sconcompetelawyer.com/physician-non-competes-upheld-by-south-carolina-court-of-appeals-baugh-v-columbia-heart-clinic-p-a/> (last visited July 15, 2013).

a. *Baugh v. Columbia Heart Clinic, P.A.*, 402 S.C. 1, 738 S.E.2d 480 (S.C. Ct. App. 2013).

8. Joe Carlson, *First-of-Its-Kind FTC Agreement on Physician Noncompete Contracts Spurs Doc Exits*, ModernPhysician.com, Dec. 5, 2012, available at <http://www.modernphysician.com/article/20121205/MODERNPHYSICIAN/312059965> (last visited June 11, 2013).

a. *Renown Health Doctors*, F.T.C. No. C-4366 (Nov. 30, 2012), available at <http://ftc.gov/os/caselist/1110101/121204renownhealthdo.pdf> (last visited July 15, 2013).

9. Frost Brown Todd, *The Shifting Tide of Physician Non-Competition Agreements*, Frost Brown Todd Health Law News, Jan. 2005, available at <http://www.frostbrowntodd.com/resources-1132.html> (last visited June 11, 2013).

10. Parker Poe Adams & Bernstein, LLP, *South Carolina Court of Appeals Upholds Physician Non-Compete and Forfeiture Provisions*, Parker Poe EmployNews, Feb. 15, 2013, available at <http://www.parkerpoe.com/news/south-carolina-court-of-appeals-upholds-physician-non-compete-and-forfeiture-provisions/> (last visited June 11, 2013).

a. *Baugh v. Columbia Heart Clinic, P.A.*, 402 S.C. 1, 738 S.E.2d 480 (S.C. Ct. App. 2013).

11. Joseph Maya, *Non-Compete Agreements (Restrictive Covenants) for Practicing Physicians in New York and Connecticut: Just How Enforceable Are They?*, Maya Murphy LLC, May 8, 2013, available at <http://www.mayalaw.com/non-compete-agreements-restrictive-covenants-for-practicing-physicians-in-new-york-and-connecticut-just-how-enforceable-are-they/> (last visited July 15, 2013).

a. *Opticare, P.C. v. Zimmerman*, No. UWYCV075003365S, 2008 Conn. Super. LEXIS 759 (Conn. Super. Ct. Mar. 27, 2008).

12. Robert J. Dreps, *Recent Developments in Physician Non-Compete Agreements*, Godfrey Kahn, S.C., Apr. 20, 2009, available at http://www.gklaw.com/news.cfm?action=pub_detail&publication_id=842 (last visited July 12, 2013).

a. *Oudenhoven v. Nishioka, M.D.*, 52 Wis. 2d 503, 190 N.W.2d 920 (1971).

13. Erin B. Williams & Ian P. Hennessey, *Legal Matters: Considerations for Physician Non-Compete Provisions*, East Tennessee Medical News, June 5, 2012, available at <http://www.easttnmedicalnews.com/news.php?viewStory=2266> (last visited July 15, 2013).

a. *Hasty v. Rent-A-Driver, Inc.*, 671 S.W.2d 471, 1984 Tenn. LEXIS 800 (Tenn. 1984).

14. Zulima V. Farber, David M. Wissert & Denise Walsh, *Are Physician Post-Employment Noncompete Agreements Enforceable?*, The Metropolitan Corporate Counsel, Mar. 2004, available at <http://www.metrocorpounsel.com/pdf/2004/March/04.pdf> (last visited July 12, 2013).

15. Benjamin P. Roach, *Are Physician Non-Compete Agreements Under Attack in Iowa?*, Nyemaster Goode, 2008, available at www.nyemaster.com/userdocs/BPR_Physician_Non_Compete_Agreements.pdf (last visited June 11, 2013).

a. *Bd. of Regents v. Warren*, No. 8-620/08-0017, 2008 Iowa App. LEXIS 1192 (Iowa Ct. App. Nov. 26, 2008), *aff'd* at 760 N.W.2d 209 (Iowa Ct. App. 2008).

16. Jonathan Pollard, *Prominent North Carolina Doctor Wins First Round of Non-Compete Fight*, The Non-Compete Blog, Jan. 29, 2013, available at <http://thenoncompeteblog.com/2013/01/29/prominent-north-carolina-doctor-wins-first-round-of-non-competite-fight/> (last visited July 12, 2013).

a. *Carolina Asthma & Allergy Ctr. v. O'Connor*, No. 13-Cv-S328 (N.C. Bus. Ct. Jan. 25, 2013).

17. Smith & Associates, *Enforceability of Non-Compete Clauses*, June 2, 2011, available at http://smithlawtlh.com/articles/enforceability_physician_noncompete_clauses.html (Last visited June 11, 2013).

a. *Eskiloglu v. Lee Mem. Health Sys.*, No. 11-CA-000617, (N.C., 12th Jud. Cir. 2011).

18. LawServer, *Non-Competition Agreements in Mississippi*, Apr. 2012, available at <http://www.lawserver.com/law/articles/non-competition-agreements-in-mississippi> (July 12, 2013).

19. Jeffrey L. Rhodes, *Non-Compete Law*, Jeffrey L. Rhodes, 2011, available at <https://sites.google.com/site/jefflrhodes/noncompetes> (last visited July 12, 2013).

a. *Mona Electric Group, Inc. v. Truland Service Corp.*, 193 F. Supp. 2d 874 (E.D. Va. 2002), *aff'd*, 56 Fed. Appx. 108, 2003 U.S. App. LEXIS 83 (4th Cir. Va. 2003).

20. Aaron D. Hall, *Minnesota Non-Compete Agreements*, Thompson, Hall, Santi, Cerny & Dooley, May 2009, available at <http://thompsonhall.com/minnesota-noncompete-agreements/> (last visited July 15, 2013).

a. *Tenant Constr., Inc. v. Mason*, No. A07-0413, 2008 Minn. App. Unpub. LEXIS 133 (Minn. Ct. App. Feb. 5, 2008).

21. Daniel D. Quick, *Physician, Meet They Covenant: Noncompete Agreements in the Medical Profession*, Mich. Bar J., May 2007, at 22-24, available at <http://www.michbar.org/journal/pdf/pdf4article1139.pdf> (last visited June 11, 2013).
- a. *St. Clair Med., P.C. v. Borgiel*, 270 Mich. App. 260, 715 N.W. 2d 914 (Mich. Ct. App. 2006).
22. Robert W. Horton & Justin A. Page, *Restrictive Covenants in Physician Employment Relationships*, Am. Health Lawyers Ass'n Member Briefing, July 2010, available at http://www.bassberry.com/files/upload/AHLA_Article_Horton_and_Padgett_April_2013.pdf (last visited July 15, 2013).
- a. *General Surgery, P.A. v. Suppes*, 24 Kan. App. 2d 753, 953 P.2d 1055 (Kan. Ct. App. 1998).
23. Keith Clouse, *A Physician Non-Compete Agreement Must Include a Buy-Out Provision*, Clouse Dunn LLP, Mar. 29, 2012, available at http://www.cdklawyers.com/buy-out-provision_6651.html (last visited July 15, 2013).
24. Steve Pearson, *Noncompete Agreements and Physician Practices*, Armbrecht Jackson LLP, available at <http://www.ajlaw.com/CM/Custom/Noncompete-Agreements.pdf> (last visited July 12, 2013).
- a. Alabama Medical Board Rule 540-x-9-10(3).
25. Medical Justice, *Time to Rip Up Non-Compete Agreements?*, Medical Justice Blog, Dec. 28, 2012, available at <http://blog.medicaljustice.com/time-to-rip-up-non-compete-agreements/> (last visited July 15, 2013).
- a.
26. Tom Shumate, *Update on 2012 Amendment to Statute Governing Health Care Non-Compete Agreements*, Tom Shumate's Tennessee Non-Compete Law Blog, Oct. 14, 2011, available at http://www.tennesseononcompetelaw.typepad.com/tennessee_noncompete_law/2011/10/update-on-2012-amendment-to-statute-governing-health-care-non-compete-agreements.html (last visited July 15, 2013).
- a. Tenn. Code Ann. 63-1-148 (effective Jan. 1, 2012).
- b. Josh McCreary, *The Ongoing Saga of Health Care Non-Compete Agreements*, Tenn. Bar J., Sept. 7, 2011, available at <http://www.tba.org/journal/the-ongoing-saga-of-health-care-non-compete-agreements> (last visited June 11, 2013).
27. Matt Dickstein, *May a Physician Compete Against His Or Her Former Practice?*, Matt Dickstein Business Attorney, available at <http://www.matt dickstein.com/Files/>

[2Professional%20Practices/Medical%20Suite%20-%206%20Competition.htm](#) (last visited June 11, 2013).

V. Customer Lists

1. Daniel J. Fischer & J. Daniel Weidner, *How Do I Protect My Trade Secrets, Including My Customer List*, Koley Jessen, 2013, available at <http://www.koleyjessen.com/resources/how-do-i-protect-my-trade-secrets-including-my-customer-list/> (last visited July 15, 2013).
2. John D. Minton, *Trade Secret Protection for Customer Lists*, Carr McClellan, June 1, 2011, available at <http://www.carrmcclellan.com/publications/trade-secret-protection-for-customer-lists/> (last visited July 15, 2013).
3. Eric Ostroff, *Customer Lists as Trade Secrets: What Protections Are Sufficient?*, Protecting Trade Secrets, May 22, 2013, available at <http://tradesecretslaw.wordpress.com/2013/05/22/customer-lists-as-trade-secrets-what-protections-are-sufficient/> (last visited June 12, 2013).
 - a. *Farmers Ins. Exch. v. Steele Ins. Agency, Inc.*, No. 2:13-cv-00784, 2013 U.S. Dist. LEXIS 70098 (E.D. Cal. May 16, 2013).
4. Roy A. Ginsburg, *Customer Lists as Trade Secrets*, Lexology, Apr. 12, 2010, available at <http://www.lexology.com/library/detail.aspx?g=b6595b3f-da96-4196-9d1d-a0c955d5422a> (last visited June 12, 2013).
 - a. *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 898 (Minn. 1983).
5. Michael S. Neustel, *Trade Secrets*, Neustel Law Offices, available at <http://www.patentman.com/tradesecrets.htm> (last visited June 12, 2013).
 - a. *Surgidev Corp. v. Eye Technology, Inc.*, 828 F.2d 452 (8th Cir. 1987).
6. Jeffrey Huron, *Is Your Customer List a Protected Trade Secret?*, Huron Law Group, May 1, 2008, available at http://www.huronlaw.com/articles/Is_Your_Customer_List_a_Protected_Trade_Secret (last visited June 12, 2013).
7. Keith M. Gregory, *Know Your Rights When an Employee Leaves*, Protect Your Trade Secrets, 2002, available at <http://gbr.pepperdine.edu/2010/08/protect-your-trade-secrets/> (last visited June 12, 2013).
 - a. Cal. Civil Code 3426.1(b) & 3426.2 (2012).
8. John Marsh, *The Erosion of Customer Lists as Trade Secrets: Are They Still Worth Protecting?*, The Trade Secret Litigator, Jan 16, 2012, available at <http://www.hahnloeser.com/tradesecretlitigator/post/2012/01/16/The-Erosion-of-Customer-Lists-As-Trade-Secrets-Are-They-Still-Worth-Protecting.aspx> (last visited July 12, 2013).

a. *Sasqua Group, Inc. v. Courtney*, No. 10-cv-528, 2010 U.S. Dist. LEXIS 93442 (E.D.N.Y. Aug. 2, 2010).

