

2013  
YEAR IN REVIEW

# Trading Secrets

A Law Blog on Trade Secrets,  
Non-Competes, and Computer Fraud

Trading Secrets Makes  
**ABA TOP  
100**  
BLOG LIST!



# Trading Secrets



Dear Clients and Friends,

2013 was a year of great change and accolades for our Trading Secrets blog. In particular, the Trading Secrets blog was selected as an ABA top 100 blog. Since 2007, the blog has continued to grow in both readership and postings. Content from Trading Secrets has appeared on newsfeeds such as Lexology and ITechLaw, Corporate Counsel, Bloomberg News, BNA, and Kevin O’Keefe’s “Real Lawyers Have Blogs,” one of the leading sources of information and commentary on the use of blogs. We are pleased to provide you with the 2013 Year in Review, which compiles our significant blog posts from 2013 and highlights our blog’s authors. For a general overview of 2013, we again direct you to our Top 10 2013 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2013 Trade Secrets Webinar Series - Year in Review blog entry, which provide a summary of key cases and legislative developments in 2013, as well as practical advice on maintaining trade secret protections.

As the specific blog entries that are contained in this Review demonstrate, our blog authors stay on top of the latest developments in this area of law and provide timely and entertaining posts on significant new cases, legal developments and legislation. We continue to include video interviews, an informative resources page, special guest authors, cutting-edge infographics and access to our well-received Trade Secret Webinar Series from 2011 to the present. In 2013, we introduced video blog posts, audio podcasts, more special guest authors, and provided an additional enhanced Resources page on the blog. We will also offer in 2014 developments in privacy, social media, and technology into our blog coverage.

In addition to our blog, Seyfarth’s dedicated Trade Secrets, Computer Fraud, & Non-Competes Practice Group hosts a popular series of webinars, which address significant issues facing clients today in this important and ever-changing area of law. In 2013, we hosted 12 webinars, which are listed in this Review. For those who missed any of the programs in the 2013 webinar series, the webinars are available on compact disc upon request.

We are kicking-off the 2014 webinar series with a program entitled, “2013 National Year in Review: What You Need to Know About Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law.” More information on our upcoming 2014 webinars is available in the program listing contained in this Review. Our highly successful blog and webinar series further demonstrate that Seyfarth Shaw’s national Trade Secret, Computer Fraud & Non-Competes Practice Group is one of the country’s preeminent groups dedicated to trade secrets, restrictive covenants, computer fraud, and unfair competition matters and is recognized as a *Legal 500* top group.

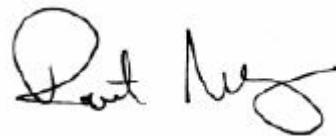
Thank you for your continued support.

Michael Wexler



Practice Group Chair

Robert Milligan



Practice Group Co-Chair and Editor



# Trading Secrets

## Table of Contents

2013 and 2014 Trade Secrets Webinar Series .....	3
Our Authors .....	5
List of Trading Secrets 2013 Blog Posts .....	11
Trading Secrets Blog Posts:	
2013 Summary Posts .....	25
Trade Secrets .....	40
Computer Fraud and Abuse Act .....	137
Non-Competes and Restrictive Covenants .....	185
Legislation .....	268
International .....	293
Social Media .....	309



# Trading Secrets



## 2013 Trade Secrets Webinar Series

- [2012 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law](#)  
*January 2013*
- [Trade Secrets in the Telecommunications Industry](#)  
*February 2013*
- [Employee Privacy and Social Networking: Can Your Trade Secrets Survive?](#)  
*March 2013*
- [How the America Invents Act Increases the Importance of Trade Secrets](#)  
*April 2013*
- [Trade Secrets in the Financial Services Industry](#)  
*May 2013*
- [Trade Secret and Non-Compete Legislative Update](#)  
*June 2013*
- [The Big Data Revolution: How Big Data Impacts Trade Secret, Computer Fraud & Privacy Law](#)  
*July 2013*
- [Trade Secret and Non-Compete Considerations in Asia](#)  
*August 2013*
- [How and Why California Is Different When It Comes To Trade Secrets and Non-Competes](#)  
*September 2013*
- [Trade Secrets in the Pharmaceuticals Industry](#)  
*October 2013*
- [My Company's Confidential Information is Posted on the Internet! What Can I Do?](#)  
*November 2013*
- [The Stakes Just Got Higher: Criminal Prosecution of Trade Secret Misappropriation](#)  
*December 2013*





# Trading Secrets



## 2014 Trade Secrets Webinar Topics

- 2013 National Year in Review: What You Need to Know About the Recent Cases/ Developments in Trade Secrets, Non-Compete, and Computer Fraud
- Employee Privacy, Big Data and Social Networking
- Data Management and Effectively Addressing Data Breaches
- Trade Secret and Non-Compete Legislative Update
- International Trade Secrets and Non-Compete law Update (Australia and EU focus)
- Protecting Confidential Information and Client Relationships in the Financial Services Industry
- Injunction Primer and Discovery in Trade Secrets, Non-Compete, and Computer Fraud Cases
- Protecting Trade Secrets and Intellectual Property in Business Transactions

# Trading Secrets



## Our Authors



**Kate Perrelli** is a partner in the firm's Boston office and Chair of Seyfarth's Litigation Department. She is a trial lawyer with over 20 years of experience representing regional, national, and international corporations in the financial services, transportation, manufacturing, technology, pharmaceutical, and staffing industries. Her commercial practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, unfair competition and complex commercial disputes, including dealer/franchise disputes, and contract disputes.



**Michael Wexler** is a partner in the firm's Chicago office, where he is Chair of the Chicago Litigation Department and Chair of the national Trade Secrets, Computer Fraud, and Non-Competes Practice Group. His practice focuses on trial work and counseling in the areas of trade secrets and restrictive covenants, corporate espionage, unfair competition, complex commercial disputes, intellectual property infringement, and white collar criminal defense in both federal and state courts. A former state prosecutor, Mr. Wexler's extensive investigatory experience and considerable jury trial practice enables him to advise clients with regard to potential disputes and represent clients through and including a determination of their rights at trial.



**Robert Milligan** is the Editor of the blog and Co-Chair of the national Trade Secrets, Computer Fraud, and Non-Competes Practice Group. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation and other intellectual property theft, real estate litigation, insurance bad faith, invasion of privacy, products liability, wrongful termination, discrimination and harassment claims, wage and hour disputes, ADA and OSHA compliance, whistleblower cases, bankruptcy and other business torts. Mr. Milligan has represented clients in state and federal courts in complex commercial litigation and employment litigation. His experience includes trials, binding arbitrations and administrative hearings, mediations, as well as appellate proceedings.



**Michael Baniak** is a highly experienced Intellectual Property litigator and trial lawyer. Mr. Baniak has a broad-based practice, and expertise that spans all facets of IP transactions, counseling, and litigation and appellate work, in patent, trademark, copyright and trade secret law. He is a true "hybrid," working in every aspect of IP virtually daily. Mr. Baniak counsels an international array of clients.

# Trading Secrets



**Justin Beyer** is a partner in the Chicago office of Seyfarth Shaw LLP and a member of the firm's Commercial Litigation Practice Group. Mr. Beyer focuses his practice in the areas of product liability, complex commercial litigation, and trade secrets, including seeking and defending against injunctive relief based on claims of misappropriation of trade secrets and breaches of non-competition agreements. Mr. Beyer has represented plaintiffs and defendants in the agricultural, banking, construction, food processing equipment manufacturing, general manufacturing, healthcare, pharmaceutical, real estate development, and transportation industries.



**Misty Blair** is an associate in the Intellectual Property and Commercial Litigation Practice Groups of Seyfarth Shaw LLP. She practices in the areas of complex civil litigation, patent litigation, trade secrets litigation, and a variety of intellectual property matters, including patent and trademark prosecution. She is a registered Patent Attorney before the United States Patent and Trademark Office.



**Randy Bruchmiller** is a senior associate in the Commercial Litigation and Trade Secrets practice groups of Seyfarth Shaw LLP. Mr. Bruchmiller was a principal at a medium-size litigation firm in Houston prior to joining Seyfarth Shaw in 2010. He has handled a variety of cases while representing both plaintiffs and defendants. He has obtained numerous favorable outcomes for those clients through summary judgments, settlements and trial.



**Paul Freehling** is senior counsel with the Chicago office of Seyfarth Shaw LLP. With more than 40 years of professional experience, Mr. Freehling has tried cases in both state and federal courts and before arbitration tribunals, and he has argued before three U.S. Circuit Courts of Appeal as well as the Illinois Appellate Court. In addition to his practice in a wide variety of complex litigated matters, Mr. Freehling has significant experience in alternative dispute resolution both as a neutral and as an advocate. He has been appointed to the Roster of Distinguished Neutrals by the CPR Institute for Dispute Resolution, the premier organization for alternative methods of dispute resolution. Mr. Freehling is also a Fellow of the American College of Trial Lawyers and elected member of the American Law Institute.



**Gary Glaser** is a partner in the New York office practicing in the area of labor and employment law and litigation. In addition to his litigation practice, Mr. Glaser also counsels and represents clients in litigation involving corporate espionage / non-compete / restrictive covenant / trade secrets issues; wage and hour issues; employment agreements; human resources policies and procedures; management training regarding sexual harassment and other EXEO and labor law issues.

# Trading Secrets



**Daniel Hart** is an associate in the Atlanta office of Seyfarth Shaw LLP. A member of the Labor & Employment department, he focuses his practice in all aspects of labor and employment litigation, including race, gender, national origin, age, and disability discrimination claims, wage and hour disputes, and common law tort claims, before various state and federal courts and administrative agencies.



**Scott Humphrey** is a partner in Seyfarth Shaw LLP's Trade Secrets, Restrictive Covenants and Corporate Espionage Group. He serves on the Group's National Steering Committee and has successfully prosecuted and defended trade secrets and restrictive covenant cases throughout the United States. In doing so, Scott has successfully obtained and defeated temporary restraining orders, preliminary injunctions and permanent injunctions involving trade secret and restrictive covenant matters for clients in the technology, securities and financial services, transportation, electronics, software, insurance, healthcare, consumer products, and manufacturing industries. Scott has also written and reviewed restrictive covenant agreements for both Fortune 100 and small privately held corporations.



**Sarah Izfar** is a commercial litigation associate in Seyfarth Shaw LLP's Washington, D.C. office. Ms. Izfar has experience representing a wide range of companies in business disputes in both state and federal courts. Her practice focuses on complex commercial litigation, including breach of contract, fraud, and trade secret claims. Prior to joining the firm, Ms. Izfar served as a law clerk for a judge in the New York State Commercial Division and a corporate associate at a large New York firm specializing in bank finance and capital markets transactions.

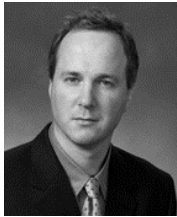


**Molly Joyce** focuses on litigation involving all aspects of restrictive covenants and trade secret and intellectual property protection. She also regularly counsels clients on hiring decisions relating to restrictive covenants and has written restrictive covenant agreements for a variety of entities. Ms. Joyce has represented a wide range of clients — including consulting companies, medical device manufacturers, commercial and residential developers, hospitals, insurance companies, property managers, private business owners and telecommunications carriers — through all phases of litigation, including emergency injunctions, trials and appeals. Ms. Joyce was recognized by Super Lawyers as a 2011 and 2012 "Rising Star" in Illinois for Business Litigation.



**Georgina McAdam** is an associate in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP, based in the firm's London office. Her focus is on all areas of employment law, both contentious and non-contentious. Prior to joining Seyfarth Shaw, Ms. McAdam worked in one of London's top-tier employment departments.