9. Michael J. Nader, *California Court Affirms that Customer Lists Can Qualify as Trade Secrets*, Ogletree Deakins, Oct. 24, 2012, available at <http://blog.ogletreedeakins.com/california-court-affirms-that-customer-lists-can-qualify-as-trade-secrets/> (last visited July 15, 2013).

a. *Wanke, Industrial, Commercial, Residential, Inc. v. Keck*, 209 Cal. App. 4th 1151, 147 Cal. Rptr. 651 (Cal. App. 4th Dist. 2012).

10. Fisher & Talwar, P.C., *Trade Secret Disputes Involving Customer Lists*, Fisher & Talwar, P.C., 2013, available at <http://www.contractdisputeresolution.com/trade-secret-disputes-involving-customer-lists> (last visited July 15, 2013).

a. Cal. Civil Code 3426.1(b) & 3426.2 (2012)

11. Trade Secrets Institute, *Cases from Customer Lists/Information*, Brooklyn Law School, 2013, <http://tsi.brooklaw.edu/category/subject-matter-trade-secrets-claim/customer-listsinformation> (last visited July 15, 2013).

a. *Sunpower Corp. v. SolarCity Corp.*, No. 12-cv-00694, 2012 U.S. Dist. LEXIS 176284 (N.D. Cal. Dec. 11, 2012).

12. Richard Santalesa, *Is Social Networking Disclosing Your Trade Secret Customer Lists?*, Information Law Group, Oct. 26, 2010, available at <http://www.infolawgroup.com/2010/10/articles/social-networking/is-social-networking-disclosing-your-trade-secret-customer-lists/> (last visited July 15, 2013).

a. *Network Telecommunications, Inc. v. Boor-Crepeau*, 790 P.2d 901, 1990 Colo. App. LEXIS 60 (Colo. Ct. App. 1990).

13. Andy Arnold, *When Are Client Lists Trade Secrets? A Case Study: Atwood Agency v. Black, Beat Your Non-Compete*, Aug. 9, 2009, available at <http://www.snoncompetelawyer.com/when-are-client-lists-trade-secrets-a-case-study-atwood-agency-v-black/> (last visited July 12, 2013).

a. *Atwood Agency v. Black*, 374 S.C. 68, 646 S.E.2d 882 (S.C. 2007)

14. Brian A. Hall, *Customer List Not Always a Trade Secret*, UnIntellectual Property, May 14, 2013, available at <http://unintellectualproperty.com/customer-list-not-always-a-trade-secret/> (last visited July 12, 2013).

a. *Calisi v. Unified Fin. Servs., LLC*, No. 1-Ca-cv-11-0812, 2013 Ariz. App. LEXIS 62 (Ariz. Ct. App. Apr. 11, 2013).

15. Boyd Contreras A.P.C., *When Are Customer Lists Trade Secrets?*, Boyd Contreras A.P.C., Mar. 1, 2012, available at <http://www.karieboydlaw.com/blog/2012/03/when-are-customer-lists-trade-secrets.shtml> (last visited July 15, 2013).

16. Marti Ashcraft, *Is Your Customer List a Trade Secret? Don't Be So Sure*, Ashcraft Law, Mar. 1, 2012, available at <http://ashcraftlawyers.com/2012/03/is-your-customer-list-a-trade-secret-dont-be-so-sure/> (last visited July 15, 2013).

17. Jay Barry Harris, *Protecting Trade Secrets*, Fineman Krekstein & Harris, 2013, available at <http://www.finemanlawfirm.com/fineman/index.cfm/publications/publication-details/?dynapsisfuse=showdetails&pkid=209&tableid=2details/?dynapsisfuse=showdetails&pkid=209&tableid=2> (last visited July 15, 2013).

18. Michael R. Greco, *Maintaining Trade Secret Status For Customer Lists: Five Steps Every Company Can Take to Protect Customer Information*, Non-Compete and Trade Secrets, Oct. 7, 2010, available at <http://www.noncompetenews.com/post/2010/10/07/Maintaining-Trade-Secret-Status-For-Customer-Lists-Five-Steps-Every-Company-Can-Take-to-Protect-Customer-Information.aspx> (last visited July 15, 2013).

a. Colo. Rev. Stat. Ann. § 7-74-102(4).

19. Mary Bellis, *All About Trade Secrets*, About.com Guide, 2013, available at http://inventors.about.com/od/tradesecrets/a/trade_secret.htm (last visited July 15, 2013).

20. Fenwick & West L.L.P., *Trade Secrets Protection*, A Primer and Desk Reference for Managers and In House Counsel, Fenwick & West, 2001, available at http://www.fenwick.com/FenwickDocuments/Trade_Secrets_Protection.pdf (last visited July 15, 2013).

21. Timothy K. Sendek, *Customer Lists as Trade Secrets*, National Law Review, Dec. 30, 2009, available at <http://www.natlawreview.com/article/customer-lists-trade-secrets> (last visited July 15, 2013).

a. *Sys. Dev. Servs. v. Haarmann*, 389 Ill. App. 3d 561, 907 N.E.2d 63 (Ill. App. Ct. 5th Dist. 2009).

22. Dietrich Law Firm, *Customer Lists May Be Trade Secrets*, On Texas Law, Mar. 3, 2013, available at <http://www.dietrichlawblog.com/2013/03/customer-lists-may-be-trade-secrets.html> (last visited June 12, 2013).

a. *Alliantgroup, L.P. v. Feingold*, 803 F. Supp. 2d 610 (S.D. Tex. 2011).

23. Howard Fischer, *Customer List May Be Trade Secret, But Not Always*, AZ Central, Apr. 25, 2013, available at <http://www.azcentral.com/business/abg/articles/20130425customer-list-may-trade-secret-not-always.html> (last visited June 12, 2013).

- a. *Calisi v. Unified Fin. Servs., LLC*, No. 1-Ca-cv-11-0812, 2013 Ariz. App. LEXIS 62 (Ariz. Ct. App. Apr. 11, 2013).
24. Michael Geibelson, *Taking an Old Route: Protecting Trade Secrets By Applying The Route Cases*, Robins, Kaplan, Miller & Ciresi, L.L.P., July/Aug. 2004, available at <http://www.rkmc.com/publications/articles/taking-an-old-route-protecting-trade-secrets-by-applying-the-route-cases> (last visited July 15, 2013).
- a. *Morlife, Inc. v. Perry*, 56 Cal. App. 4th 1514, 66 Cal. Rptr. 2d 731 (Cal. App. 1st Dist. 1997).
25. Barbara A. Lawless & Tanisha Shafer, *When Customer Lists Are Not Trade Secrets,: Making the Case Against Enforcing Non-Solicitation Agreements*, Plaintiff Magazine, May 2011, available at http://www.plaintiffmagazine.com/May11/Lawless-&-Shafer_When-customer-lists-are-no-trade-secret_Plaintiff-magazine.pdf (last visited July 15, 2013).
- a. *Alliance Payment Systems, Inc. v. Walczar*, 152 Cal. App. 4th 620, 61 Cal. Rptr. 3d 789 (Cal. App. 1st Dist. 2007).
26. Robert A. Bleicher, *Customer Lists – Trade Secrets – Preparation Counts: Two Courts Reaffirm the Benefit of Identifying and Takeing Steps to Protect Trade Secrets*, JD Supra Law News, June 7, 2013, available at <http://www.jdsupra.com/legalnews/preparation-counts-two-courts-reaffirm-24620/> (last visited June 12, 2013).
- a. *Farmers Ins. Exch. v. Steele Ins. Agency, Inc.*, No. 2:13-cv-00784, 2013 U.S. Dist. LEXIS 70098 (E.D. Cal. May 16, 2013).
27. Rob Radcliff, *Are Customer Lists Trade Secrets?*, Smooth Transitions Blog, Aug. 24, 2009, available at <http://www.smoothtransitionslawblog.com/2009/08/articles/trade-secrets/are-customer-lists-trade-secrets-sometimes/> (last visited July 15, 2013).
- a. *Adco Indus. v. Metro Label Corp.*, No. 05-99-01128-CV, 2000 Tex. App. LEXIS 5644 (Tex. App. Dallas Aug. 23, 2000).
28. William Monty Simmons, *Trade Secret*, Simmons Patents, available at <http://www.simmonspatents.com/id71.html> (last visited July 15, 2013).
- a. Restatement (Second) of Torts 757.
29. R. Mark Halligan, *Trade Secrets*, Nixon Peabody, 2013, available at http://www.nixonpeabody.com/trade_secrets (last visited June 12, 2013).

VI. Inevitable Disclosure

1. *Inevitable Disclosure*, Wikipedia, available at http://en.wikipedia.org/wiki/Inevitable_disclosure (last visited June 23, 2013).
2. Ryan M. Wiesner, *A State-By-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard*, 16 Intellectual Property L. Rev. 211 (2012), available at <http://scholarship.law.marquette.edu/cgi/viewcontent.cgi?article=1187&context=iplr> (last visited June 23, 2013).
 - a. *Cardinal Freight Carriers, Inc. v. J.B. Hunt Transp. Servs., Inc.*, 336 Ark. 143, 987 S.W.2d 642 (Ark. 1999).
3. Joel D. Bush, Audra A. Dial & Jeffrey H. Fisher, *Inevitable Disclosure of Trade Secrets is Not an Independent Cause of Action in Georgia*, Kilpatrick Townsend, May 24, 2013, available at <http://www.mondaq.com/unitedstates/x/241080/disclosure+electronic+discovery+privilege/Inevitable+Disclosure+of+Trade+Secrets+is+Not+an+Independent+Cause+of+Action+in+Georgia> (last visited July 15, 2013).
 - a. *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 2013 Ga. LEXIS 414 (Ga. May 6, 2013).
4. Ivan Hoffman, *Inevitable Disclosure of Trade Secrets*, Ivan Hoffman Attorney at Law, 2002, available at <http://www.ivanhoffman.com/inevitable.html> (last visited July 15, 2013).
 - a. Cal. Civil Code 3426.2 (2012).
5. Geoffrey S. Klein & Gregory Silbert, *Inevitable Disclosure of Trade Secrets: The Rebirth of a Controversial Doctrine and Where Courts Stand*, Bloomberg L. Rep. Vol. 4, No. 3, 2010, available at http://www.weil.com/files/Publication/92fcb204-d5df-489a-97cd-01526a8fb5f4/Presentation/PublicationAttachment/2b30d71b-211d-4c1c-b936-0665afa43a89/inevitable_disclosure.pdf (last visited July 15, 2013).
 - a. *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995).
6. Dale C. Campbell, *Threatened Misappropriation of Trade Secrets vs. Inevitable Disclosure Doctrine -- When Is Line Crossed?*, Weintraub Tobin IP Law Blog, Apr. 13, 2009, available at <http://www.theiplawblog.com/archives/-trade-secrets-threatened-misappropriation-of-trade-secrets-vs-inevitable-disclosure-doctrinewhen-is-the-line-crossed.html> (last visited June 23, 2013).
 - a. *Central Valley General Hospital v. Smith*, 162 Cal. App. 4th 501, 75 Cal. Rptr. 3d 771 (Cal. App. 5th Dist. 2008).

7. Evan Brown, *Former Employer's Trade Secret Claim Under Inevitable Disclosure Doctrine Moves Forward*, Internet Cases Law & Technology, Sept. 12, 2011, available at <http://blog.internetcases.com/2011/09/12/former-employers-trade-secret-claim-under-inevitable-disclosure-doctrine-moves-forward/> (last visited July 15, 2013).
- a. *Mobile Mark, Inc. v. Pakosz*, No. 11-c-2983, 2011 U.S. Dist. LEXIS 99865 (N.D. Ill. Sept. 6, 2011).
8. Paul C. Goulet, *The Doctrine of Inevitable Disclosure*, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Jan. 2004, available at <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=a8e16e42-c6c8-4061-89f1-954f49b504e8> (last visited June 23, 2013).
- a. *First Health Group Corp. v. National Prescrip. Admin., Inc.*, 155 F. Supp. 2d 194, 236 (M.D. Pa. 2001).
9. Kerry L. Bundy, Randall E. Kahnke, Kenneth A. Liebman, *Doctrine of Inevitable Disclosure*, Faegre & Benson, Sept. 2008, available at <http://www.faegrebd.com/webfiles/Inevitable%20Disclosure.pdf> (last visited July 15, 2013).
- a. *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995).
10. Klemchuk Kabasta LLP, *Texas Inevitable Disclosure Doctrine*, Klemchuk Kabasta LLP, available at <http://www.kk-llp.com/356-Texas-Inevitable-Disclosure-Doctrine> (last visited July 15, 2013).
- a. *Electronic Data Sys. Corp. v. Powell*, 508 S.W.2d 137, 1974 Tex. App. LEXIS 2156 (Tex. Civ. App. Dallas 1974).
11. Trepanier Law, *Trade Secret Law: The Inevitable Disclosure Doctrine*, Trepanier Law, Dec. 10, 2010, available at <http://www.trepanierlaw.com/whatsnew.asp?id=200911090360&keywords=%3Ci%3ETrade+Secret+Law%3A+The+Inevitable+Disclosure+Doctrine+%3C%2Fi%3E> (last visited June 23, 2013).
- a. *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 125 Cal. Rptr. 2d 277 (Cal. App. 4th Dist. 2002).
12. Smith, Gambrell & Russell, *The Georgia Supreme Court Rejects the Inevitable Disclosure Doctrine in a Trade Secret Dispute*, Smith, Georgia Appellate Developments, May 8, 2013, available at <http://www.sgrlaw.com/blog/2013/05/the-georgia-supreme-court-rejects-the-inevitable-disclosure-doctrine-in-a-trade-secret-dispute/> (last visited June 23, 2013).
- a. *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 2013 Ga. LEXIS 414 (Ga. May 6, 2013).

13. Eleanore R. Godfrey, *Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights*, 3 J. High Tech. L. 161 (2004), available at <http://web.law.suffolk.edu/highlights/stuorgs/jhtl/docs/pdf/Godfrey-Note-PDF.pdf> (last June 23, 2013).
- a. *Wexler v. Greenberg*, 399 Pa. 569, 160 A.2d 430, 437 (Pa. 1960).
14. Linda K. Stevens, *Trade Secrets and Inevitable Disclosure*, 36 Tort & Ins. L. J. 917 (2001), available at <http://www.jstor.org/stable/25763530> (last visited July 15, 2013).
15. Fox Rothschild, LLP, *No Inevitable Disclosure of Trade Secrets in California*, Cal. UPDATE Employment Law, 4th Qtr. 2009, available at <http://www.foxrothschild.com/newspubs/newspubsArticle.aspx?id=11858> (last visited July 15, 2013).
- a. *Les Concierges, Inc. v. Robeson*, No. 09-1510, 2009 U.S. Dist. LEXIS 39414 (N.D. Cal. Apr. 27, 2009).
16. Betsy Cook Lanzen, *Trade Secret "Inevitable Disclosure" Taking Shape in North Carolina*, The Compass, Apr. 9, 2013, available at <http://www.nclitigation.com/2013/04/trade-secret-inevitable-disclosure-doctrine-still-a-mystery-in-nc/> (last visited July 15, 2013).
- a. *Allegis Group, Inc. v. Zachary Piper LLC*, 2013 NCBC 13 (N.C. Super. Ct. 2013)
17. Cameron G. Shilling, *The Inevitable Disclosure Doctrine: A Necessary and Precise Tool For Trade Secret Law*, Findlaw, Mar. 26, 2008, available at <http://corporate.findlaw.com/intellectual-property/the-inevitable-disclosure-doctrine-a-necessary-and-precise-tool.html> (last visited July 15, 2013).
- a. *Kewanee v. Bicron*, 416 U.S. 470, 94 S.Ct. 1879 (U.S. 1974).
18. Ken LaMance, *Inevitable Disclosure Doctrine and Trade Secrets Lawyers*, LegalMatch, June 17, 2009, available at <http://www.legalmatch.com/law-library/article/inevitable-disclosure-doctrine-and-trade-secrets.html> (last visited July 15, 2013).
19. Randy Burton, Sam Johnson & Cara Burton, *The Sound of Inevitability: The Doctrine of Inevitable Disclosure of Trade Secrets Comes to Texas*, Tex. J. of Bus. L. 103-121 (2009), available at <http://www.burlesonllp.com/media/51186/Burton%20-%20The%20Sound%20of%20Inevitability.pdf> (last visited July 15, 2013).
- a. *Hyde Corp. v. Huffines*, 158 Tex. 566, 314 S.W.2d 763 (Tex. 1958).
20. Goodwin Procter LLP, *De Facto Non-Competition Agreements: The Inevitable Disclosure Doctrine*, Inc. Mag., 2001, available at <http://www.inc.com/articles/2001/08/23292.html> (last visited July 15, 2013).

a. *Marcam Corp. v. Orchard*, 885 F. Supp. 294 (D. Mass. 1995).

21. W. Aaron Daniel, *Georgia Rejects the Inevitable Disclosure of Trade Secrets Doctrine*, Attorney Breakfast Club, May 2013, available at <http://www.abcforNetworking.com/georgia-rejects-the-inevitable-disclosure-of-trade-secrets-doctrine/> (last visited July 15, 2013).

a. *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 2013 Ga. LEXIS 414 (Ga. May 6, 2013).

22. Eric Ostroff, *Georgia Supreme Court Rejects Independent Claim for Inevitable Disclosure of Trade Secrets*, Protecting Trade Secrets, May 7, 2013, available at <http://tradesecretslaw.wordpress.com/2013/05/07/georgia-supreme-court-rejects-independent-claim-for-inevitable-disclosure-of-trade-secrets/> (last visited July 15, 2013).

a. *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 2013 Ga. LEXIS 414 (Ga. May 6, 2013).

23. Elizabeth Rowe, *When Trade Secrets Become Shackles: Fairness and the Inevitable Disclosure Doctrine*, 7 Tul. J. Tech. & Intell. Prop. 167 (2005), available at <http://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1065&context=facultypub> (last visited July 15, 2013).

a. *Merck & Co. v. Lyon*, 941 F. Supp. 1443 (M.D.N.C. 1996).

24. Fenwick & West, LLP, *Trade Secrets Group Client Alert: Inevitable Disclosure is not the Law in California*, Fenwick & West, LLP, Sept. 12, 2002, available at <http://www.fenwick.com/publications/Pages/Trade-Secrets-Group-Client-Alert-Inevitable-Disclosure-is-not-the-Law-in-California.aspx> (last visited June 23, 2013)

a. *Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443 (Cal. App. 4th Dist. 2002), available at <http://euro.ecom.cmu.edu/program/law/08-732/TradeSecrets/Schlage.pdf> (last visited June 23, 2013).

25. Mari L. Myer, *Georgia Supreme Court Rejects Independent Cause of Action for Inevitable Disclosure of Trade Secrets*, Myer Law Firm, June 6, 2013, available at <http://myerlawatlanta.com/2013/06/georgia-supreme-court-rejects-independent-cause-of-action-for-inevitable-disclosure-of-trade-secrets/> (last visited June 25, 2013).

a. *Holton v. Physician Oncology Servs., LP*, 292 Ga. 864, 2013 Ga. LEXIS 414 (Ga. May 6, 2013).

26. Sonya P. Passi, *Compensated Injunctions: A More Equitable Solution to the Problem of Inevitable Disclosure*, Berkeley Tech. L. J. Annual Review (2012), available at http://btlj.org/data/articles/27_AR/927-956_Passi_Final_071012_WEB.pdf (last visited July 15, 2013).

a. *Ecolab, Inc. v. Paolo*, 753 F. Supp. 1100 (E.D.N.Y. 1991).

27. Edward A. Kaplan & Melissa M. Hanlon, *Doctrine of Inevitable Disclosure*, Sulloway & Hollis PLLC, available at http://www.sulloway.com/index.php?option=com_content&view=article&id=292:the-doctrine-of-inevitable-disclosure&catid=54&Itemid=70 (last visited July 15, 2013).

a. *PepsiCo v. Redmond*, 54 F.3d 1262 (7th Cir. 1995).

28. Michael A. Stick & Julie Rodriguez Aldort, *How “Inevitable Disclosure” is Shifting Trade Secrets Litigation*, Corporate Counsel, Jan. 2003, available at <http://www.butlerrubin.com/wp-content/uploads/How-%E2%80%9CInevitable-Disclosure%E2%80%9D-is-Shifting-Trade-Secrets-Law-Corporate-Counsel-January-2003-1.pdf> (last visited July 15, 2013).

29. Matthew K. Miller, *Inevitable Disclosure Where No Non-Competition Agreement Exists: Additional Guidance Needed*, B.U. J. Sci. & Tech. available at <http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume6/miller.pdf> (last visited June 23, 2013).

a. *Lumex, Inc. v. Highsmith*, 919 F. Supp. 624 (E.D.N.Y. 1996).