# Trading Secrets



**James McNairy** is a partner in the Sacramento office of Seyfarth Shaw LLP. He is a member of the Litigation department and his practice focuses on commercial, trade secret, and employment litigation. Mr. McNairy's commercial litigation practice focuses on complex matters involving breach of contract; insurance bad faith; franchise, dealer and distribution disputes; unfair competition; business torts; false advertising; discriminatory pricing; and anti-trust. Mr. McNairy prosecutes and defends trade secret misappropriation claims, including obtaining associated expedited discovery and relief. Mr. McNairy's employment litigation practice focuses on restrictions on competition and freedom of employment (non-compete and non-solicitation agreements), ERISA, discrimination, harassment, wrongful termination, and wage and hour class actions brought under state and federal law.



**Marcus Mintz** is a senior associate in the Chicago office of Seyfarth Shaw LLP. Mr. Mintz's practice focuses on complex commercial litigation, including cases involving post-merger disputes, misappropriation of trade secrets and intellectual property, equity rights, and business tort claims. Mr. Mintz has represented a wide range of clients, including medical device manufacturers, clinical research organizations, automotive manufacturers, defense contractors, construction companies, insurance companies, and a variety of private business owners. Mr. Mintz has represented and counseled clients through all phases and forms of litigation, including pre-litigation resolution, alternative dispute resolution, administrative law proceedings, emergency injunctions, jury trials, and appeals.



**Jacob Oslick** is an associate in the New York office of Seyfarth Shaw LLP, and a member of the Labor & Employment Department. Mr. Oslick has experience in all aspects of labor & employment litigation, including discrimination, retaliation, hostile work environment, and wage-and-hour claims, as well as claims arising from alleged breaches of executive compensation arrangements. Before joining Seyfarth Shaw, Mr. Oslick maintained a diverse commercial litigation practice that, in addition to labor & employment cases, included breach of contract, securities, shareholder derivative, Foreign Sovereign Immunities Act, and internet property matters. Additionally, as a pro bono Special Assistant District Attorney, Mr. Oslick successfully litigated three criminal appeals.



**Eddy Salcedo** is an experienced first-chair trial lawyer and is currently in the New York office of Seyfarth Shaw LLP. He has successfully represented a wide range of clients in trade secret, enforcement of non-competition agreements, partnership disputes, and trademark infringement litigations. He has also served as trial counsel for parties in construction and real estate development disputes, contract disputes, and general commercial and civil litigation. His experience includes state and federal bench and jury trials, appeals and arbitrations. He has appeared as counsel of record in the Appellate Division and the Court of Appeals of New York (New York's highest state court), and the U.S. Court of Appeals for the Second Circuit. Mr. Salcedo is a native Spanish speaker.



# Trading Secrets



**Joshua Salinas** is an attorney in the Los Angeles office of Seyfarth Shaw LLP, practicing in the areas of trade secrets, restrictive covenants, computer fraud, and commercial litigation. Joshua's experience includes the prosecution and defense of trade secret misappropriation and unfair competition claims.



**Scott Schaefers** is a partner in Seyfarth Shaw's Chicago office, where he specializes in commercial litigation, antitrust and trade regulation, and trade secrets and restrictive covenants. He has significant experience in representing clients in a wide range of litigation matters.



**Bob Stevens** is a partner in the Labor and Employment and Trade Secrets, Computer Fraud and Non-Competes Groups of Seyfarth Shaw LLP. He has over 15 years of experience representing public and privately held companies throughout the United States in employment related litigation. He concentrates his practice on litigation and counseling matters involving employment discrimination, restrictive covenant, trade secret, and wage and hour issues.



**Jason Stiehl** is a partner in the Litigation Department of Seyfarth Shaw LLP. Mr. Stiehl represents clients in complex commercial disputes involving trade secrets and restrictive covenants, unfair competition, corporate espionage, contract, and intellectual property claims in both state and federal court. He also has extensive nationwide class action experience, including involvement in multi-district litigation.



**Peter Talibart** is a partner in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP and leads the firm's London office. He is qualified in both Canada and the UK. Mr. Talibart is employment counsel to major multinationals and financial institutions on strategic cross-border employment issues. His expertise is in all aspects of UK and cross-border employment law, in particular corporate restructuring, mergers and acquisitions, corporate governance (employment), financial services compliance and ethical issues.



**John Tomaszewski** is Senior Counsel in the International Data Protection Practice Group. He has significant experience counseling companies regarding data protection and information security throughout the Americas, Europe and Asia. His clients have included a myriad of technology companies as well as financial services, pharmaceuticals, and e-commerce companies of all sizes. John has prepared privacy and security documentation for HR departments, cloud service providers, social media companies, and a host of both traditional "brick-and-mortar" and emerging technology clients. He has also developed fair information practice statements, certification practice statements, PKI policies, non-disclosure agreements, and similar information security and confidentiality instruments.

# Trading Secrets



**Erik Weibust** is a partner in the Litigation Department of Seyfarth Shaw LLP, and is a member of the Securities and Financial Litigation and Trade secrets, Computer Fraud & Non-Competes practice groups. He is also an active member of the firm's national Whistleblower Team.



**Matthew Werber** is an associate in the firm's litigation practice group. His practice focuses primarily on areas of intellectual property litigation and counseling. Mr. Werber has represented some of the world's largest manufacturers and retailers in federal courts, state courts and the U.S. International Trade Commission in litigation matters involving semiconductors, smart phone mobile devices, e-commerce, information systems, software, mechanical devices, water treatment systems and computerized modeling, among other technologies.



**Rebecca Woods** is a partner in the Washington, D.C. office of Seyfarth Shaw LLP. She is a seasoned litigator with trial experience. She also counsels clients on litigation avoidance strategies. As a commercial litigator at heart, her subject matter experience is broad, and includes trade secrets, insurance coverage, business torts, construction litigation and real estate matters.



**James Yu** is a partner in the Litigation and Labor & Employment Departments. He has defended several class action lawsuits, including wage and hour class and collective actions, and is experienced in handling multi-district litigations. He has regularly handled and tried a diverse range of matters, including complex contract disputes, trade secret misappropriation and business tort cases, products liability and toxic tort defense, and several actions defending servicers of commercial mortgage loans involving multi-level debt structures.



# Trading Secrets



## 2013 Summary Posts

- [2013 Trade Secrets Webinar Series – Year in Review](#)  
*By Daniel Joshua Salinas (January 29, 2014)*
- [Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2013](#)  
*By Robert Milligan and Daniel Joshua Salinas (March 6, 2014)*

## Trade Secrets

- [Rankings Of NFL Prospects May Constitute Trade Secrets](#)  
*By Paul Freehling (January 7, 2013)*
- [Department of Justice Issues Report Highlighting Trade Secret Theft Prosecutions And Need For Companies To Vigilantly Protect Their Data](#)  
*By Jessica Mendelson and Robert Milligan (January 9, 2013)*
- [Connecticut Court Has Jurisdiction Over Canadian Defendant Charged With Misappropriation of Canadian Company's Trade Secret Emails](#)  
*By Paul Freehling (January 10, 2013)*
- [3D Printing and Intellectual Property](#)  
*By Joren De Wachter (January 21, 2013)*
- [Ninth Circuit Overturns \\$172 Million Trade Secrets Award in Rival Toy Makers' Epic Dispute](#)  
*By Robert Milligan and Daniel Joshua Salinas (January 25, 2013)*
- [Fashion Designer Resolves "Preppy Clothing" Trade Secrets Dispute](#)  
*By Jessica Mendelson (January 31, 2013)*
- [Aleynikov Case Continues to Grab Headlines in Trade Secrets Community](#)  
*By Jessica Mendelson (February 1, 2013)*
- [Fashion Company Launches Breach of Confidentiality/Unfair Competition Suit Against Former Employee](#)  
*By Jessica Mendelson (February 7, 2013)*
- [Recent California Supreme Court Decision Stokes Debate Over Scope of Trade Secret Preemption](#)  
*By James McNairy (February 5, 2013)*
- [Second Circuit Largely Affirms \\$18.1 Million Trade Secrets Misappropriation Verdict](#)  
*By Scott Schaefer (February 14, 2013)*





# Trading Secrets



- [United States Announces Multifaceted Plan To Combat Trade Secret Theft At Home And Abroad](#)  
*By Jessica Mendelson and Robert Milligan (February 21, 2013)*
- [California Federal Court Allows Non-Signatory to Arbitration Agreement to Compel Arbitration in Trade Secrets Dispute](#)  
*By Paul Freehling (February 25, 2013)*
- [Federal Court Rules That Government's Service Attempts Fail In Criminal Trade Secret Matter](#)  
*By Jessica Mendelson (March 4, 2013)*
- [Nuts and Bolts for Terms Commonly Used in Trade Secret Computer Forensic Investigations](#)  
*By Guest Author Jonathan Karchmer (March 13, 2013)*
- [Preliminary Injunction Issued By Nebraska Federal District Court To Level The Playing Field in Trade Secrets Dispute](#)  
*By Paul Freehling (March 13, 2013)*
- [Trouble in Paradise? Trade Secret Theft Alleged in Hawaii Surrounding Zipline Technology](#)  
*By Robert Milligan and Grace Chuchla (March 15, 2013)*
- [Growing California Trade Secret Preemption Doctrine May Thwart Efforts To Combat Employee Data Theft](#)  
*By Robert Milligan, Jessica Mendelson and Daniel Joshua Salinas (March 28, 2013)*
- [If a Company in China Steals Your Trade Secrets, Do You Have to Litigate Your Lawsuit in China? Maybe...](#)  
*By Randy Bruchmiller (April 12, 2013)*
- [Obama Administration's Request for Public Comment on Trade Secrets Law Underscores Importance for Companies to Protect Their Proprietary Assets Now](#)  
*By Robert Milligan (April 16, 2013)*
- [California Court Tosses Idea Theft Suit Over LOST Television Show Out to Sea](#)  
*By Michael Baniak and Puya Partow-Navid (April 24, 2013)*
- [Illinois Federal Court Issues Preliminary Injunction Prohibiting Use Of Misappropriated Trade Secrets But Rejects Request For Expanded Injunction Based On Alleged "Inevitable Disclosure"](#)  
*By Paul Freehling (April 28, 2013)*
- [Is Your Company's Customer List Still A Trade Secret If Your Company Uses Labeled Delivery Trucks?](#)  
*By Jessica Mendelson (May 4, 2013)*



# Trading Secrets



- [New York State Court Rejects Double Jeopardy Argument In Data Theft Case](#)  
*By Jessica Mendelson (May 10, 2013)*
- [Pennsylvania Appellate Court Orders Sanctions for Plaintiff's Bad-Faith Trade Secret Misappropriation Claims](#)  
*By Scott Schaefer (May 28, 2013)*
- [Hey, I Thought We Had An Agreement: California Appellate Court Allows Party To Seek Attorney's Fees In Trade Secret Case](#)  
*By Mark Hansen (June 6, 2013)*
- [In Setting Genes Free, Supreme Court Decision Will Put Greater Emphasis on Trade Secret Protection in Biotech](#)  
*By Michael Baniak (June 14, 2013)*
- [Foreign Engineer Arrested For Trade Secret Theft Involving Medical Technology](#)  
*By Jessica Mendelson (June 24, 2013)*
- [Obama Administration Issues Joint Strategic Plan To Protect America's Intellectual Property](#)  
*By Misty Blair (June 29, 2013)*
- [An Employee Is Stealing Company Documents...That Can't Be Protected Activity, Right?](#)  
*By Robert Milligan (July 3, 2013)*
- [Words Matter: Your Non-Disclosure Agreement May Trump Governing Trade Secret Law](#)  
*By Jason Stiehl (July 12, 2013)*
- [Are Sunny Skies Ahead for Plaintiff After Clearing An Early Hurdle in A Trade Secret Case Involving Weather Service?](#)  
*By Jessica Mendelson (July 25, 2013)*
- [Pennsylvania Federal Court Affirms Broad Pleading Standard for Uniform Trade Secrets Act and Ability to Plead Preempted Claims in the Alternative](#)  
*By Rebecca Woods (July 26, 2013)*
- [Conversion Claim for Theft of Confidential Information Not Preempted By Trade Secrets Act](#)  
*By Robert Milligan (August 4, 2013)*
- [California Federal Court Finds Specific Jurisdiction Over South Dakota Company For Alleged Involvement in Misappropriation of Trade Secrets](#)  
*By Daniel Joshua Salinas (August 12, 2013)*
- [U.S. Senators Propose Legislation To Strengthen Federal Criminal Trade Secret Laws](#)  
*By Robert Milligan (August 13, 2013)*



# Trading Secrets



- [Best Practices and Latest Developments in Trade Secret Law](#)  
*By Robert Milligan (August 27, 2013)*
- [Court Awards Attorney's Fees for "Bad Faith" Trade Secret Misappropriation Claim](#)  
*By Erik von Zeipel (September 5, 2013)*
- [What's for Lunch? Trade Secrets!](#)  
*By Jessica Mendelson (September 9, 2013)*
- [Are the Last Episodes of "Breaking Bad" Trade Secrets?](#)  
*By Jessica Mendelson (September 11, 2013)*
- [Careful, that Slice of Pizza You're Eating Might Be Full of Trade Secrets...](#)  
*By Jessica Mendelson (September 30, 2013)*
- [Federal Court Rules Trade Secret Misappropriation Sufficiently Alleged Based on Improper Acquisition, Even in Absence of Use or Disclosure](#)  
*By Erik von Zeipel (October 8, 2013)*
- [Judgment on Willful And Malicious Trade Secret Claim Is Not Dischargeable In Bankruptcy](#)  
*By Paul Freehling (October 9, 2013)*
- [Neglect of Cloud Computing Policies In Workplace Can Provide Perfect Storm for Trade Secret Theft](#)  
*By Robert Milligan, Jessica Mendelson and Daniel Joshua Salinas (October 10, 2013)*
- [Federal Appellate Court Finds Motion To Enjoin Disclosure Of Confidential Information Should Not Be Denied Merely Because The Same Information Could Have Been Acquired Lawfully](#)  
*By Paul Freehling (October 28, 2013)*
- [The Romance of Trade Secrets: Competing Speed Dating Companies Engaged in Trade Secret Misappropriation Battle](#)  
*By Jessica Mendelson (November 5, 2013)*
- [A Whale of A Trade Secret. . . Or Not?](#)  
*By Jessica Mendelson (December 4, 2013)*
- [Protected Status Of Trade Secrets May Be Lost By Not Insisting On Confidentiality](#)  
*By Paul Freehling (December 11, 2013)*

## Computer Fraud and Abuse Act

- [Computer Fraud and Abuse Act Circuit Split Remains Unresolved: United States Supreme Court Challenge Dismissed](#)  
*By Robert Milligan (January 7, 2013)*



# Trading Secrets



- [Computer Fraud and Abuse Act Claims Subject to Heightened Pleading Requirements](#)  
*By Jessica Mendelson (January 14, 2013)*
- [Activist's Death May Spur Legislative Changes To The Computer Fraud and Abuse Act](#)  
*By Jessica Mendelson and Robert Milligan (January 16, 2013)*
- [Computer Activists Take Over Sentencing Commission Website](#)  
*By Jessica Mendelson (February 2, 2013)*
- [Missouri Federal Court Finds Violations of Employment Agreement May Constitute Unlawful Access Under the Computer Fraud and Abuse Act](#)  
*By Paul Freehling and Daniel Joshua Salinas (February 6, 2013)*
- [North Carolina Federal Court Uses Computer Fraud and Abuse Act Claim to Exercise Supplemental Jurisdiction Over State Law Claims Against Former Employee and her New Employer](#)  
*By Paul Freehling (March 20, 2013)*
- [Recent California Federal Court Rulings Muddy the Interpretation of the Computer Fraud and Abuse Act](#)  
*By Paul Freehling (March 28, 2013)*
- [The Computer Fraud and Abuse Act and Disloyal Employees: A Narrow Bridge To Nowhere](#)  
*By Gary Glaser and Jacob Oslick (April 15, 2013)*
- [Employee Data Theft and Corporate Hacking Studies Point to Need for Additional Federal Trade Secrets Legislation](#)  
*By Robert Milligan (April 22, 2013)*
- [Corporate Recruiter Convicted of Computer Fraud and Trade Secret Theft By San Francisco Jury](#)  
*By Robert Milligan and Daniel Joshua Salinas (April 29, 2013)*
- [California Federal Court Dismisses Computer Fraud and State Unfair Competition Claims Alleged Against Ex-Employees Accused Of Stealing Computer Source Code](#)  
*By Paul Freehling (May 6, 2013)*
- [No Damages? Illinois Federal Court Tosses Computer Fraud and Abuse Act Claim Alleging Hacking of Law Firm Network](#)  
*By Paul Freehling (May 13, 2013)*
- [Recent Alleged Cyberattack By Ex-Employee Demonstrates Importance of Employer Diligence On Protecting Network Passwords](#)  
*By Robert Milligan and Grace Chuchla (June 3, 2013)*



# Trading Secrets



- [Minnesota Federal Court Dismisses Computer Fraud and Abuse Act Claim Based on Departing Employee's Downloading of Customer List](#)  
*By Erik von Zeipel (June 17, 2013)*
- [Massachusetts Federal Court Narrowly Construes Computer Fraud and Abuse Act and Holds That Company Cannot Sue Former Employees For Downloading Proprietary Information Absent Showing of Fraud](#)  
*By Erik Weibust and Ryan Malloy (June 25, 2013)*
- [Significant Amendments Proposed to the Computer Fraud and Abuse Act to Limit Its Use to Traditional Hacking Scenarios](#)  
*By Robert Milligan and Grace Chuchla (June 26, 2013)*
- [Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part I](#)  
*By Erik von Zeipel (August 29, 2013)*
- [Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part II](#)  
*By Erik von Zeipel (August 30, 2013)*
- [Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part III](#)  
*By Erik von Zeipel (September 3, 2013)*
- [Computer Fraud And Abuse Act Violated By Bundling Facebook And Other Social Networking Accounts Without Authorization](#)  
*By Paul Freehling (October 7, 2013)*
- [Whatever Happened to Detention? Principal Sues Students Under Computer Fraud and Abuse Act For Allegedly Creating Fake Social Media Account](#)  
*By Jessica Mendelson (October 25, 2013)*

## Non-Competes & Restrictive Covenants

- [To Work or Not to Work – Maryland's Senate Considers Changes To Non-Compete Law for Those on Unemployment](#)  
*By Scott Schaefer (January 17, 2013)*
- [California Appellate Decision Clarifies Standard for Injunctive Relief Carve-Outs Within California Arbitration Agreements](#)  
*By Robert Milligan (January 22, 2013)*



# Trading Secrets



- [Massachusetts Legislators Introduce “Noncompete Agreement Duration Act”](#)  
*By Erik Weibust and Ryan Malloy (January 29, 2013)*
- [Federal Trade Commission Removes Bleach Companies’ Non-Compete Agreement](#)  
*By Jessica Mendelson (January 30, 2013)*
- [California Federal Court Ships Fiduciary Duty and Unfair Competition Suit to Delaware Based Upon Forum Selection Clause](#)  
*By Robert Milligan and Grace Chuchla (January 31, 2013)*
- [California Federal Court Dismisses California Employee’s Challenge Of His Non-Compete Agreement Based Upon Enforceable Forum Selection Provision](#)  
*By Robert Milligan and Grace Chuchla (February 12, 2013)*
- [New York Federal Court Denies Injunction to Enforce Restrictive Covenants Against Terminated Employee](#)  
*By Paul Freehling (February 13, 2013)*
- [Federal Court Requires Foreign Resident To Litigate Non-Compete Dispute in Missouri Based Upon Forum Selection Clause](#)  
*By Robert Milligan and Grace Chuchla (February 26, 2013)*
- [California Style Non-Compete Legislation Introduced In Minnesota](#)  
*By Justin Beyer (March 14, 2013)*
- [Massachusetts Governor Weighs In On Non-Compete Reform Debate](#)  
*By Ryan Malloy (March 14, 2013)*
- [Illinois Legislator Proposes Unique Employment Noncompete Agreement Act](#)  
*By Paul Freehling (March 19, 2013)*
- [Protecting Company Information When Employees Bail: California Alternatives to Employee Non-Compete Agreements](#)  
*By Robert Milligan, Jessica Mendelson and D. Joshua Salinas (March 22, 2013)*
- [New Jersey Legislators Propose Banning Non-Compete Agreements With Employees Who Can Claim Unemployment](#)  
*By Robert Milligan and Jessica Mendelson (April 9, 2013)*
- [New Jersey Appellate Court Affirms No Damages Award Against Individual Defendants In Non-Compete Case](#)  
*By Paul Freehling (April 26, 2013)*



# Trading Secrets



- [Non-Compete Legislation Proposed in Connecticut](#)  
*By Jessica Mendelson (May 25, 2013)*
- [Illinois Appellate Court Partially Reverses Broad Non-Compete Injunction Against Physicians](#)  
*By Molly Joyce (May 29, 2013)*
- [New Oklahoma Law Clarifies Enforceability of Non-Solicitation of Employee Covenants](#)  
*By Daniel Joshua Salinas (May 30, 2013)*
- [Massachusetts Federal District Court Rules That Initiating Contact Not Necessary For Finding of Solicitation In Breach of Customer Non-Solicitation Agreement](#)  
*By Erik Weibust and Ryan Malloy (June 4, 2013)*
- [Massachusetts Case Demonstrates Benefit of “Material Change in Employment” Clause in Non-Compete Agreement](#)  
*By Erik Weibust and Ryan Malloy (June 10, 2013)*
- [Pleading Former Employer’s Breach Of Employment Contract: Affirmative Defense Or Counterclaim To Suit For Violating Non-Compete And Non-Solicitation Covenants?](#)  
*By Paul Freehling (June 11, 2013)*
- [Wyoming Supreme Court Upholds Non-Compete Prohibiting Sale of Booze At Bowling Alley](#)  
*By Paul Freehling (June 18, 2013)*
- [Doc Rivers: Will He Stay or Will He Go to La La Land](#)  
*By Erik Weibust (June 21, 2013)*
- [Connecticut Legislature Passes Non-Compete Legislation](#)  
*By Daniel Hart (July 1, 2013)*
- [Illinois Appellate Court Rules That Employment For Less Than Two Years Is Inadequate Consideration For Enforcement Of Non-Compete And Non-Solicitation Covenants](#)  
*By Paul Freehling (July 2, 2013)*
- [Connecticut Governor Vetoes Noncompetes Statute Passed By Legislature](#)  
*By Daniel Hart (July 16, 2013)*
- [Material Change Defense To Non-Compete Enforcement Gaining Acceptance In Massachusetts](#)  
*By Erik Weibust (July 17, 2013)*



# Trading Secrets



- [You've Already Signed Your Offer Letter– Can You Still Be Subject to a Non-Compete Agreement Signed at the Inception of Employment Without New Consideration? Pennsylvania Supreme Court Says Yes](#)  
*By Jessica Mendelson (July 18, 2013)*
- [Comply or Lose: New York Affirms Enforcement of Non-Compete in Rescission Action for Employee Equity Grants](#)  
*By Marcus Mintz (July 19, 2013)*
- [Even Preparing To Compete In Texas May Be Prohibited During A Non-Competition Covenant Period](#)  
*By Paul Freehling (July 22, 2013)*
- [Physician Noncompetition Agreements May Be Challenged More Often After Recent Texas Appellate Decision](#)  
*By Randy Bruchmiller (July 23, 2013)*
- [Massachusetts Non-Compete Legislative Update](#)  
*By Erik Weibust (July 24, 2013)*
- [Employment Agreement Mandating Arbitration With Exclusion To Seek Equitable Relief From Court For Non-Compete Violations Found Unconscionable](#)  
*By Paul Freehling (July 29, 2013)*
- [Georgia Court Rules That Non-Compete Does Not Bind Seller's Agents](#)  
*By Paul Freehling (August 2, 2013)*
- [New Hampshire Court Voids Non-Compete Clause in Independent Contractor Agreement](#)  
*By Paul Freehling (August 21, 2013)*
- [Missouri Federal Court Finds Forfeiture-For-Competition Provision in Stock Option Agreement Enforceable](#)  
*By Paul Freehling (September 4, 2013)*
- [Is Massachusetts Inching Closer to California? Governor Deval Patrick Issues Public Support for the "Outright Elimination" of Non-Compete Agreements](#)  
*By Erik Weibust (September 10, 2013)*
- [Referring Former Employer's Customers To New Employer Held Violation Of Injunction, Resulting In Finding Of Criminal Contempt](#)  
*By Paul Freehling (September 12, 2013)*