VII. Cease and Desist Letter

1. Trepanier & MacGillis, P.A., *Sample Reminder Letter to Departing Employee to Protect Trade Secrets*, Minnesota Trade Secrets Attorney, available at http://minnesotatradesecretsattorney.com/Sample_Letter.html (last visited June 24, 2013).
2. Lauri F. Rasnick, *Court Finds Potential Liability For Sending Cease and Desist Letter*, Epstein Becker Green Trade Secrets & Noncompete Blog, June 3, 2013, available at <http://www.tradesecretsnoncompetelaw.com/2013/06/articles/nonsolicit-agreements/court-finds-potential-liability-for-sending-cease-and-desist-letter/> (last visited June 24, 2013).
 - a. *Gentile v. Olan*, No. 12-cv-3664, 2013 U.S. Dist. LEXIS 64472 (S.D.N.Y. May 6, 2013).
3. John Marsh, *Cease and Desist Letter: Defamation May Not Be An Issue But Watch Out for Tortious Interference*, Trade Secret Litigator Blog, Apr. 6, 2013, available at <http://www.hahnloeser.com/tradesecretlitigator/?tag=/cease+and+desist+letter> (last visited June 24, 2013).
 - a. *Murphy v. LivingSocial, Inc.*, No. 12-864, 2013 U.S. Dist. LEXIS 36742 (D.D.C. Mar. 18, 2013).
 - b. *Hidy Motors, Inc. v. Sheaffer*, 183 Ohio App. 3d 316 (Ct. App. Ohio 2009).
4. Thompson Hall Santi Cerny & Dooley, *Cease & Desist Letter Templates, Examples & Sample Forms*, Thompson Hall Santi Cerny & Dooley, Nov. 2011, available at <http://thompsonhall.com/cease-desist-letter-template-example-sample-forms/> (last visited June 23, 2013).
5. Kara M. Maciel, *Cease And Desist Letters Enjoy an Absolute Privilege From Libel Claims*, Epstein Becker & Green, Apr. 3, 2013, available at <http://www.lexology.com/library/detail.aspx?g=db2af47c-2b6f-4fc6-8e28-3836dd4459fa> (last visited July 15, 2013).
 - a. *Murphy v. LivingSocial, Inc.*, No. 12-864, 2013 U.S. Dist. LEXIS 36742 (D.D.C. Mar. 18, 2013).
6. *Cease and Desist Form Letter - Unfair Business Practices and Infringement of Trade Secrets*, DocStoc, available at <http://premium.docstoc.com/docs/107466956/Cease-and-Desist-Form-Letter---Unfair-Business-Practices-and-Infringement-of-Trade-Secrets> (last visited July 15, 2013).
7. Bay Oak Law, *When Cease-and-Desist Means Start Right Now*, Bay Oak Law, 2011,

available at <http://www.bayoaklaw.com/when-cease-and-desist-means-start-right-now/> (last visited July 15, 2013).

a. Cal. Com. Code 2312.

8. Richard Stim & Steven Fishman, *The Cease & Desist Letter*, NDAs For Free, available at <http://www.ndasforfree.com/CeaseandDesist.html> (last visited July 15, 2013).

9. Jonathan B. Tropp, *What Should You Do When You Receive a Cease-And-Desist Notice?*, Day, Berry & Howard LLP, available at <http://www.daypitney.com/news/docs/dbh/news.3702.pdf> (last visited July 15, 2013).

10. Daniel Davidson, *Trademark Infringement - Jack Daniel's Cease and Desist Letter*, Tactical IP, July 24, 2012, available at <http://tacticalip.com/2012/07/24/trademark-infringement-jack-daniels-cease-and-desist-letter/> (last visited July 15, 2013).

11. Eric E. Johnson, *Black Friday Blog Leaks Ads, Stores Make Legal Threats*, Blog Law Blog, Nov. 26, 2010, available at <http://bloglawblog.com/blog/?tag=cease-and-desist-letters> (last visited July 15, 2013).

12. Norah Olson Bluvshein, *Social Shaming - The Latest Response to Cease and Desist Letters*, Networked, Nov. 7, 2011, available at <http://www.networkedlawyers.com/social-shaming-the-latest-response-to-cease-and-desist-letters/> (last visited July 15, 2013).

13. Lisa Honey, *Cease and Desist Letter Template*, Rocket Lawyer, 2013, available at <http://www.rocketlawyer.com/form/cease-and-desist-letter.rl> (last visited July 15, 2013).

14. Santa Clara University School of Law, *MediaDefender's Trade Secrets and Confidential Information*, Chilling Effects Clearinghouse, Sept. 17, 2007, available at <http://www.chillingeffects.org/tradeseecret/notice.cgi?NoticeID=15254> (last visited July 15, 2013).

15. Jonathan Pollard, *Responding to Cease & Desist Letters: Reasonable Assurances*, Florida Non-Compete Lawyer, Mar. 27, 2013, available at <http://floridanoncompetelawyers.com/2013/03/27/responding-to-cease-desist-letters-reasonable-assurances/> (last visited July 15, 2013).

16. Arnold, Knobloch & Saunders, L.P., *Cease and Desist/ Demand Letters*, Arnold, Knobloch & Saunders, L.P., 2012, available at http://www.usptclaw.com/cease_and_desist.htm (last visited July 15, 2013).

17. Mark Malek, *Tim Tebow Sends Cease and Desist Letters to T-Shirt Company*, Tactical IP, May 17, 2013, available at <http://tacticalip.com/2012/05/17/tim-tebow-sends-cease-desist-letter-to-t-shirt-company-copyright-trademark-endorsement/> (last visited July 15, 2013).

18. Traverse Legal, *Trademark Cease and Desist Letter Samples*, Traverse Legal, Oct. 27, 2012,

available at <http://tcattorney.typepad.com/ip/2012/10/trademark-cease-and-desist-letter-samples.html> (last visited July 15, 2013).

19. Dan Harris, *Cease and Desist Letters for China IP Violations. They Can Work.*, China Law Blog, Feb. 3, 2011, available at http://www.chinalawblog.com/2011/02/cease_and_desist_letters_for_china_ip_violations_they_can_work.html (last visited July 15, 2013).

20. Jean L. Batman, *Protecting Intellectual Property: Letters*, GPSolo eReport, Feb. 2012, available at http://www.americanbar.org/publications/gpsolo_ereport/2012/february_2012/intellectual_property_letters.html (last visited July 15, 2013).

21. Post from “panerainovice”, *Cease and Desist Letter Received But Not Sure What Other Troubles I Can Get Into*, TheLaw.com, Feb. 2011, available at <http://www.thelaw.com/forums/showthread.php?t=45635> (last visited July 15, 2013).

22. “imcista”, *Suterra Issues Cease and Desist Letter to Indybay Regarding “Secret” Ingredient in CheckMate Pesticide*, Media Activism, Oct. 12, 2007, available at <http://www.indybay.org/newsitems/2007/10/12/18453681.php> (last visited June 24, 2013).

23. Enrico Schaefer, *Cease and Desist Letter Do’s and Don’ts: A Copyright Attorney’s Perspective*, Traverse Legal, Feb. 26, 2013, available at <http://www.traverselegal.com/copyright-infringement/copyright/cease-and-desist-letter-dos-and-don%E2%80%99ts-a-copyright-attorney%E2%80%99s-perspective/> (last visited June 24, 2013).

24. Deborah E. Bouchoux, *Resolving an Infringement Dispute*, in *Intellectual Property: The Law of Trademarks, Copyrights, Patents, and Trademarks* 406, available at http://books.google.com/books?id=x4H0ulrSDIUC&pg=PA406&lpg=PA406&dq=trade+secrets++cease+and+desist+letter&source=bl&ots=iYrMq-OQG6&sig=zLSII8RP2RkuDiZxkiiriDbcH_k&hl=en&sa=X&ei=kWTIUdKhKuLy0gH7z4GIBg&ved=0CD4Q6AEwAzgU#v=onepage&q=trade%20secrets%20-%20cease%20and%20desist%20letter&f=false (last visited June 24, 2013).

25. Sam Bayard, *Not Every Cease-and-Desist Letter is a DMCA Takedown Notice*, Digital Media Law Project, Sept. 28, 2007, available at <http://www.dmlp.org/blog/2007/not-every-cease-and-desist-letter-dmca-takedown-notice> (last visited June 24, 2013).

26. Simon Heseltine, *Cease and Desist Letter News - Google Webmaster Tools: An Overview*, Search Engine Watch, July 18, 2012, available at <http://searchenginewatch.com/article/2191991/Google-Webmaster-Tools-An-Overview> (last visited June 24, 2013).

27. Not Just Patents LLC, *Trade Name (Business Name) or Trademark Cease and Desist Letters*, Not Just Patents LLC, available at <http://trademark2d.com/trademarktradename.html> (last visited June 24, 2013).

28. David Cotta & Adam Samansky, *Effective Strategies for Sending and Receiving Cease and Desist Letters: Protect Your Client's Interests*, Commercial Law Web Advisor, Apr. 9, 2013, available at <http://commerciallawwebadvisor.com/schedule/detail/Effective-Strategies-for-Sending-and-Receiving-Cease-and-Desist> (last visited June 24, 2013).

29. S.E. Smith, *What Is a Cease and Desist Order?*, WiseGEEK, available at <http://www.wisegeek.org/what-is-a-cease-and-desist-order.htm> (last visited June 24, 2013).

30. Ian Cockburn, *What to Do When Confronted With a "Cease and Desist" Letter*, Evan Carmichael, available at <http://www.evancarmichael.com/Branding/508/What-to-do-when-confronted-with-a-Cease-and-Desist-Letter.html> (last visited June 24, 2013).

VIII. Plead with Particularity

1. Tyler Paetkau, *California's "Reasonable Particularity" Requirement in Trade Secret Litigation*, Cal. Labor & Empl. L. Bulletin, July/August 2005, available at <http://www.hartnettsmith.com/wp-content/themes/hartnettsmithpaetkau-082012/docs/California-Resonable-Particularity-Requirement.pdf> (last visited June 23, 2013).

a. *Struthers Scientific & International Corp. v. General Foods Corp.*, 51 F.R.D. 149, 1970 U.S. Dist. LEXIS 9483 (D. Del. 1970).

2. Brooklyn Law Trade Secrets Institute, *Further Refinement of the Pleading Standard for Trade Misappropriation Claims*, 2012, available at http://tsi.brooklaw.edu/cases/%5Bfield_case_reference-title-raw%5D/reports/further-refinement-pleading-standard-trade-secret-mis (last visited June 23, 2013).

a. *Eastman Chem. Co. v. AlphaPet Inc.*, No. 11-702, 2011 U.S. Dist. LEXIS 152907 (D. Del. Dec. 29, 2011).

3. Christopher A. Pace, *Fundamental Steps to Pleading a Trade Secret Claim in Florida*, Avvo.com, available at <http://www.avvo.com/legal-guides/ugc/fundamental-steps-to-pleading-and-proving-a-trade-secret-claim-in-florida> (last visited June 23, 2013).

a. Fla. Stat. 688.001, et. seq. (2012).