# Trading Secrets



- [First Circuit Holds that Solicitation is Barred by Non-Compete Agreement Regardless of Who Initiates Contact](#)  
*By Erik Weibust (September 24, 2013)*
- [Federal Appellate Court Lacks Jurisdiction To Hear Appeal of Expired Non-Compete Preliminary Injunction](#)  
*By Paul Freehling (October 2, 2013)*
- [How Do I Get a TRO Against a Former Employee If Arbitration in FINRA Is Mandatory?](#)  
*By Nicholas De Baun (October 4, 2013)*
- [Virginia Supreme Court Rules Enforceability of Non-Competes Cannot Be Determined in a Factual Vacuum](#)  
*By Sarah Izfar (October 14, 2013)*
- [Illinois Supreme Court Won't Take Up Non-Compete Case, Adequate Consideration Questions Remain](#)  
*By Michael Wexler (October 18, 2013)*
- [13 Scary Years Ago Court Issued Death Sentences In Horrid Dispute Over Vampire Fangs.](#)  
*By Erik von Zeipel (October 30, 2013)*
- [Top Five Trends in Georgia Restrictive Covenants Law Three Years After Constitutional Amendment](#)  
*By Bob Stevens and Daniel Hart (November 11, 2013)*
- [Georgia Federal Court Disregards Forum Selection Clause In Non-Compete And Non-Solicitation Covenant Dispute](#)  
*By Paul Freehling (November 12, 2013)*

## Legislation

- [Employers Take Note: Michigan Adopts Social Media Privacy Legislation](#)  
*By Robert Milligan and Jessica Mendelson (January 8, 2013)*
- [President Obama Signs Economic Espionage Act Amendments That Significantly Enhance The Penalties For Trade Secret Theft By Foreigners](#)  
*By Robert Milligan (January 15, 2013)*
- [President Obama Signs Significant Cybersecurity Executive Order](#)  
*By Misty Blair and Ken Wilton (February 15, 2013)*
- [Is Massachusetts Next to Adopt the Uniform Trade Secrets Act?](#)  
*By Ryan Malloy (February 20, 2013)*



# Trading Secrets



- [Texas Considers Adopting the Uniform Trade Secrets Act](#)  
*By Randy Bruchmiller (March 12, 2013)*
- [Federal Legislation Proposed To Combat Cyber-Espionage](#)  
*By Jessica Mendelson (June 14, 2013)*
- [Representative Zoe Lofgren Introduces Bill to Create Private Civil Claim for Trade Secrets Theft Under the Economic Espionage Act](#)  
*By Daniel Joshua Salinas and Robert Milligan (June 26, 2013)*
- [Texas Uniform Trade Secrets Act Now Applicable](#)  
*By Randy Bruchmiller (September 2, 2013)*
- [Texas Changes Law To Strengthen The Ability Of Companies To Protect Their Information](#)  
*By Randy Bruchmiller (September 18, 2013)*
- [Obama Administration Releases Draft Voluntary Cybersecurity Framework for U.S. Business](#)  
*By John Tomaszewski (October 28, 2013)*

## International

- [International Update: Recent Decisions by UK Courts Highlight Protection of Confidential and Proprietary Information in Employment Context — Part I](#)  
*By Daniel Hart, Peter Talibart and Georgina McAdam (August 5, 2013)*
- [International Update: Recent Decisions by UK Courts Highlight Protection of Confidential and Proprietary Information in Employment Context — Part II](#)  
*By Daniel Hart, Peter Talibart and Georgina McAdam (August 6, 2013)*
- [A New and Potentially Powerful Weapon Against Foreign Counterfeiters and Pirates](#)  
*By Erik von Zeipel (August 20, 2013)*
- [AMSC/Sinovel Industrial Espionage Thriller Takes a Procedural Detour, Threatening U.S. Criminal Prosecution](#)  
*By Justin Beyer (September 9, 2013)*
- [U.S. Counsels Cross-Border Consistency In Criminal Consequences For Trade Secret Theft](#)  
*By Mark Hansen (October 3, 2013)*
- [Two Former Eli Lilly Scientists Accused of Stealing \\$55 Million in Trade Secrets on Behalf of Chinese Pharmaceutical Company In Southern District of Indiana Indictment](#)  
*By Justin Beyer (October 28, 2013)*



# Trading Secrets



- [Sino Legend Urges U.S. International Trade Commission \(ITC\) to Consider Parallel Chinese Court Proceeding in Ongoing Trade Secret Litigation Brought by SI Group](#)  
*By Matthew Werber (November 11, 2013)*

## Social Media

- [Hands Off My Tweets: Washington State Senate Proposes Ban on Mandatory Disclosure of Employee Social Networking Passwords](#)  
*By Scott Schaefer (February 6, 2013)*
- [Federal Court Rules That Twitter Invites and Facebook Posts Do Not Constitute Impermissible Employee Solicitations](#)  
*By Justin Beyer (February 19, 2013)*
- [Federal Court Questions Whether Damages Exist in LinkedIn Account Ownership Dispute](#)  
*By Jessica Mendelson and Robert Milligan (March 2, 2013)*
- [New Jersey Poised To Adopt New Social Media Legislation](#)  
*By Jessica Mendelson (April 1, 2013)*
- [Court Issues Decision in Eagle v. Morgan: Employee Owns LinkedIn Account But Fails To Recover Any Damages Against Former Employer](#)  
*By Jessica Mendelson and Robert Milligan (April 3, 2013)*
- [Federal Court Allows Service On Foreign Defendants Through Facebook](#)  
*By Jessica Mendelson (April 18, 2013)*
- [Utah, New Mexico, and Arkansas Pass Social Media Legislation Restricting Employer Access to Personal Social Media Accounts](#)  
*By Robert Milligan and Jessica Mendelson (April 23, 2013)*
- [New Jersey Federal Court Issues Sanctions For Deletion of Facebook Profile](#)  
*By Jessica Mendelson and Grace Chuchla (April 30, 2013)*
- [New Jersey Assembly Passes Revised Employee Social Media Privacy Bill](#)  
*By Guest Authors Carlos Lopez, Caroline Keller and Chris Lower (May 20, 2013)*
- [Washington State Passes Social Networking Privacy Legislation](#)  
*By Scott Schaefer (May 27, 2013)*
- [Mobile Device Forensics – Are You in the Know?](#)  
*By Guest Authors James Whitehead and Arnold Garcia (June 5, 2013)*
- [Illinois Passes Social Media Legislation To Regulate Flash Mobs](#)  
*By Jessica Mendelson (June 7, 2013)*



# Trading Secrets



- [Oregon the Latest State to Pass Social Networking Privacy Legislation; Vermont Establishes Committee to Study and Recommend Such Legislation](#)  
*By Scott Schaefers (June 7, 2013)*
- [Nevada and Colorado Pass Employee Social Networking Privacy Laws](#)  
*By Scott Schaefers (July 1, 2013)*
- [New Jersey Becomes the Thirteenth State to Pass Employee Social Networking Privacy Legislation](#)  
*By Scott Schaefers (August 30, 2013)*
- [Nevada District Court Finds No Reasonable Expectation of Privacy in Private Twitter Posts](#)  
*By Erik von Zeipel (September 10, 2013)*
- [California Legislature Passes Bill To Extend Social Media Privacy Laws To Public Employers](#)  
*By Robert Milligan (September 17, 2013)*
- [District Court of New Jersey Continues Growing National Trend Permitting Employers to View "Publicly" Available Social Media Posts](#)  
*By Justin Beyer (September 19, 2013)*
- [Fourth Circuit Holds That Facebook "Like" Is Protected by the First Amendment](#)  
*By Jessica Mendelson (September 20, 2013)*
- [When does LinkedIn Activity Violate Non-Solicitation Agreements?](#)  
*By Erik von Zeipel (November 4, 2013)*
- [Massachusetts Judge Rules That Updating LinkedIn Does Not Constitute Solicitation](#)  
*By Erik Weibust (November 20, 2013)*



# Trading Secrets



## 2013 Summary Posts

# Trading Secrets



## 2013 Trade Secrets Webinar Series – Year in Review

*By Daniel Joshua Salinas (January 29, 2014)*

Throughout 2013, Seyfarth Shaw LLP's dedicated hosted a series of CLE webinars [Trade Secrets, Computer Fraud & Non-Competes Practice Group](#) that addressed significant issues facing clients today in this important and ever changing area of law. The series consisted of 12 webinars:



1. 2012 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law
2. Trade Secrets in the Telecommunications Industry
3. Employee Privacy and Social Networking: Can Your Trade Secrets Survive?
4. How the America Invents Act Increases the Importance of Trade Secrets
5. Protecting Confidential Information and Client Relationships in the Financial Services Industry
6. Trade Secret and Non-Compete Legislative Update
7. The Big Data Revolution: How Big Data Impacts Trade Secret, Computer Fraud and Privacy
8. Trade Secret and Non-Compete Considerations in Asia
9. How and Why California Is Different When It Comes To Trade Secrets and Non-Competes
10. Trade Secrets in the Pharmaceuticals Industry
11. My Company's Confidential Information is Posted on the Internet! What Can I Do?
12. The Stakes Just Got Higher: Criminal Prosecution of Trade Secret Misappropriation

As a conclusion to this well-received 2013 webinar series, we compiled a list of key takeaway points for each of the webinars, which are listed below. For those clients who missed any of the programs in this year's webinar series, the webinars are available on CD upon request or you may click on the title listed below for each webinar to access the online recording. We are also pleased to announce that Seyfarth will continue its trade secrets webinar programming in 2014 and has several exciting topics lined up. We will release the 2014 trade secrets webinar series schedule in the coming weeks.

### [2012 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law](#)

The first webinar of the year, led by Michael Wexler, Robert Milligan and Joshua Salinas reviewed noteworthy cases and other legal developments from across the nation from 2012 in the areas of trade secrets and data theft, non-compete enforceability, computer fraud, and company owned social media accounts and social media policies, as well as provided predictions for what to watch for in 2013.



# Trading Secrets



- As government agencies are becoming more active in the areas of trade secret law, such as the FBI's initiative to curb the growing rise of trade secret and other intellectual property theft, high profile prosecutions under the Economic Espionage Act, and the National Labor Relations Board's increased scrutiny of employers' social media policies, employers should consider these government agencies' reports and memoranda when analyzing and revising company policies and practices.
- Disputes over the ownership of company social media accounts and account "followers" involving Twitter, LinkedIn, Facebook, and Myspace illustrate the necessity for employers to have social media ownership agreements with their employees when utilizing company social media accounts to conduct business.
- Trade secret preemption remains a significant issue in many jurisdictions as courts grapple with whether the theft of non-trade secret information is actionable in tort and, thus, claimants should consider, before filing any pertinent pleadings, the existence of any potential alternative theories for their non-trade secret claims (and any corresponding support thereof), and then draft the pleadings such that it is clear that the alternative theories are distinct from a misappropriation of information theory.

## *Trade Secrets in the Telecommunications Industry*

In our second webinar of the series, Justin Beyer, Mark Hansen and James McNairy addressed the role that trade secrets play in the telecommunications industry.