4. Emily C. Haas, *Could You Be More Specific? The Requirement to Plead NC Trade Secret Claims with Specificity*, Coats & Bennett, PLLC, Feb. 21, 2011, available at <http://www.coatsandbennett.com/emily-haas/could-you-be-more-specific-the-requirement-to-plead-nc-trade-secrets-claims-with-specificity> (last visited June 23, 2013).

a. *Stephenson v. Langdon*, No. COA09-1494, 2010 N.C. App. LEXIS 1682 (N.C. Ct. App. Sept. 7, 2010).

5. Scott Cameron, *Obvious, Within General Knowledge, And ... Trade Secret?*, Weintraub Tobin IP Law Blog, Mar. 31, 2009, available at <http://www.theiplawblog.com/archives/-trade-secrets-obvious-within-general-knowledge-and-trade-secret-an-update-to-the-disclosure-requirement-of-ccp-2019210.html> (last visited June 23, 2013).

a. *Brescia v. Angelin*, 172 Cal. App. 4th 133 (Cal. App. 2d Dist. 2009).

6. Charles Tait Graves, Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 NW. J. Tech. & Intell. Prop. 68 (2006), available at <http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1049&context=njtip> (last visited June 23, 2013).

a. *Intermedics, Inc. v. Ventritex, Inc.*, 822 F. Supp. 634 (N.D. Cal. 1993).

7. Margaret A. Esquenet & John F. Hornick, *Trade Secret Identification: The Importance of Timing in Discovery*, Finnegan, Henderson, Farabow, Garrett & Dunner, LLP, Feb. 2005, available at <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=ac7cf37b-c333-4b4e-bafe-6cb9dda0db42> (last visited July 15, 2013).

a. *Engelhard Corp. v. Savin Corp.*, 505 A.2d 30 (Del. Ch. 1986).

8. Benjamin Riley, *Three Pitfalls for Trade Secret Plaintiffs*, ABA Bus. Torts J., Spring/Summer 2008, available at http://www.bzbn.com/wp-content/uploads/2012/07/B.Riley-Article-ABA_Pitfalls_for_Trade_Secret_Plaintiffs-Spring-Summer20081.pdf (last visited July 15, 2013).

a. *Advanced Modular Sputtering, Inc. v. Superior Court*, 132 Cal. App. 4th 826 (Cal. App. 2d Dist. 2005).

9. Daniel Joshua Salinas, *New York Federal Court Rejects Heightened Specificity Pleading Standard for Breach of Confidentiality and Non-Disclosure Claim*, Seyfarth Shaw Trading Secrets Blog, Dec. 4, 2012, available at <http://www.tradesecretslaw.com/2012/12/articles/trade-secrets/new-york-district-court-rejects-heightened-specificity-pleading-standard-for-breach-of-confidentiality-and-non-disclosure-provisions-claim/> (last visited July 15, 2013).

a. *Dorset Indus. v. Unified Grocers, Inc.*, 893 F. Supp. 2d 395 (E.D.N.Y. 2012).

10. Kevin R. Casey, *Identification of Trade Secrets During Discovery*, Stradley, 1996, available at <http://www.stradley.com/library/files/krc-identification.pdf> (last visited July 15, 2013).

a. *Engelhard Corp. v. Savin Corp.*, 505 A.2d 30 (Del. Ch. 1986).

11. Mack Sperling, *A Claim for Misappropriation of Trade Secrets Must Be Plead with "Sufficient Particularity"*, N.C. Business Litigation Report, May 7, 2008, available at <http://www.ncbusinesslitigationreport.com/2008/05/articles/a-claim-for-misappropriation-of-trade-secrets-must-be-plead-with-sufficient-particularity/> (last visited July 15, 2013).

a. *Washburn v. Yadkin Valley Bank & Trust Co.*, 190 N.C. App. 315 (N.C. Ct. App. 2008).

12. Eric Welsh, *Trade Secret Misappropriation Claims Under Attack in North Carolina?*, Trade Secret & Unfair Competition Reporter, Mar. 16, 2013, available at <http://blogs.parkerpoe.com/tradesecrets/uncategorized/trade-secret-misappropriation-claims-under-attack-in-north-carolina/> (last visited July 15, 2013).

a. *AECOM Technology Corp. v. Keating*, 2012 NCBC 10, 2012 NCBC LEXIS 9 (N.C. Super. Ct. 2012).

13. Paul H. Derrick & Rupen F. Fofaria, *Secret's Out. Trade Secrets Remain Important Component of Company IP*, N.C. Bar Ass'n Intellectual Property Section, June 17, 2013, available at <http://intellectualpropertylaw.ncbar.org/newsletters/iplinksjune2013/secret> (last visited July 15, 2013).

a. *Akzo Nobel Coatings, Inc. v. Rogers*, 2011 NCBC 41, 2011 NCBC LEXIS 42 (N.C. Super. Ct. 2011).

14. David Monachino, *Failure to Specifically Identify Trade Secrets in a Complaint Does Not Bar a Complaint in New Jersey Federal Court*, Seyfarth Shaw Trading Secrets Blog, Oct. 27, 2011, available at <http://www.tradesecretslaw.com/2011/10/articles/practice-procedure/failure-to-specifically-identify-trade-secrets-in-a-complaint-does-not-bar-a-complaint-in-new-jersey-federal-court/> (last visited July 15, 2013).

a. *Reckitt Benckiser Inc. v. Tris Pharma, Inc.*, No. 09-3125, 2011 U.S. Dist. LEXIS 19713 (D.N.J. Feb. 28, 2011).

15. Christopher A. Pace, *Secrets Revealed: Fundamental Steps to Pleading and Proving a Trade Secret Claim in Florida – Part 1*, Orange Cnty. Bar Ass'n Briefs, June 2001, available at http://www.pace-law.com/wp-content/themes/Pace-Law_2.0/downloads/CAP - BLC Article - Part I.pdf (last visited July 15, 2013).

16. *South Carolina Code 39-8-60: Preservation of Secrecy During Discovery Proceedings of Civil Actions; Substantial Need Defined*, LawServer, available at http://www.lawserver.com/law/state/south-carolina/sc-code/south_carolina_code_39-8-60 (last visited July 15, 2013).

a. S.C. Code Ann. 39-8-60 (2012).

17. Sid Leach, *Defending Trade Secret Misappropriation Claims: The Identification of Trade Secrets*, Snell & Widmer LLP, Dec. 5, 2005, available at <http://www.swlaw.com/assets/pdf/publications/2005/12/05/Defending-Trade-Secret-Misappropriation-Claims.pdf> (last visited July 15, 2013).

a. *MAI Sys. Corp. v. Peak Computer*, 991 F.2d 511 (9th Cir. 1993).

18. Charles Bieneman, *Patent Applications and Stolen Trade Secrets*, The Software Intellectual Property Report, Sept. 26, 2012, available at <http://swipreport.com/patent-applications-and-stolen-trade-secrets/> (last visited July 15, 2013).

a. *Vasonova Inc. v. Grunwald*, No. 12-02422, 2012 U.S. Dist. LEXIS 133380 (N.D. Cal. Sept. 18, 2012).

19. *Diodes, Inc. v. Franzen*, 260 Cal. App. 2d 244 (Cal. App. 2d Dist. 1968), available at <http://law.justia.com/cases/california/calapp2d/260/244.html> (last visited June 25, 2013).

20. *Uniform Trade Secrets Act*, IT Law Wiki, available at http://itlaw.wikia.com/wiki/Uniform_Trade_Secrets_Act (last visited June 23, 2013).
21. Cristina Hernandez, John McCann Jr. & Michael Martin, *When Your R&D Is No Longer A Trade Secret: Litigating and Calculating Damages*, ABA Section on Litigation Annual Meeting, Apr. 24, 2013, available at http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac2013/sac_2013/22_when_your_r_and_d.authcheckdam.pdf (last visited June 23, 2013).
22. Stuart A. Nelson, *Trade Secret Pleadings*, K & L IP News, Summer 2010, available at <http://www.kinney.com/newsletter/Vol2Issue2.pdf> (last visited June 23, 2013).
- a. *Medafor, Inc. v. Starch Med., Inc.*, No. 09-cv-0441, 2009 U.S. Dist. LEXIS 61345 (D. Minn. July 16, 2009).
- b. *Am. Petroleum Inst. v. TechnoMedia Int'l, Inc.*, No. 09-529, 699 F. Supp. 2d 258 (D.D.C. 2010).
- c. *ACS Partners, LLC v. Americon Group, Inc.*, 2010 U.S. Dist. LEXIS 19907 (W.D.N.C. Feb. 12, 2010).
23. *Misappropriation of Trade Secrets*, Cal. Code Civ. P. 2019.210 (2010), available at <http://www.resolvingdiscoverydisputes.com/C.C.P.%20C%20A72019.210%20%28pdf%29.pdf> (last visited June 25, 2013).
24. Peter J. Toren, *Current Trade Secret Litigation Issues – Recent EEA Prosecutions*, AIPLA Annual Meeting, Oct. 18, 2012, available at <http://petertoren.com/wp-content/uploads/2012/10/AIPLA-PP-trade-secrets1.pptx> (last visited June 25, 2013).
25. Eric W. Shweinbenz & Lisa Mandrusiak, *Discovering Trade Secrets: The Devil Is In the Details*, Bloomberg Patent, Trademark, and Copyright J., Jul. 20, 2012, available at <http://www.oblon.com/sites/default/files/news/schweibenz%20mandrusiak%20trade%20secrets.pdf> (last visited June 25, 2013).
26. John M. Kirby, *Trade Secret Laws in North Carolina*, Law Offices of John M. Kirby, 2012, available at <http://www.legal-nc.com/trade-secret-north-carolina.html> (last visited June 23, 2013).
- a. *Barburino v. Cappuccine*, No. 10-cvs-1417 (N.C. Ct. App. Mar. 6, 2012) (unpublished opinion).
27. *2010 Unfair Competition Law Case Summaries*, Texas Bar Intellectual Property Section, 2011, available at <http://texasbariplaw.org/committees/committee/trade-secrets/documents/download/5%2F2010%2520Unfair%2520Competition%2520Law.doc> (last visited June 25, 2013).

28. *2011 Trade Secret Case Law Report*, ABANet, 2012, available at http://meetings.abanet.org/webupload/.../Trade_Secret_Case_Law_Reportc.doc (last visited June 25, 2013).

29. *Treco Int'l v. Kromka*, 706 F. Supp. 2d 1283 (S.D. Fla. 2010), available at <http://www.joffelaw.com/caselaw/2010/04/07/treco-international-s-a-v-kromka-case-no-09-cv-22987-king-april-7-2010/> (last visited June 25, 2013).

30. Rebecca Tushnet, *Pleading Agency and Vicarious Liability with Particularity*, Rebecca Tushnet's 43(B)log, Aug. 3, 2012, available at <http://tushnet.blogspot.com/2012/08/pleading-agency-and-vicarious-liability.html> (last visited June 25, 2013).

a. *W. Sugar Coop. v. Archer-Daniels-Midland Co.*, No. cv-11-3473, 2012 U.S. Dist. LEXIS 109927 (C.D. Cal. July 31, 2012).