- Due to the nature of the telecommunications industry, information tends to be quite portable (for example, courts have held the following constitute trade secrets: search index and query logs of Google; telephone company's electronic database containing customer information; elements of technology for DVD encryption system; and product descriptions for international telephone switching system), and companies need to be forever diligent in protecting that information from employee misappropriation, particularly through use of external storage devices and smart phones.
- Telecomm trade secrets also take somewhat unique forms such as infrastructure and wireless hardware technologies, as well as future programming. Given these somewhat industry-specific trade secrets, companies should be consistent in entering into non-disclosure or confidentiality agreements with any employees exposed to such projects as well as entering into invention assignment agreements to ensure there is no concern over disclosure or question of ownership.
- As more and more companies utilize social media through Twitter, Instagram, and Facebook, for example, companies need to design and develop policies as to who owns the account, what to do when the employee who manages the account leaves, and policies for account usage. In the long-run, requiring employees to enter into contracts regarding social media usage is likely cheaper than litigation over these questions. But, in crafting such policies, it is important to be mindful of NLRB policies and opinions, as well as any state-specific statutes and regulations concerning social media.



# Trading Secrets



## [Employee Privacy and Social Networking: Can Your Trade Secrets Survive?](#)

The third installment of the series was presented by Gary Glaser, Scott Schaefer and Jessica Mendelson as they discussed the relationship between trade secrets and social media.

- For social networking sites (e.g., LinkedIn, Twitter), have clear written policies that spell out what company information may/may not be posted on such sites, and identify what information belongs to the company (e.g., contact lists, company photos or graphics, etc.), as well as a process for purging the company-owned information from their contact lists posted on social networking sites such as LinkedIn at the time the employee departs (but remember that LinkedIn contact lists can generally be downloaded and copied by the exiting employee once they know they are leaving the company). One should strongly consider using ownership agreements that specify that the company owns the particular social media accounts that the employee may use for networking or use for other business-related purposes, and remember to include in the agreement or the company's social media policy that the employee has an obligation to provide their password to the company and notify the company if/when they change the password, and that the company has the right to obtain the password from the employee to the company-owned social media account before the employee leaves. (But check to make sure that you are not in a state that has passed a social media privacy law that would prohibit such requirement – *see below*.)
- An exit interview should also be conducted at the time any employee separates, and as part of that exit interview process, each exiting employee should be given a written reminder of their ongoing trade secret, confidentiality and social networking obligations, and should be asked to sign the reminder acknowledging receipt and their agreement to comply with such obligations. If an employee leaves the company without such clear written direction, the company risks waiving a proprietary interest in the information in his/her LinkedIn or other social media.
- State social media legislation has become increasingly common in the United States. Issues related to social media privacy in the workplace are not going away and we expect to see more litigation and legislation to define acceptable practices in this area. In light of this uncertainty, employers should determine whether their company has employees in any of the states that have adopted or are planning on adopting social media privacy laws in order to ensure compliance with such laws. Employers should also be aware that state laws may restrict requests for information about such activity. Counsel should review the applicable state social media access law before asking an employee for any account-related information. Additionally, employers should not overlook social media evidence in conducting employee investigations and in employee lawsuits but make sure that your company's review and access of such information does not violate applicable law.

## [How the America Invents Act Increases the Importance of Trade Secrets](#)

The fourth webinar in the series, presented by Michael Baniak, James McNairy and Joseph Walker, deliberated how the America Invents Act (AIA) impacts the value of trade secret and patent protection, and what the implications may be for technology innovators.





# Trading Secrets



- Neither trade secret nor patent protection will be available if the information/idea/innovation is disclosed to the public (failure to maintain secrecy destroys trade secret status; as to patents, patentability is lost if the innovation is disclosed by the inventor and more than a year goes by). Thus, it is never too early to create a culture of confidentiality within your organization.
- Questions bearing on whether trade secret or patent protection may be more advantageous include: Does innovation have value that may go beyond 20-year patent term (if so, perhaps trade secret protection is desirable)? Is the innovation susceptible to reverse engineering (if yes, perhaps patent protection is more advisable)? Can reasonable steps to preserve secrecy be implemented? Implemented indefinitely? Can the owner of the innovation make more money from the innovation as a trade secret or patent?
- The America Invents Act's expansion of the prior commercial use defense and continual use requirement to patent types beyond business method patents creates a greater likelihood that more innovations will be protected as trade secrets, and for longer periods of time, than prior to enactment of the AIA.

## *Protecting Confidential Information and Client Relationships in the Financial Services Industry*

The fifth webinar in the 2013 series was presented by Scott Humphrey, Dan Lanciloti and Jason Stiehl and focused on trade secret and client relationship considerations in the banking and finance industry, with a particular focus on a firm's relationship with its FINRA members.

- Enforcement of restrictive covenants and confidentiality obligations for FINRA and non-FINRA members are different. Although FINRA allows a former employer to initially file an injunction action before both the Court and FINRA, FINRA, not the Court, will ultimately decide whether to enter a permanent injunction and/or whether the former employer is entitled to damages as a result of the former employee's illegal conduct.
- Address restrictive covenant enforcement and trade secret protection before a crisis situation arises. An early understanding of the viability of your restrictive covenants and the steps that you have taken to ensure that your confidential information remains confidential will allow you to successfully and swiftly evaluate your legal options when a crisis arises.
- Understand the Protocol for Broker Recruiting's impact on your restrictive covenant and confidentiality requirements. The Protocol significantly limits the use of restrictive covenants and allows departing brokers to take client and account information with them to their new firm.

## *Trade Secret and Non-Compete Legislative Update*

The sixth webinar of the year, led by Bob Stevens, Erik Weibust and Dan Hart, focused on new and pending legislative changes to non-compete, trade secret and social media laws, including recent and pending legislative changes to state restrictive covenant laws; recent and proposed statutory changes to trade secret laws, incorporating the proposed national trade secret law; and the avalanche of social media laws proposed and passed in state houses throughout the United States in 2013.



# Trading Secrets



- To the extent employers have not already done so, they should re-evaluate their restrictive covenant agreements in states, which are considering or who have enacted new or revised restrictive covenant laws in 2013 including New Jersey, Massachusetts, New Hampshire, Illinois, Minnesota and Maryland.
- With respect to the protection of employers' trade secrets, employers should not only remain vigilant in their efforts to protect their trade secrets by using the tools at their disposal such as non-disclosure agreements and password protection, but they should also remain aware of their current and proposed legal remedies including the proposed federal trade secret statute – "Protecting American Trade Secrets and Innovation Act of 2012"; the White House's 5-Point Plan intended to combat American trade secret theft; and state trade secret statutes including the new law in Texas and the proposed statute in Massachusetts.
- Given the lightning quick evolution of social media laws on a state-by-state basis, enacted by different states at times throughout 2013 on almost a weekly if not monthly basis, employers need to ensure that they have policies in effect to comply with the state's patchwork of social media laws. Depending on the state or states that an employer operates its business, it needs to ensure that its employment, labor and trade secret policies and practices do intentionally or inadvertently violate one of the newly minted laws by taking or permitting newly illegal actions such as requesting employees' passwords to their social media accounts or taking an adverse action based on the employees' refusal to provide access to such an account.

## [The Big Data Revolution: How Big Data Impacts Trade Secret, Computer Fraud and Privacy](#)

The seventh webinar in our series, presented by Robert Milligan, John Tomaszewski and Joshua Salinas, along with Anthony Wong a renowned IP and IT expert from AGW Consulting in Australia, discussed how the Big Data Revolution created a new age of discovery and opportunity by equipping companies with tools to derive valuable insight from once unnavigable oceans of data.

- Privacy isn't going away. Understanding how to manage data collection, use, and distribution is becoming more and more critical to the viability of businesses. Be clear on what you are going to do with the data you collect - especially if it is from a third party data source. When the data subject doesn't expect you to use data about them in a certain way, that use creates risks.
- "Do No Harm." While this was Google's mantra, it works for everyone else. If the use of big data or analytics has an adverse effect on a person, the risk of liability being realized increases. Make sure you understand the "unintended consequences" of using big data analytics - you may inadvertently discriminate against a protected class.
- Don't rely on anonymization alone as a privacy protection. Data, by itself, isn't actionable. When it comes into contact with other data, it transforms into information - which *is* actionable. Information is what is protected (not raw data). Since anonymization seeks to decouple data points so that they stop being "information," any "recoupling" may end up destroying the anonymization. Also remember, context is data as well. Where data comes from is just as valuable (sometimes *more* valuable) than the discrete data point itself.



# Trading Secrets



- Good privacy is like good security - it's context-based, and requires a "defense in depth" mentality. There is no "silver bullet," or one answer. Privacy programs need to be flexible and contextually oriented, so that they can keep up with business without strangling business.

## *Trade Secret and Non-Compete Considerations in Asia*

The eighth installment was led by Wan Li, Dominic Hodson, Robert Milligan and Leon Mao as they focused on non-compete and trade secret considerations from an international perspective. Specifically, the webinar involved a discussion of non-compete and trade secret issues in China, which included best practices to protect trade secrets and confidential information in the country. The similarities and differences in approach among China and other Asian countries or provinces were touched upon and compared to the United States. This webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these regions and ensure protection of their trade secrets and confidential information, including the effective use of non-compete and non-disclosure agreements.

- Legal systems differ widely across Asia and courts and other forms of legal redress do not always provide a predictable outcome, particularly in developing and emergent economies. It is particularly important for companies to take proactive practical steps to protect themselves from misuse of their trade secrets because legal remedies may be of little help.
- One Chinese court has recently ruled, for the first time, in favor of the company to ban the circulation of trade secrets by a former employee. Future cases may be judged based on such milestone, but prevention is always better than cure.
- In China, non-compete duties shall be imposed on employees with specific positions and within limited time period. Compensation is required, otherwise the non-compete duties may be determined null and void by the court.

## *How and Why California Is Different When It Comes To Trade Secrets and Non-Competes*

The ninth webinar this year, presented by Mark Hansen, James McNairy and Jessica Mendelson, discussed the ways in which California trade secret law is similar to and diverse from other jurisdictions, including the California Uniform Trade Secrets Act, trade secret identification requirements, remedies, and the interplay between trade secret law and Business & Professions Code Section 16600, which codifies California's general prohibition of employee non-compete agreements.

California Code of Civil Procedure section 2019.210 requires that, prior to commencing discovery, trade secret Plaintiffs describe with reasonable particularity the information claimed to be trade secret and misappropriated by defendant.

- Because preemption (or "supersession") under California's Uniform Trade Secrets Act increasingly is invoked by defendants as a basis to dismiss claims related to the taking of trade secret information, it is imperative that potential plaintiffs plead carefully non-trade secret claims as distinct from the trade secret allegations within the complaint. Failure to do so can



# Trading Secrets



cause related claims to be preempted, resulting in their dismissal. And, if the trade secret claim itself is faulty, it too may be dismissed, potentially resulting in dismissal of the entire lawsuit.

- Create a culture of confidentiality within your company so that at every turn employees are aware of the importance of protecting confidential, proprietary, and trade secret information and the steps required of all employees to protect the company's information assets. Doing so may help moderate high employee mobility in California.
- When trying to invoke California Business & Professions Code Section 16601's "sale of business" exception to California's general prohibition against contractual provisions that impair employee mobility and competition, such non-competition provisions should be incorporated into the terms of the purchase agreements (as opposed to stand alone but related employment agreements) and reflect a clear purpose to protect business goodwill. Reasonable and limited non-compete provisions may also be enforced in connection with the dissolution of a partnership or a limited liability corporation.
- Recently, federal courts in California have exhibited a willingness to enforce forum selection provisions in employment contracts requiring California-based employees to litigate the enforceability of non-compete provisions in states other than California. Doing this increases the likelihood that the non-compete provision will be enforced against the California employee by an out-of-state court despite California's strong public policy to the contrary. California state courts continue to look beyond forum selection clauses, applying choice of law principles which usually result in the application of California law and thus the invalidation of the non-compete provision.

## *Trade Secrets in the Pharmaceuticals Industry*

The tenth installment in our 2013 series, led by Justin Beyer, Scott Schaefer and Shashank Upadhye, focused on trade secrets in the pharmaceutical industry.

- Require NDAs and IP-ownership agreements of all key participants at each and every step of the R&D and clinical-trial process.
- Re-visit your R&D security measures (restricted access to campus; limited, need-to-know permissions to R&D files; periodic reminders of confidentiality restrictions and policies).
- Consider law-enforcement assistance against egregious misappropriation and NDA breaches, especially if the time has passed for emergency injunctive relief, or if you have jurisdictional issues regarding defendant's residence.

## *My Company's Confidential Information is Posted on the Internet! What Can I Do?*

The eleventh webinar was led by Paul Freehling, Scott Humphrey and Jeffrey Swatzell, and involved a high-level discussion about the steps and responses companies should take when their confidential information and/or trade secrets appear, or are threatened to appear, on the internet.



# Trading Secrets



- The Uniform Trade Secrets Act most likely applies to any misappropriation of your trade secrets. Under the Act, a “trade secret” is confidential information that (i) has independent economic value; (ii) is not generally known or readily ascertainable by proper means; and (iii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
- Do not wait until after a crisis arises; address trade secret protection before information is misappropriated.
- If your trade secrets are misappropriated and posted on the Internet or social media, but you don’t know who did the posting, you may be able to identify that person by demanding the information in a subpoena served on the Internet service provider or host of the social media site.

## *The Stakes Just Got Higher: Criminal Prosecution of Trade Secret Misappropriation*

In Seyfarth’s final installment of its 2013 Trade Secret Webinar series, attorneys Michael Wexler, Molly Joyce and Justin Beyer presented on criminal liability for trade secret misappropriation.

- Private companies can investigate misappropriation claims and provide information to authorities for purposes of prosecuting Economic Espionage Act and/or Computer Fraud & Abuse Act claims, but be certain to follow accepted forensic practices in collecting information.
- When considering criminal prosecutions always be cognizant of the ethical rule that generally prohibits threatening or initiating criminal proceedings to gain an advantage in a civil proceeding.
- No private right of action exists yet under the Economic Espionage Act.

## **2014 Trade Secret Webinar Series**

Beginning in January 2014, we will begin another series of trade secret webinars. The first webinar of 2014 will be “2013 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law.” To receive an invitation to this webinar or any of our future webinars, please sign up for our Trade Secrets, Computer Fraud & Non-Competes mailing list by clicking [here](#).



# Trading Secrets



## Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2013

*By Robert Milligan and Daniel Joshua Salinas (March 6, 2014)*

As part of our annual tradition, we are pleased to present our discussion of the top 10 developments/headlines in trade secret, computer fraud, and non-compete law for 2013. Please join us for [our complimentary webinar](#) on March 6, 2014, at 10:00 a.m. P.S.T., where we will discuss them in greater detail. As with [all of our other webinars](#) (including the 12 installments in our 2013 Trade Secrets webinar series), this webinar will be recorded and later uploaded to our Trading Secrets blog to view at your convenience.



[Last year](#) we predicted that social media would continue to generate disputes in trade secret, computer fraud, and non-compete law, as well as in privacy law. 2013 did not disappoint with significant social media decisions involving the ownership of social media accounts and “followers” and “connections,” as well as cases addressing liability or consequences for actions taken on social media, such as [updating one’s status](#), [communicating with “restricted” connections](#), [creating fake social media accounts](#), or [deleting one’s account](#) during pending litigation.

We also saw more states (e.g., [Arkansas](#), [Utah](#), [New Mexico](#), [California](#), [Colorado](#), [Nevada](#), [Michigan](#), [New Jersey](#), [Oregon](#), and [Washington](#)) enact [legislation](#) to protect employees’ “personal” social media accounts and we expect more states to follow.

The circuit split regarding the interpretation of what is unlawful access under the Computer Fraud and Abuse Act (“CFAA”) remains [unresolved](#) and another case will need to make its way up to the Supreme Court or legislation passed to clarify its scope as federal courts continue to reach differing results concerning whether employees can be held liable under for violating computer use or access policies.

There have also been several legislative efforts to modify trade secret, computer fraud, or non-compete law in various jurisdictions. Texas adopted a version of the [Uniform Trade Secrets Act](#), leaving Massachusetts and New York as the lone holdouts. [Oklahoma](#) passed legislation expressly permitting employee non-solicit agreements. [Massachusetts](#), [Michigan](#), [Illinois](#), [New Jersey](#), [Maryland](#), [Minnesota](#), and [Connecticut](#) considered bills that would provide certain limitations on non-compete agreements but they were not adopted.

We expect more legislative activity in 2014, particularly regarding privacy, the scope of the CFAA, and trade secret legislation to curb foreign trade secret theft and cyber-attacks.





# Trading Secrets



Finally, while the Snowden kerfuffle and NSA snooping captured the headlines in 2013, government agencies remained active, including some high profile [prosecutions](#) under the Economic Espionage Act, the release of the Obama Administration's [Strategy on Mitigating the Theft of U.S. Trade Secrets](#), and the [National Labor Relations Board's](#) continued scrutiny of employers' social media policies. We expect more government activity in this space in 2014.

Here is our listing of top developments/headlines in trade secret, computer fraud, and non-compete law for 2013 in no particular order:

## **1. Dust Off Those Agreements . . . Significant New Non-Compete Cases Keep Employers On Their Toes**

Employers were kept on their toes with some significant non-compete decisions which forced some employers to update their agreements and onboarding/exiting practices. First, in [Fifield v. Premier Dealer Services](#), an Illinois appellate court found that less than two years employment is inadequate consideration to enforce a non-compete against an at-will employee where no other consideration was given for the non-compete. Second, in [Dawson v. Ameritox](#), an Alabama federal court found that a non-compete executed prior to employment was unenforceable. Next, in [Corporate Tech. v. Hartnett](#), a Massachusetts federal court held that initiating contact was not necessary for finding solicitation in breach of a customer non-solicitation agreement. Lastly, in [Assurance Data v. Malyevac](#), the Virginia Supreme Court found that a demurrer (i.e., a pleading challenge) should not be used to determine the enforceability of non-compete provisions but rather evidence should be introduced before making such a determination.

## **2. Continued Split of Authority On the Computer Fraud and Abuse Act and Efforts to Reform CFAA and Enhance Federal Trade Secret and Cybersecurity Law**

Courts in [Massachusetts](#), [Minnesota](#), and [New York](#) joined the Ninth Circuit's narrow reading of the CFAA and limited its applicability to pure hacking scenarios rather than violations of employer computer usage or access policies. Additionally, in 2013, Representative Zoe Lofgren [introduced](#) Aaron's Law, named after the political hackvist Aaron Swartz, to reform of the Computer Fraud and Abuse Act. Her proposed legislation would limit the CFAA to pure hacking scenarios and exclude violations of computer usage policies and internet terms of service from its scope. Lofgren also introduced legislation which would create a federal civil cause of action in federal court for trade secret misappropriation. Other legislation to prevent intellectual property theft was also introduced including the [Deter Cyber Theft Act](#), which aims to block products that contain intellectual property stolen from U.S. companies by foreign countries from being sold in the United States. The [Cyber Economic Espionage Accountability Act](#) was also introduced and allows U.S. authorities to "punish criminals backed by China, Russia or other foreign governments for cyberspying and theft." We expect Congress to consider similar legislation in 2014.



# Trading Secrets



### 3. Texas Adopts Uniform Trade Secrets Act

Texas joined forty-seven other states in [adopting](#) some version of the Uniform Trade Secrets Act. Until recently, Texas common law governed misappropriation of trade secrets lawsuits in Texas. The new changes under the Texas UTSA (which we discuss in more detail [here](#)) provide protection for customer lists, the ability to recover attorneys' fees, a presumption in favor of granting protective orders to preserve the secrecy of trade secrets during pending litigation, and that information obtained by reverse engineering does not meet the definition of a trade secret. Legislation has been [introduced](#) in Massachusetts to adopt the Act but has yet to pass. For additional information on recent trade secret and non-compete legislative updates, check out our webinar "[Trade Secrets and Non-Compete Legislative Update](#)."

### 4. High Profile Prosecutions and Trials under Computer Fraud and Abuse Act and Economic Espionage Act

2013 saw several high profile prosecutions and trials under the CFAA and Economic Espionage Act. [Bradley Manning](#), who allegedly leaked confidential government documents, to WikiLeaks, and [Andrew 'Weev' Auernheimer](#), who allegedly hacked AT&T's servers, were both convicted under the CFAA. Executive recruiter David Nosal was [convicted](#) by a San Francisco jury of violating federal trade secret laws and the CFAA and [sentenced](#) to one year and a day in federal prison. In *U.S. v. Jin*, the Seventh Circuit [upheld the conviction](#) of a Chicago woman sentenced to four years in prison for stealing trade secrets of her employer before boarding a plane for China. For additional information on criminal liability for trade secret misappropriation, check out our webinar "[The Stakes Just Got Higher: Criminal Prosecution of Trade Secret Misappropriation](#)."

### 5. More Social Media Privacy Legislation

[Arkansas](#), [Utah](#), [New Mexico](#), [Colorado](#), [Nevada](#), [Michigan](#), [New Jersey](#), [Oregon](#), and [Washington](#) all passed legislation social media privacy legislation in 2013 that prohibited employers from asking or insisting that their employees provide access to their personal social networking accounts. [California](#) extended its current social media privacy law to specify that it encompassed public employers. We expect more states to enact social media privacy legislation in 2014.

### 6. Continued Uncertainty on the Scope of Trade Secret Preemption

Courts have continued to struggle with the scope and timing of applying preemption in trade secret cases, but there is a growing movement to displace common law tort claims for the theft of information. Such claims are typically tortious interference with contract, conversion, unfair competition, and a breach of fiduciary duty. In essence, plaintiffs may only be left with breach of contract and a trade secret claim for the theft of information if a jurisdiction adopted a broad preemption perspective. Courts in western states such as [Arizona](#), [Hawaii](#), [Nevada](#), [Utah](#), and [Washington](#) have preempted "confidential information" theft claims under their respective trade secret preemption statutes.





# Trading Secrets



In [\*K.F. Jacobsen v. Gaylor\*](#), an Oregon federal court, however, found that a conversion claim for theft of confidential information was not preempted. In [\*Triage Consulting Group v. IMA\*](#), a Pennsylvania federal court permitted the pleading of preempted claims in the alternative. Additionally, in [\*Angelica Textile Svcs. v. Park\*](#), a California Court of Appeal found that there was no preemption of claims for breach of contract, unfair competition, conversion, or tortious interference because the claims were based on facts distinct from the trade secret claim and the conversion claim asserted the theft of tangible documents. In contrast, in [\*Anheuser-Busch v. Clark\*](#), a California federal court found that a return of personal property claim based on the taking of “confidential, proprietary, and/or trade secret information” was preempted because there was no other basis beside trade secrets law for a property right in the taken information. For additional information on the practical impact of preemption on protecting trade secrets and litigating trade secret cases, check out our webinar [“How and Why California is Different When it Comes to Trade Secrets and Non-Competes.”](#)

## **7. Growing Challenge of Protecting of Information in the Cloud with Increasing Prevalence of BYOD and Online Storage**

While the benefits of cloud computing are well documented, the growth of third party online data storage has facilitated the ability for [rogue employees to take valuable trade secrets](#) and other proprietary company electronic files, in the matter of minutes, if not seconds. The increasing use of mobile devices and cloud technologies by companies both large and small is likely to result in more mobile devices and online storage being relevant in litigation. A recent article in The Recorder entitled [“Trade Secrets Spat Center on Cloud,”](#) observed that the existence of cloud computing services within the workplace makes it “harder for companies to distinguish true data breaches from false alarms.”