IX. Valuation of Goodwill

1. Rebecca Woods, *Virginia Supreme Court Muddies Damages Valuation of Lost Goodwill in Trade Secret Matter*, Seyfarth Shaw Trading Secrets Blog, June 18, 2012, available at <http://www.tradesecretslaw.com/2012/06/articles/trade-secrets/virginia-supreme-court-muddies-damages-valuation-of-lost-goodwill-in-trade-secret-matter/> (last visited June 26, 2013).
 - a. *21st Century Sys. v. Perot Sys. Gov't Servs.*, 284 Va. 32 (Va. 2012).
2. Kara M. Maciel, *Virginia Supreme Court Overturns Multi-Million Dollar "Goodwill" Damages Award in Trade Secrets Conspiracy Case*, Trade Secrets and Non-Compete Blog, June 13, 2012, available at <http://www.tradesecretsnoncompetelaw.com/2012/06/articles/trade-secrets/virginia-supreme-court-overturns-multimillion-dollar-goodwill-damages-award-in-trade-secrets-conspiracy-case/print.html> (last visited June 26, 2013).
3. James B. Kinsel, *Va. Supreme Court Overturned a Multi-Million Dollar Goodwill Damages Award*, LeClair Ryan Unfair Business Practices Blog, Aug. 28, 2012, available at <http://unfairbusinesspractices.blogspot.com/2012/08/recently-in-case-of-21st-century.html> (last visited June 26, 2013).
4. Stanley J. Feldman, *Principles of Private Firm Valuation* 164 (2005), available at <http://books.google.com/books?id=Y58PcrvMtlMC&lpg=PA164&ots=D-VxrNcvVJ&dq=trade%20secrets%20-%20valuation%20of%20goodwill&pg=PA164#v=onepage&q=trade%20secrets%20-%20valuation%20of%20goodwill&f=false> (last visited June 26, 2013).

X. Computer Fraud and Abuse Act –Latest Developments

1. Computer Fraud and Abuse Act, Wikipedia, *available at* http://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act (last visited June 27, 2013).
2. Dave Smith, *Computer Fraud and Abuse Act 2013: New CFAA Draft Aims to Expand, Not Reform, the “Worst Law in Technology,”* International Business Times, Mar. 28, 2013, *available at* <http://www.ibtimes.com/computer-fraud-abuse-act-2013-new-cfaa-draft-aims-expand-not-reform-worst-law-technology-1158515> (last visited June 27, 2013).
3. Jason Mick, *Bill to Reform Computer Fraud and Abuse Act Proposed in Aaron Swartz’s Name*, DailyTech, June 24, 2013, *available at* <http://www.dailytech.com/Bill+to+Reform+Computer+Fraud+and+Abuse+Act+Proposed+in+Aaron+Swartzs+Name/article31812.htm> (last visited June 27, 2013).
4. Recent Zwillgen articles with tag “Computer Fraud and Abuse Act”:
 - a. Randy Sabett, *Live from Georgetown Cybersecurity Law Institute*, ZwillGen, May 22, 2013, *available at* <http://blog.zwillgen.com/2013/05/22/live-from-the-georgetown-cybersecurity-law-institute/> (last visited June 27, 2013).
 - b. Randy Sabett, *Georgetown Cybersecurity Law Institute, Part 2*, ZwillGen, May 28, 2013, *available at* <http://blog.zwillgen.com/2013/05/28/georgetown-cybersecurity-law-institute-part-2/> (last visited June 27, 2013).
5. William Peacock, *Aaron’s Law Introduced Today, Revises Computer Fraud and Abuse Act*, Findlaw Technologist, June 20, 2013, *available at* <http://blogs.findlaw.com/technologist/2013/06/aarons-law-introduced-today-revises-computer-fraud-and-abuse-act.html> (last visited June 27, 2013).
6. Electronic Frontier Foundation, *Computer Fraud and Abuse Act*, Electronic Frontier Foundation, Apr. 24, 2013, *available at* https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29 (last visited June 27, 2013).
7. Stephanie Francis Ward, *Hacker’s Hell: Many Want to Narrow the Computer Fraud and Abuse Act*, ABA Journal, May 1, 2013, *available at* http://www.abajournal.com/magazine/article/hackers_hell_many_want_to_narrow_the_computer_fraud_and_abuse_act/ (last visited June 27, 2013).
8. *Computer Fraud and Abuse Act*, 18 U.S.C. 1030 *et. seq.*, as found on Dep’t of Energy website, last updated Sept. 22, 2006, *available at* <http://energy.gov/sites/prod/files/cioprod/documents/ComputerFraud-AbuseAct.pdf> (last visited June 27, 2013).

9. Peter J. Toren, *Amending the Computer Fraud and Abuse Act*, Bloomberg Law, 2013 available at <http://about.bloomberglaw.com/practitioner-contributions/amending-the-computer-fraud-and-abuse-act/> (last visited June 27, 2013).
10. Recent Volokh Conspiracy archive for blog posts with “Computer Fraud and Abuse Act”:
 - a. Orin Kerr, *Washington Post on United States v. Auernheimer*, The Volokh Conspiracy, Apr. 29, 2013, available at <http://www.volokh.com/2013/04/29/washington-post-on-united-states-v-auernheimer/> (last visited June 27, 2013).
 - b. Orin Kerr, *A Question for Supporters of Increasing Maximum Sentences Under the Computer Fraud and Abuse Act*, The Volokh Conspiracy, Mar. 28, 2013, available at <http://www.volokh.com/2013/03/28/a-question-for-supporters-of-increasing-maximum-sentences-under-the-computer-fraud-and-abuse-act/> (last visited June 27, 2013).
11. Recent CNet Posts with “Computer Fraud and Abuse Act”:
 - a. Declan McCullagh, *Craigslist Wins Early Legal Victory Against PadMapper*, 3Taps, CNet, Apr. 30, 2013, available at http://news.cnet.com/8301-13578_3-57582252-38/craigslist-wins-early-legal-victory-against-padmapper-3taps/ (last visited June 27, 2013).
 - b. Declan McCullagh, *‘Aaron’s Law’ Rewrite Backfires, Reformers Now on Defensive*, CNet, Apr. 2, 2013, available at http://news.cnet.com/8301-13578_3-57577520-38/aarons-law-rewrite-backfires-reformers-now-on-defensive/ (last visited June 27, 2013).
12. Eric Goldman, *The Computer Fraud and Abuse Act is a Failed Experiment*, Forbes, Mar. 28, 2013, available at <http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/> (last visited June 27, 2013).
13. Margaret Rouse, *Computer Fraud and Abuse Act*, SearchCompliance, June 2012, available at <http://searchcompliance.techtarget.com/definition/The-Computer-Fraud-and-Abuse-Act-CFAA> (last visited June 27, 2013).
14. “Ms. Smith,” *Reporters Threatened with CFAA, Labeled Hackers for Finding Security Hole*, Network World Privacy and Security Fanatic, May 20, 2013, available at <http://www.networkworld.com/community/blog/reporters-threatened-cfaa-labeled-scripps-hackers-finding-security-hole> (last visited June 27, 2013).
15. Recent Mashable Articles with “Computer Fraud and Abuse Act”:

- a. Lorenzo Franceschi-Biccherai, *Aaron's Law Introduces Reform to Anti-Hacking Legislation*, Mashable, June. 20, 2013, available at <http://mashable.com/2013/06/20/aarons-law/> (last visited June 27, 2013).
 - b. Alex Fitzpatrick, *Activists Abhor Draft Computer Fraud and Abuse Act Amendment*, Mashable, Mar. 25, 2013, available at <http://mashable.com/2013/03/25/cfaa-amendment/> (last visited June 27, 2013).
16. Press Release, ThoughtWorks, *ThoughtWorks Supports Reform of the United States' Computer Fraud and Abuse Act (CFAA)* (May 14, 2013), available at <http://finance.yahoo.com/news/thoughtworks-supports-reform-united-states-130000763.html> (last visited June 27, 2013).
17. Electronista Staff, *'Aaron's Law' Introduced to Reform the US Computer Fraud and Abuse Act*, Electronista, June 20, 2013, available at <http://www.electronista.com/articles/13/06/20/activist.aaron.swartz.prosecuted.under.old.version.of.law/> (last visited June 27, 2013).
18. WOT Forum Post linking to:
- a. Major Geeks, *'Aaron's Law' Looks to Modify the Computer Fraud and Abuse Act*, Major Geeks, June 21, 2013, available at http://www.majorgeeks.com/news/story/aarons_law_looks_to_modify_the_computer_fraud_and_abuse_act.html (last visited June 27, 2013).
19. Amanda Whitney, *Aaron's Law Introduces Reform to Anti-Hacking Legislation*, Fitzgibbon Media, June 21, 2013, available at <http://www.fitzgibbonmedia.com/aarons-law-introduces-reform-to-anti-hacking-legislation/> (last visited June 27, 2013).
20. Paul Rosenzweig, *Opposition to the House Computer Fraud and Abuse Act (CFAA) Draft*, Lawfare, Apr. 2, 2013, available at <http://lawfareblog.com/2013/04/opposition-to-the-house-computer-fraud-and-abuse-act-cfaa-draft/> (last visited June 27, 2013).
21. SC Magazine, *Is the Computer Fraud and Abuse Act Too Broad?*, SC Magazine, Apr. 18, 2013, available at <http://www.scmagazine.com/is-the-computer-fraud-and-abuse-act-too-broad/slideshow/1219/#2> (last visited June 27, 2013).
22. Tim Wu, *Fixing the Worst Law in Technology*, The New Yorker, Mar. 18, 2013, available at <http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html> (last visited June 27, 2013).
23. InfoSecurity, *Computer Fraud and Abuse Act Used to Threaten Journalists*, InfoSecurity, May 24, 2013, available at <http://www.infosecurity-magazine.com/view/32602/computer-fraud-and-abuse-act-used-to-threaten-journalists/> (last visited June 27, 2013).