An insightful Symantec/Ponemon [study](#) on employees’ beliefs about IP and data theft was released in 2013. It surveyed 3,317 employees in 6 countries (U.S., U.K., France, Brazil, China, South Korea). According to the survey, 1 in 3 employees move work files to file sharing apps (e.g. Drop Box). Half of employees who left/lost their jobs kept confidential information 40% plan to use confidential information at a new job. The top reasons employees believe data theft acceptable: (1) does not harm the company does not strictly enforce its policies; (2) information is not secured and generally available; or (3) employee would not receive any economic gain. The results of this study serve as a reminder that employers [must be vigilant](#) to ensure that they have robust agreements and policies with their employees as well as other sound trade secret protections, including employee training and IT security, to protect their valuable trade secrets and company data before they are compromised and stolen. Employers should implement policies and agreements to restrict or clarify the use of cloud computing services for storing and sharing company data by employees. Some employers may prefer to simply block all access to such cloud computing services and document the same in their policies and agreements. For a further discussion about steps and responses companies can take when their confidential information and/or trade secrets appear, or are threatened to appear, on the Internet, check out our webinar [“My Company’s Confidential Information is Posted on the Internet! What Can I Do?”](#)



# Trading Secrets

## 8. Continued Significance of Choice of Law and Forum Selection Provisions In Non-Compete and Trade Secret Disputes

The U.S. Supreme Court's recent decision in [Atlantic Marine v. U.S.D.C. for the W.D. of Texas](#) appears to strengthen the enforceability of forum selection clauses as it held that courts should ordinarily transfer cases pursuant to applicable and enforceable forum selection clauses in all but the most extraordinary circumstances. While *Atlantic Marine* did not concern restrictive covenant agreements or the employer-employee context, it may nonetheless make it more difficult for current and/or former employees to circumvent the forum selection clauses contained in their non-compete or trade secret protection agreements. Many federal courts continue to enforce out-of-state forum selection clauses in non-compete disputes (see [AJZN v. Yu](#) and [Meras Eng'r'g v. CH2O](#)), while some courts have [disregarded](#) forum selection clauses in such disputes "in the interests of justice." The Federal Circuit in [Convolve and MIT v. Compaq and Seagate](#) held that information at issue lost its trade secret protection when the trade secret holder disclosed the information because it failed to comply with the confidential marking requirement set forth in a non-disclosure agreement. Accordingly, trade secret holders should be careful what their non-disclosure agreements say about trade secret protection otherwise they may lose such protection if they fail to follow such agreements.

## 9. Social Media Continues to Change Traditional Legal Definitions and Analyses

Social media continues to change the way we define various activities in employment, litigation, and our everyday lives. A Pennsylvania federal district court in the closely watched [Eagle v. Morgan](#) case found that a former employee was able to successfully prove her causes of action against her former employer for the theft of her LinkedIn account, but she was unable to prove damages with reasonable certainty. Recent cases in [Massachusetts](#) and [Oklahoma](#) held that social media posts, updates and communications with former customers did not violate their non-solicitation restrictive covenants with their former employer. In the litigation context, a New Jersey federal court issued sanctions against a litigant for [deleting his Facebook profile](#), while a New York federal court allowed the FTC to [effectuate service of process on foreign defendants](#) through Facebook. The Fourth Circuit held that "liking" something on Facebook is "a form of free speech protected by the First Amendment." Federal district courts in [Nevada](#) and [New Jersey](#) illustrated the growing trend of courts finding that individuals may lack a reasonable expectation of privacy in social media posts. For further discussion on the relationship between social media and trade secrets, check out our webinar "[Employee Privacy and Social Networking: Can Your Trade Secret Survive?](#)"

## 10. ITC Remains Attractive Forum to Address Trade Secret Theft

The Federal Circuit caught the attention of the ITC and trade secret litigators alike when it ruled in *TianRui Group Co. v. ITC* that the ITC can exercise its jurisdiction over acts of misappropriation occurring entirely in China. Since then, victims of trade secret theft by foreign entities are increasingly seeking relief from the ITC (e.g. [In the Matter of Certain Rubber Resins and Processes for Manufacturing Same](#) (Inv. No. 337-TA-849)). For valuable insight on protecting trade secrets and confidential information in China and other Asian countries, including the effective use of non-compete



# Trading Secrets



and non-disclosure agreements, please check out our recent webinar titled, "[Trade Secret and Non-Compete Considerations in Asia](#)."

We thank everyone who followed us this year and we really appreciate all of your support. We also thank everyone who helped us make the [ABA's Top 100 Law Blogs](#) list. We will continue to provide up-to-the-minute information on the latest legal trends and cases across the country, as well as important thought leadership and resource links and materials.



# Trading Secrets



## Trade Secrets

# Trading Secrets



## Rankings Of NFL Prospects May Constitute Trade Secrets

*By Paul Freehling (January 7th, 2013)*

With today's college football National Championship game between Alabama and Notre Dame, a recent trade secret decision regarding the interplay between trade secrets and NFL scouting grades caught our eye.

National Football Scouting authors several hundred six-page biographical reports annually on outstanding college football players. The reports are sold for \$75,000 each to 21 NFL teams to use during the player draft. Every prospect receives an overall numeric grade reflecting the scouts' opinion of the likelihood that the player will succeed in the NFL. Rang, a part-time sports reporter, obtained and published National's grades for 18 college players. When he was sued in a State of Washington federal court for trade secret misappropriation, he moved for summary judgment. He, argued that only facts can constitute trade secrets and that the numeric grades are subjective opinions, not facts. The court [disagreed](#) and said that the assignment of specific grades to particular prospects are facts with independent significance that could be trade secrets. [National Football Scouting, Inc. v. Rang](#), Case No. 11-cv-5762-RBL (W.D. Wash., Dec. 13, 2012).



The Washington Uniform Trade Secrets Act defines a trade secret, in part, as “information . . . that (a) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means, by other persons who can obtain economic value from its disclosure or use, and (b) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” A 1999 Washington Supreme Court held that the Restatement (Third) of Unfair Competition can provide guidance on trade secrets. Quoting the Restatement, the Washington federal court concluded that “[t]he status of information claimed as a trade secret must be ascertained through a comparative evaluation of the relevant factors, including the value, secrecy, and definiteness of the information as well as the nature of the defendant’s misconduct.”

That same Washington Supreme Court decision held that the question of whether specific information is protectable under trade secret law is to be determined by the trier of fact. Rang’s motion for summary judgment with respect to the misappropriation cause of action was denied. There were material disputed issues of fact, including the reasonableness of National’s efforts to preserve the secrecy of the numeric grades — the reports were shared only with the teams and a computer consultant all of whom signed confidentiality agreements — and the extent to which the grades had economic value by reason of not being generally known.

National’s reports purport to be copyrighted as unpublished works. A numeric expression of a professional opinion can be copyrighted — for example, appraisals and predictions, but Rang’s summary judgment motion relating to the infringement claim was granted based on the “fair use” doctrine. The only parts of National’s comprehensive work-product that Rang published were a few of the grades. Moreover, he transformed those grades by adding material in the public domain concerning the players as well as his own impressions.



# Trading Secrets



The federal court decision pushes the envelope to the extent that it is read as granting trade secret protection to (and potentially upholding the validity of copyrighting) a numeric grade. Please see [Eric Goldman's blog](#) regarding the copyright aspects of the court's decision. Yet, many cases hold that misappropriation of a compilation of numbers, such as a price list or a telephone directory, could be actionable. Moreover, the method or process for assigning value to property might be a trade secret (or copyrightable). So, perhaps it is not surprising that a court would protect an expert's predictions as to the potential commercial success that ideas or persons may achieve.

# Trading Secrets



## Department of Justice Issues Report Highlighting Trade Secret Theft Prosecutions And Need For Companies To Vigilantly Protect Their Data

*By Jessica Mendelson and Robert Milligan (January 9th, 2013)*

In December 2012, the Department of Justice released a [“Summary of the Major U.S. Export Enforcement, Economic Espionage, Trade Secret and Embargo-Related Criminal Cases.”](#)

The report includes the major export enforcement, trade secret theft, economic espionage, and embargo-related criminal prosecutions handled by the United States Department of Justice between January 2007 and December 2012.

The cases resulted from investigations conducted by various governmental agencies, including the Federal Bureau of Investigation (FBI), the Department of Homeland Security’s U.S. Immigration and Customs Enforcement (ICE), the Department of Commerce’s Bureau of Industry and Security (BIS), the Pentagon’s Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. The full report can be found [here](#).



In honor of the new year, here are the major trade secret cases handled by the Department of Justice in 2012:

**Chemical Company Trade Secrets to China** – In January 2012, a former employee of a large chemical company, was sentenced to five years in prison, two years supervised release, a \$25,000 fine and was required to forfeit \$600,000. The employee was convicted in the Middle District of Louisiana of conspiracy to commit trade secret theft for stealing trade secrets from his former employer and selling them to companies in China.

**Pharmaceutical Company Trade Secrets to United States Subsidiary of a Chinese Company** – In January 2012, a former employee of an American pharmaceutical company, pled guilty to stealing trade secrets and making them available to an American subsidiary of a Chinese company. The former employee downloaded and accessed the company’s information from her personal computer in order to steal trade secrets. She pled guilty in the District of New Jersey to theft of trade secrets.

**Chemical Company Trade Secrets to China** – In March 2012, a former chemical company employee pled guilty in the Northern District of California to “conspiracy to commit economic espionage, admitting that he provided trade secret” to companies controlled by the Chinese government.

**Irrigation Company Trade Secrets to Competitors in China** – In May 2012, two former employees, as well as their current employers, were charged with theft of trade secrets, wire fraud, and conspiracy





# Trading Secrets



to commit wire fraud in connection with the theft of trade secrets. The defendants allegedly stole trade secrets pertaining to sales and prices from their former employer, an irrigation company based in Utah. The defendants allegedly planned to use the information to devise a scheme to undermine the irrigation company's position in the market.

**Telecommunications Trade Secrets to China** – In August 2012, a former software engineer was tried for theft of trade secrets in the Northern District of Illinois for allegedly stealing proprietary telecommunications technology from his former employer. Jin's former employer had spent more than \$400 million developing the technology. While on sick leave, the former employee pursued other employment in China, and accessed hundreds of confidential documents from the company's secure internal network. She was convicted of theft of trade secrets and sentenced to four years in prison, however she was found not guilty of economic espionage for China's benefit.

**Theft of Futures and Options Traders' Trade Secrets for Potential Use in China** – In September 2012, a former senior software engineer for a futures and options trading firm, was convicted of stealing trade secrets in the Northern District of Illinois. The employee allegedly had downloaded more than 10,000 files of source code and other confidential and proprietary information from his former employer while working to improve an electronic trading exchange in China. Allegedly, the employee's actions resulted in a government loss of over \$50 million.

**Manufacturing Trade Secrets to China** – In September 2012, two former employees were indicted in the Western District of Missouri for attempting to purchase stolen trade secrets. The two allegedly stole trade secrets from their employer, a glass insulation manufacturer, in order to open a competing plant in China. The defendants allegedly offered to pay \$100,000 to an FBI cooperating source to obtain trade secret, confidential and proprietary information from the company.

**Military Technical Data and Trade Secrets to China** – In September 2012, a former senior staff engineer at a space communications company, was "convicted in the District of New Jersey of exporting sensitive U.S. military technology to China, stealing trade secrets and lying to federal agents." According to documents filed in the case and evidence presented at trial, in 2010, the employee stole thousands of electronic files from his employer, which included "the performance and design of guidance systems for missiles, rockets, target locators, and unmanned aerial vehicles. Allegedly, the employee planned to use these items for his future employment in China.

**Trade Secrets to Kolon Industries**—In October 2012, several employees of South Korea-based Kolon Industries Inc. were indicted in the Eastern District of Virginia for allegedly "engaging in a multi-year campaign to steal trade secrets." The indictment seeks more than \$225 million in profits from the theft of trade secrets from Kolon's competitors. Allegedly, Kolon obtained confidential information related to DuPont's manufacturing process for Kevlar, a type of fiber used to make various products including body armor and fiber optic cables. Kolon's employees allegedly misappropriated confidential information related to Kevlar's manufacturing process, and within three years, the company was able to replicate the product, and allegedly develop a multi-phase plan to steal additional trade secret information. The FBI investigated the allegations, and the indictment seeks forfeiture of at least \$225 million in proceeds from the alleged theft of trade secrets and charges Kolon with "one count of conspiring to convert trade secrets, four counts of theft of trade secrets and one count of obstruction of justice." A separate civil case was brought against Kolon in Virginia and DuPont was awarded close to a billion dollars and a 20 year permanent injunction. Please see John Marsh's excellent [summary of the case](#).