24. Isaak Foerster, *Blackhawk Mines B06n Gaming Review-Computer Fraud and Abuse Act 2013: New CFAA Draft Aims to Expand, Not Reform, the “Worst Law in Technology”*, Blackhawk Mines, Apr. 24, 2013, available at <http://www.slideshare.net/isaakfoerster/computer-fraud-and-abuse-act-2013> (last visited June 27, 2013).
25. Anonymous, *#OpAngel 2 – The Computer Fraud and Abuse Act Reform Begins Now!*, Anon Insiders, Jan. 17, 2013, available at <http://anoninsiders.net/opangel-2-797/index.html> (last visited June 27, 2013).
26. Tor Ekeland, P.C., *Computer Fraud and Abuse Defense Fund – Access Unauthorized!!*, The Computer Fraud and Abuse Act Defense Fund, 2012, available at <http://cfaadefensefund.com/> (last visited June 27, 2013).
27. Recent Huffington Post Articles with “Computer Fraud and Abuse Act”:
- a. Gerry Smith, *Aaron Swartz Honored with Proposed Reform to Controversial Law*, Huffington Post, June 20, 2013, available at http://www.huffingtonpost.com/2013/06/20/aaron-swartz-aarons-law_n_3473930.html (last visited June 27, 2013).
 - b. Gerry Smith, *Scripps Employees Called ‘Hackers’ for Exposing Massive Security Flaw*, Huffington Post, May 23, 2013, available at http://www.huffingtonpost.com/2013/05/22/scripps-reporters-hackers_n_3320701.html (last visited June 27, 2013).
28. Cory Doctorow, *Understanding the Computer Fraud and Abuse Act: Can You Go to Jail for Violating a Clickthrough Agreement?*, Boing Boing, Feb. 18, 2013, available at <http://boingboing.net/2013/02/18/understanding-the-computer-fra.html> (last visited June 27, 2013).
29. Jason C. Schwartz & Michael Murray, *Recent Developments in Trade Secret Law: The Computer Fraud and Abuse Act*, SHRM Federal Resources, June 10, 2011, available at <http://www.shrm.org/legalissues/federalresources/pages/tradesecretlawcfaa.aspx> (last visited June 27, 2013).
30. Keith Kupferschmid, *Update on Recent Computer Fraud and Abuse Act Cases*, Digital Disclosure, Sept. 5, 2012, available at <http://www.siia.net/blog/index.php/2012/09/update-on-recent-computer-fraud-and-abuse-act-cases/> (last visited June 27, 2013).
- a. *Musket Corp. v. Star Fuel of Okla., LLC*, 2013 U.S. Dist. LEXIS 64309 (W.D. Okla. May 6, 2013).
 - b. *Craigslist, Inc. v. Kerbel*, No. 11-3309, 2012 U.S. Dist. LEXIS 108573 (N.D. Cal. Aug. 2, 2012).

c. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. S.C. 2012).

d. *Wentworth-Douglass Hosp. v. Young & Novis P.A.*, No. 10-cv-120, 2012 U.S. Dist. LEXIS 90446 (D.N.H. 2012).

XI. Preemption

1. James Kachmar, *Trade Secrets and Preemption*, Weintraub Tobin, Mar. 13, 2009, available at <http://www.theiplawblog.com/archives/-trade-secrets-trade-secrets-and-preemption.html> (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Technology & Operations, Inc.*, 171 Cal. App. 4th 939 (Cal. App. 6th Dist. 2009).
2. Daniel Joshua Salinas, *Growing California Trade Secret Preemption Doctrine May Thwart Efforts to Combat Employee Data Theft*, Seyfarth Shaw, Mar. 28, 2013, available at <http://www.seyfarth.com/publications/2869> (last visited June 20, 2013).
3. Michael Jacobs, *Uniform Trade Secrets Act Preemption: An Obscure Doctrine Finally Gets Its Day in Court*, Morrison Foerster, Sept. 11, 2007, available at <http://www.mofo.com/Uniform-Trade-Secrets-Act-Preemption-An-Obscure-Docctrine-Finally-Gets-Its-Day-in-Court-09-11-2007/> (last visited June 20, 2013).
4. Joel Leeman, *Federal Preemption Has Its Limits: State Law Governs Theft of Trade Secrets Even When a Patent Is Involved*, Sunstein, Kann, Murphy & Timbers, LLP, Feb. 2009, available at <http://sunsteinlaw.com/federal-preemption-has-its-limits-state-law-governs-theft-of-trade-secrets-even-when-a-patent-is-involved/> (last visited June 20, 2013).
 - a. *Russo v. Ballard Med. Prods.*, 550 F.3d 1004 (10th Cir. Utah 2008).
5. Eric Ostroff, *District of Connecticut Addresses Trade Secret Act Preemption*, Protecting Trade Secrets, May 30, 2013, available at <http://tradesecretslaw.wordpress.com/2013/05/30/district-of-connecticut-addresses-trade-secret-act-preemption/> (last visited June 20, 2013).
 - a. *Allstate Ins. Co. v. Sawicki*, No. 3:12-cv-1584, 2013 U.S. Dist. LEXIS 72899 (D. Conn. May 23, 2013).
6. Peter Boyer, *Preemption of Business Torts Under the Uniform Trade Secrets Act*, Am. Bar Ass'n, Feb. 19, 2013, available at <http://apps.americanbar.org/litigation/committees/businesstorts/articles/winter2013-0213-preemption-business-torts-uniform-trade-secrets-act.html> (last visited June 20, 2013).
7. Andrew Stround, *Trade Secret Preemption: Too Much Too Soon?*, New Matter, 2009, available at http://www.mgslaw.com/documents/trade_secret_preemption.pdf (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Technology & Operations, Inc.*, 171 Cal. App. 4th 939 (Cal. App. 6th Dist. 2009).
8. Wilson, Sonsini, Goodrich & Rosati, P.C., *Indiana Joins the Emerging Majority Position on Uniform Trade Secrets Act Preemption of State-Law Tort Claims*, WSGR Alert, Sept. 20, 2012, available at <http://www.wsgr.com/publications/PDFSearch/wsgralert-indiana-UTSA-position.pdf> (last visited June 20, 2013).
 - a. *HDNet LLC v. N. Am. Boxing Council*, 972 N.E.2d 920 (Ind. Ct. App. 2012).
9. Joseph Tadros, *California Court Takes On Trade-Secret Preemption Of Other Civil Claims*, Intellectual Property Law Blog, May 21, 2010, available at <http://www.intellectualpropertylawblog.com/archives/271315-print.html> (last visited June 20, 2013).

- a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
10. Mike Young, *Finally, A Citable California Case Confirming Trade Secret Preemption!*, Alston & Bird, Mar. 24, 2009, available at <http://www.alston.com/laborandemploymentblog/?entry=1729> (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
11. Andres Quintana, *Preemption Under California's Uniform Trade Secrets Act*, Quintana Law Group, APC, available at <http://www.qlglaw.com/docs/qlg-article-new-matter-trade-secrets-preemption.pdf> (last visited June 20, 2013).
12. York M. Faulkner, *Overlooking the Obvious "Extra Element of Secrecy in Avoiding Copyright Preemption of Trade Secret Misappropriation Claims*, Finnegan, Feb. 2003, available at <http://www.finnegan.com/resources/articles/articlesdetail.aspx?news=34972c89-2963-47f0-9226-611ffa993baa> (last visited June 20, 2013).
 - a. *Dun & Bradstreet Software Services, Inc. v. Grace Consulting, Inc.*, 307 F.3d 197 (3rd Cir. 2002).
13. Charles Tait Graves & Elizabeth Tippet, *USTA Preemption and the Public Domain: How Courts Have Overlooked Patent Preemption of State Law Claims Alleging Employee Wrongdoing*, 65 Rutgers L. Rev. __ (2013) available at <http://www.stanford.edu/dept/law/ipsc/Paper%20PDF/Tippet%20&%20Graves%20-%20Paper.pdf> (last visited June 20, 2013).
14. Patrick E. Premo & Julie Nokleberg, *California's Uniform Trade Secrets Act Preempts State Common Law Claims*, Fenwick & West LLP, Apr. 7, 2009, available at <http://www.mondaq.com/unitedstates/x/77070/Californias+Uniform+Trade+Secrets+Act+Preempts+State+Common+Law+Claims> (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
15. Kenneth J. Vanko, *California Court Holds Trade Secrets Preemption Issue Premature for Ruling*, Legal Developments in Non-Competition Agreements, Nov. 2, 2011, available at <http://www.non-competes.com/2011/11/california-court-holds-trade-secrets.html> (last visited June 20, 2013).
 - a. *Amron Int'l Diving Supply, Inc. v. Hydrolinx Diving Commun., Inc.*, No. 11-cv-1890-H, 2011 U.S. Dist. LEXIS 122420 (S.D. Cal. Oct. 21, 2011).
16. Dylan B. Carp, *California's Uniform Trade Secrets Act Preempts Other Employment Torts Based on the Same Nucleus of Facts as a Claim for Trade Secret Misappropriation*, The Job Description, July 29, 2009, available at http://www.imakenews.com/employlaw/e_article001502168.cfm?x=b11,0,w (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
17. Jason B. Lattimore, *Chancery Division Holds that New Jersey Trade Secrets Act Does Not Preempt Related Action*, Jason Lattimore, Esq., available at <http://lattimorelaw.com/preemption-under-the-nj-trade-secrets-act/> (last visited June 20, 2013).

- a. *SCS Healthcare Mktg., LLC v. Allergan USA, Inc.*, No. C-268-12, 2012 N.J. Super. Unpub. LEXIS 2704 (Ch.Div. Dec. 7, 2012).
- 18. Gibson, Dunn & Crutcher LLP, *California Court of Appeal Issues Decision Upholding Preemption of Claims for Breach of Confidence, Interference with Contract, and Statutory Unfair Competition Under the California Uniform Trade Secrets Act*, Gibson, Dunn & Crutcher LLP, June 3, 2009, available at <http://www.gibsondunn.com/publications/pages/CADecision-PreemptionofClaims-CAUniformTradeSecrets.aspx> (last visited June 20, 2013).
 - a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
- 19. Marian Solomon Lubinsky, *Patents and Trade Secrets – Does Federal Law Preempt State Law?*, 2 Western New England L. Rev. 110 (1979), available at http://assets.wne.edu/159/13_note_Patent_L.pdf (last visited June 20, 2013).
 - a. *Aronson v. Quick Point Pencil Co.*, 440 U.S. 257 (U.S. 1979).
- 20. Dylan Wiseman & Todd Ratshin, *A California Federal Court Reinigorates the Growing Tension Over The Preemptive Scope of California’s Uniform Trade Secrets Act*, Littler Mendelson, P.C., Nov. 16, 2011, available at <http://www.littler.com/publication-press/publication/california-federal-court-reinigorates-growing-tension-over-preemptive> (last visited June 20, 2013).
 - a. *Amron Int’l Diving Supply, Inc. v. Hydrolinx Diving Commun., Inc.*, No. 11-cv-1890-H, 2011 U.S. Dist. LEXIS 122420 (S.D. Cal. Oct. 21, 2011).
- 21. Charles Jung, *Preemption – Northern District of California Holds That CUTSA Supersedes Common Law Claims Where Plaintiff Alleges a Confidentiality Agreement But Failed to Allege Defendant Was Bound By It*, California Trade Secrets, Feb. 14, 2012, available at <http://caltradesecrets.com/2012/02/14/northern-district-of-california-holds-that-cutsa-supersedes-common-law-claims-where-plaintiff-alleges-a-confidentiality-agreement-but-failed-to-allege-defendant-was-bound-by-it/> (last visited June 20, 2013).
- 22. William J. Brutocao, *Does the California Uniform Trade Secrets Act Preempt A Common Law Breach of Loyalty Claim?*, LexisNexis Labor & Employment Law Community, Jan. 3, 2013, available at <http://www.lexisnexis.com/community/labor-employment-law/blogs/emergingissues/archive/2013/01/03/does-the-california-uniform-trade-secrets-act-preempt-a-common-law-breach-of-loyalty-claim.aspx> (last visited June 20, 2013).
- 23. W. Thomas Haynes, *Trade Secrets – Federal Patent Law Preemption of State Trade Secret Law*, 16 B.C. L. Rev. 291 (1975), available at <http://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1471&context=bclr> (last visited June 20, 2013).
 - a. *Kewanee v. Bicron*, 416 U.S. 470 (U.S. 1974).
- 24. Dennis L. Hall, *Preempt .. Preempt .. The Trade Secrets Act is Strong*, Dennis L. Hall, Attorney, PLLC, Apr. 11, 2013, available at <http://www.dlhall.net/blog/2013/4/11/preempt-preempt-the-trade-secrets-acts-is-strong> (last visited June 20, 2013).
 - a. *Firetrace USA, LLC v. Jesclard*, 800 F. Supp. 2d 1042 (D. Ariz. 2010).
- 25. Owen J. McKeon, *New Jersey Superior Court Finds the Recently-Enacted New Jersey Trade Secrets Act Does Not Preempt Common Law Claims*, Gibbons IP Law Alert, Dec. 14, 2012, available at <http://www.iplawalert.com/2012/12/articles/trade-secret/new->

- [jersey-superior-court-finds-the-recently-enacted-new-jersey-trade-secrets-act-does-not-preempt-common-law-claims/](#) (last visited June 20, 2013).
- a. *SCS Healthcare Mktg., LLC v. Allergan USA, Inc.*, No. C-268-12, 2012 N.J. Super. Unpub. LEXIS 2704 (Ch.Div. Dec. 7, 2012).
26. Charles Post, *California Uniform Trade Secrets Act Preemption: Golden Bullet or Much Ado About Nothing*, The Trade Secret & Employee Raiding Law Blog, Oct. 1, 2011, available at <http://www.tradesecretemployee raiding.com/2011/10/01/california-uniform-trade-secrets-act-preemption-golden-bullet-or-much-ado-about-nothing/> (last visited June 20, 2013).
- a. *K.C. Multimedia, Inc. v. Bank of America Tech. & Ops., Inc.*, 171 Cal. App. 4th 939 (2009).
27. Kelly M. Fiege, *Federal Patent Law Preempts Minnesota Trade Secrets Law*, Trepanier & MacGillis, P.A., Apr. 2, 2012, available at <http://www.trepanierlaw.com/whatsnew.asp?id=201205012140> (last visited June 20, 2013).
- a. *C.G.H., Inc. v. Nash Finch, Inc.*, No. A11-1598, 2012 Minn. App. Unpub. LEXIS 266 (Minn. Ct. App. Apr. 2, 2012).
28. Robert Rohrberger, *Court Finds That Common Law Claims Are Not Preempted By the Recently Adopted New Jersey Trade Secret Act*, Fox Rothschild New Jersey Litigation Law Blog, Dec. 21, 2012, available at <http://njlitigationlaw.foxrothschild.com/business-law/court-finds-that-common-law-claims-are-not-preempted-by-the-recently-adopted-new-jersey-trade-secret/> (last visited June 20, 2013).
- a. *SCS Healthcare Mktg., LLC v. Allergan USA, Inc.*, No. C-268-12, 2012 N.J. Super. Unpub. LEXIS 2704 (Ch.Div. Dec. 7, 2012).
29. David Pardue, *The Walls Closing In on IP Torts: The State Trade Secret Preemption in Georgia and Other States*, Trade Secrets and IP Today, Mar. 4, 2013, available at <http://tradesecretstoday.blogspot.com/2013/03/the-walls-closing-in-on-ip-torts-state.html> (last visited June 20, 2013).
- a. *Robbins v. Supermarket Equip. Sales, LLC*, 290 Ga. 462 (Ga. 2012).

Non-Compete Developments

by

Robert B. Fitzpatrick, Esq.
Robert B. Fitzpatrick, PLLC
1666 Connecticut Ave NW, Suite 230
Washington, D.C. 20009
(202) 588-5300 (phone)

rfitzpatrick@robertbfitzpatrick.com (e-mail)
<http://www.robertbfitzpatrick.com> (website)

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 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.

Non-Compete Unenforceable for Lack of Consideration

- *Charles T. Creech, Inc. v. Brown*, 433 S.W.3d 345 (Ky. Jun. 19, 2014)
 - Agreement gave employee no rights; imposed no duties on employer; employer not required to forebear the exercise of a legal right.



Offer of At-Will Employment, or Continuation of At-Will Employment, is Not Sufficient Consideration

- *Durrell v. Tech Elecs., Inc.*, 2016 U.S. Dist. LEXIS 157689 (E.D. Mo. Nov. 15, 2016)



Continued Employment is Not Adequate Consideration for a Restrictive Covenant

- *Socko v. Mid-Atlantic Sys. of CPA, Inc.*, 126 A.3d 1266 (Pa. Nov. 18, 2015)



Continued Employment Alone Constitutes Adequate Consideration for a Non-Compete

- *Std. Register Co. v. Keala*, 2015 U.S. Dist. LEXIS 73695, *1 (D. Haw. June 8, 2015)
- *Runzheimer International, Ltd. v. Friedlen*, 862 N.W.2d 879 (Wisc. 2015)



Non-Solicitation Violation: \$4.5 Million Punitive Damage Award Upheld

- [*B.G. Balmer & Co. v. Frank Crystal & Co.*](#), 148 A.3d 454 (Pa. Super. Ct. Sept. 9, 2016). LEXIS 104374 (D. Or. August 7, 2016)



LinkedIn Posts Did Not Amount to Solicitation

- [*BTS, USA, Inc. v. Exec. Perspectives, LLC*](#), 2014 Conn. Super. LEXIS 2644 (Conn. Super. Ct. Oct. 16, 2014)



Texts and Facebook Posts Found Not to Constitute Solicitation

- [Herrick v. Potandon Produce, LLC](#), 2016 U.S. Dist. LEXIS 160555 (D. Idaho Nov. 17, 2016)



Facebook Posts are not Solicitation Under Restrictive Covenant Agreements

- *Pre-Paid Legal Servs. v. Cahill*, 924 F. Supp. 2d 1281 (E.D. Okla. Jan. 22, 2013)
- *Enhanced Network Solutions Group, Inc. v. Hypersonic Technologies Corp.*, 951 N.E.2d 265 (Ind. Ct. App. 2011)



The Texas Citizens Participation Act may be the Basis of a Motion to Dismiss a Trade Secret Misappropriation Claim

- [*Elite Auto Body LLC v. Autocraft Bodywerks, Inc.*](#), 2017 Tex. App. LEXIS 4108 (Tex. App. May 5, 2017)
 - The case is pending in the Texas Supreme Court.



Non-Compete Covenant is assignable, absent specific language prohibiting an assignment, even though the covenant is part of a personal services contract

- [*Great Am. Opportunities, Inc. v. Cherrydale Fundraising, LLC*](#), 2010 Del. Ch. LEXIS 15 (Del. Ch. Jan. 29, 2010)



An employer's material breach of an employment agreement precludes the employer's action for breach of violation of a non-compete, where non-competition occurred after employer's material breach

- [Jumbosack Corp. v. Buyck](#), 407 S.W.3d 51 (Mo. Ct. App. May 21, 2013)



A voluntary dismissal of a claim under the Trade Secrets Act, absent an adjudication on the merits or a settlement agreement, does not render the defendant a “prevailing party” entitled to attorneys’ fees.

- [Matrix Basement Sys. v. Drake](#), 2017 Ill. App. Unpub. LEXIS 592 (Ill. App. Ct. Mar. 24, 2017)



Geographic limitation covering North America, Europe, and China is unreasonable as it precluded employee from working in an industry employee had worked for much of career

- [*NBTY, Inc. v O'Connell Vigliante*](#), 2015 N.Y. Misc. LEXIS 4302 (N.Y. App. Div. Nov. 24, 2015)



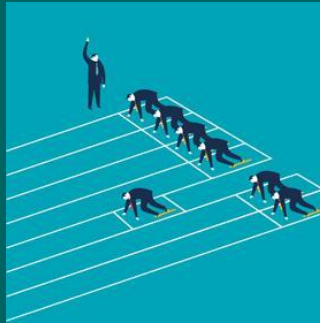
Potential Client List is a Trade Secret

- [*Nucar Consulting, Inc. v. Doyle*](#), 2005 Del. Ch. LEXIS 43 (Del. Ch. Ap. 5, 2005)



Copyright Act Preempts State Law Unfair Competition Claim

- [Ultraflo Corp. v. Pelican Tank Parts, Inc.](#), 845 F.3d 652 (5th Cir. Jan. 11, 2017)



Employees of Skincare Salon possessed conventional job knowledge and skills and customer goodwill belonged stylists.

- *Elizabeth Grady Face First, Inc. v. Garabedian*, 33 Mass. L. Rep. 324 (Sup. Ct. Mass. March 25, 2016)



Employees' appropriation of employer's files violated confidentiality agreement

- *Cafasso v. Gen. Dynamics C4 Sys.*, 637 F.3d 1047 (9th Cir. 2011)



Restrictive covenant prohibiting employees from working *in any capacity* is overbroad

- *Reading & Language Learning Ctr. v. Sturgill*, 2016 Va. Cir. LEXIS 125 (Va. 2016)



Blue penciling rejected by deeply divided court

- *Golden Rd. Motor Inn, Inc. v. Islam*, 376 P.3d 151 (Nev. 2016)



“Allowing litigants to assign to the Court their drafting duties as parties to a contract would put the Court in the role of scrivener ...”

- *Beverage Sys. Of the Carolinas, LLC v. Associated Bev. Repair, LLC*, 368 N.C. 693 (N.C. Mar. 18, 2016)



Tortious Interference with Non-Compete Requires Actual Knowledge of Agreement at Issue

- *Acclaim Sys. v. Infosys*, 679 Fed. Appx. 207 (3d Cir. Pa. Feb. 9, 2017)

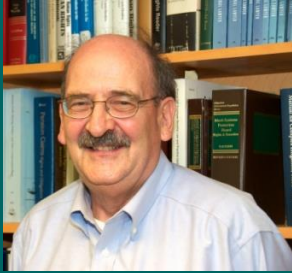


Relief Denied Because Non-Competition Agreement Did Not Have an Extension Clause

- *Citadel Inv. Group, LLC v. Teza Techs. LLC*, 924 N.E.2d 95 (Ill. App. Ct. 1st Dist. Feb. 24, 2010)



Questions/Comments?



Feel free to contact me at:
(202) 588-5300
rfitzpatrick@robertbfitzpatrick.com