**New Legislation**—Congress just [passed two amendments](#) to the Economic Espionage Act which will protect more trade secrets and enhance the penalties for violations. The legislation directly responds to



# Trading Secrets



the Second Circuit's decision in *U.S. v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012), which overturned a jury verdict finding the defendant violated 18 U.S.C. 1832(a) of the Economic Espionage Act by stealing computer code from his employer. The court held that the statute did not apply because the computer code failed to satisfy the requirement that the "product" was "produced for" or "placed in" interstate or foreign commerce. The amended Section 1832(a) now applies to a trade secret "that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof."

The House of Representatives recently also passed a bill enhancing the penalties for violations of the Economic Espionage Act. Under the bill, the upper limit of penalties for individual offenses at Section 1831(a) would be increased from \$500,000 to \$5,000,000; the upper limit for corporate offenses at Section 1831(b) would be increased from \$10,000,000 to the greater of \$10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided. The bill also passed in the Senate and is waiting for President Obama's signature.

The full Department of Justice [report](#) shows the increasing importance of criminal prosecution as a tool to dissuade theft of trade secrets. These cases highlight the importance of monitoring employee access to secure company databases and limiting access to important data to a need know basis. Furthermore, companies should consider using additional preventive means to prohibit employees from stealing trade secrets, such as configuring computers to restrict access to external devices, blocking a user from uploading information to a web-based site, and/or utilizing software that blocks employees from sending emails to certain domain names and either highlights or restricts the amount of data that can be sent out by a user. Companies may also wish to consider prohibiting employees from sending emails to certain domain names that are commonly used for personal email accounts and/or block such emails from being sent. In an era in which data is becoming increasingly portable, companies much increase their vigilance in monitoring the use and export of their data and trade secrets.

# Trading Secrets



## Connecticut Court Has Jurisdiction Over Canadian Defendant Charged With Misappropriation of Canadian Company's Trade Secret Emails

*By Paul Freehling (January 10th, 2013)*

The Second Circuit Court of Appeals has reversed a Connecticut federal court's order dismissing for lack of personal jurisdiction a Connecticut corporation's complaint for misappropriation of trade secrets by a Canadian employee of the plaintiff's Canadian subsidiary. The complaint alleged her knowledge that her employer's emails were stored on its parent corporation's servers in Waterbury, Connecticut. Therefore, the claim that she purposefully engaged in activities in Connecticut, by downloading confidential emails from her employer's computer to her personal computer, was adequately pleaded. [MacDermid, Inc. v. Deiter, No. 11-5388-cv \(2nd Cir., Dec. 26, 2012\), rev'g No. 3:11-CV-0855-WWE \(D. Conn., Dec. 1, 2011\).](#)



Connecticut's long-arm statute provides, in relevant part, that a non-resident is subject to the state's jurisdiction for lawsuits alleging misuse of "a computer, as defined, . . . located within the state." The statutory definition of the word "computer" includes "an electronic . . . device . . . that, pursuant to . . . human instruction . . . can automatically perform computer operations with . . . computer data and can communicate the results to another computer or to a person [or is a] connected or directly related device . . . that enables the computer to store, retrieve or communicate . . . computer data . . . to or from a person, another computer or another device." According to the Second Circuit, "a computer server meets the Connecticut long-arm statute's definition of computer."

In support of her successful motion to dismiss in the district court, the defendant noted that she did not work in the U.S. and that she had no reason to expect that a suit against her would be heard anywhere other than in Canada. The trial court's Memorandum of Decision observed that she was not alleged to have engaged in a persistent course of misconduct or to have derived any revenue from the supposed misappropriation. That court stressed that the "defendant's tortious conduct occurred, if at all, when defendant transferred plaintiff's proprietary information onto her home computer from her work computer, a transaction that occurred exclusively in Canada."

According to the Court of Appeals, however, "It is not material that [the defendant] was outside of Connecticut when she accessed the Waterbury servers. The statute requires only that the computer . . ., not the user, be located in Connecticut." While recognizing that many internet users probably do not know the location of servers where emails are stored, this defendant allegedly was aware that the servers were in Connecticut, and at the motion to dismiss stage, well pleaded factual allegations are assumed to be true. In light of the interest of a company with its principal place of business in Connecticut in obtaining redress for alleged wrongs and the public interest of the state in which the company is based, and because "efficiency and social policies against computer-based theft are



# Trading Secrets



generally served by adjudication in the state from which computer files have been misappropriated,” the Connecticut federal court could properly exercise jurisdiction.

The decision in this case constitutes a warning to all persons misappropriating confidential emails. No matter where in the world the defendant downloads the emails, he or she may be sued in Connecticut — or in any other state with a similar statute — for trade secrets misappropriation where the emails are stored on servers in the forum state, particularly if the plaintiff does business there and the defendant is alleged to have known the location of the servers. Check out [Kenneth Vanko's blog](#) for a quick analysis of the case.

See also our prior [post](#) where a California federal district court examined the issue of personal jurisdiction in an international trade secret misappropriation and breach of contract dispute between an American company and a European distributor based out of Ireland.

# Trading Secrets



## 3D Printing and Intellectual Property

*By Joren De Wachter (January 21st, 2013)*

*As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry about the impact of software on IP strategy by technology lawyer and IP strategist Joren De Wachter. Joren serves as a Vice Chair with me on the ITechLaw Intellectual Property Law Committee and has an excellent blog of his own on current technology issues. Enjoy Joren's article.*

*-Robert Milligan, Editor of Trading Secrets*

The technology of 3D-printing has made great progress and the world of Intellectual Property has started to react to the challenge posed by 3D-printing; which, in turn, has caused a surprise reaction by the 3D-printing community.



### What is 3D-Printing?

Although 3D-printing has become much more [widely known](#), not everyone knows about it, and still less people have actually seen it happen.

A 3D-printer is a machine that builds objects, by adding very tiny layers of material on top of each other. It “prints” in three dimensions.

The cheapest 3D-printers are now available at less than \$1,000, and they can print you objects such as coat hangers, teacups, decorative elements like cufflinks, toy cars, Christmas decorations at a negligible cost, but also prototype models of new product designs; something which typically costs many hundreds or thousands euros to have made.

And the technology is booming and evolving fast.

The potential impact of the 3D-printer on society at large has been compared to that of the PC – arguably, it may be bigger.

Imagine most of your products no longer manufactured in China, but around the corner in a “print-shop”? We could scrap half the world's fleet, and reduce the ecological impact of any such production significantly. Because 3D-printing is what is called “additive” manufacturing, it produces significantly less waste than traditional manufacturing, which still uses the “carving out and throwing the waste away”.

3D-printing already uses many materials such as plastics, metals, ceramics, bio-materials (including both foodstuffs and elements of human tissue such as cartilage, or a [lower jaw](#), or the carrying structure of organs such as [kidneys](#)), with drugs ([DNA-based 3D-printing](#) and [guns](#) just around the corner).



# Trading Secrets



Since I [first wrote](#) about 3D-printing and their impact on IP rights, back in March 2011, things have evolved, both in terms of technology and in terms of Intellectual Property.

## Technological and Market Evolution

3D-printing evolves quite fast, particularly at the low-end, customer facing side of the technology. While companies like [Materialise](#) and [3Dsystems](#) have grown significantly by providing better and cheaper products at the high-end (allowing much cheaper and complex prototype development), there has been a boom in businesses offering DIY (indeed) 3D-printers, from [Ultimaker](#) to [Makerbot](#) to [RepRap](#) to [PP3DP](#), and I'm forgetting [many](#).

Printers become faster and more reliable, layers of construction become smaller, allowing for more sophisticated products, the scope of prime materials continues to grow.

But, as I said earlier, the real fast growth is, as always, in software. Designs of printable objects increases spectacularly, also thanks to websites like [Fabber](#), [Shapeways](#), [Thingiverse](#) and, again, I'm forgetting [many](#).

But the really coolest thing I've seen recently is this: 3D-printing of [vinyl records](#) – with the music on it! It's really “replicating music”; while the technology is not quite yet at the desired level, it gives an idea of things to come. Does that mean I will be able to physically copy over my old vinyl record collection soon?

## Intellectual Property Developments

The world of Intellectual Property took notice, and a number of trends are starting to emerge. First, the patent trolls wanted to see if they could chip in and make a [quick buck](#) out of this. In true patent troll spirit, former Microsoft CTO Nathan Myhrvold's Intellectual Ventures, filed a [patent](#) on a system of Digital Rights Management (DRM)-control of 3D-printing.

Such a system would mean that anyone who wants to 3D-print certain files, would have to pay a license fee; it is not quite clear who to, or why, but it looks like Intellectual Ventures wants to be able to collect lots of money on the back of the innovation and creativity of others (a sad, but typical, use of Intellectual Property Rights, a system nominally designed to “promote science and the useful arts”).

In a similar vein, 3D systems, an “established” 3D-printing business, has [filed a lawsuit against Kickstarter](#) – this is an interesting case, since 3D systems seems to assume that because they own certain rights, they would have a right to stop Kickstarter from allowing fundraising for a potential competitor who might, possibly, be in breach of those rights.

So we see the first signs of IP holders trying to levy their usual tax on innovation into a new field.

Second, and more interestingly, though, a push-back has occurred by parts of the 3D-printing community. Unlike the PC, when no open source was around, a lot of 3D-printing technology, both in the hardware and the software, is open source.

This has spurred the [Electronic Frontier Foundation](#) into trying to [crowdfund](#) efforts to prevent the potential [damage to innovation](#) done by patents such as the ones filed by Intellectual Ventures.





# Trading Secrets



While this points at obvious serious flaws in the patent system, which, certainly in the US, continues to lay monopolistic claims to existing technology, or on the basis of mere ideas, it is interesting that crowdsourcing of information is used to try to remedy this. One could opine that finding out about prior art is really the job of the USPTO, but that is going to deeply into the political debate about Intellectual Property Rights.

Thirdly, the question of DRM-protection of printable files seems awkwardly timed, now that most DRM for either music or ebooks can be so [easily circumvented](#), or is indeed lifted.

## Foreseeable Trends

While it is of course very dangerous to predict the future, there are some trends that can be seen.

On the technology side, it looks like the development of 3D-printing technology is both speeding up and spreading out. More applications, more advancement, more innovation is likely to take place. When people already receive body-implants for a lower jaw printed by 3D-printing in 2012, who knows where the limits are.

Also, since 3D-printing is spreading through communities of “makers”, the innovative advantages of an open source approach will probably lead to ever faster incremental improvements, alongside

On the IP field, the issues will be more problematic. As I’ve [stated before](#), the problem with patents is that they are very hard to enforce in an open environment – when even at the level of the mobile phone market, patent litigation is clearly not cost-effective, and destroys a lot of shareholder value, how will anyone be able to enforce patents against a myriad community of developers and makers?

Unless of course legislation is changed, and the scope of patents is expanded – but that would risk a serious backlash, as anyone who remembers the SOPA/PIPA story will confirm.

Design rights remain problematic; indeed, it is hard to see how design rights or design patents will be useful in blocking access to the market of competitive designs or products. Again, the issue of cost-effectiveness of litigating someone to keep products that can be manufactured at a much lower price off the market will meet with both practical and political problems.

Finally, there is the impact of copyright on the printable files. If I design a chair, or a tower for my toy castle, and that fits neatly with a “[game of thrones](#)” game, I do actually own the copyright in the digital file of such tower I designed myself, even if that resembles or fits well with a design from someone else. It is not clear how DMCA would apply to such a file, unless copyright would be fundamentally changed – right now, the copyright only applies to the code, not what the code does.

BitTorrent sites and other peer-to-peer approaches are already developing rapidly growing [forums](#) where people can share their files to be printed. It will be a lot less clear for right holders in a product to claim that they have rights in an .stl file developed by someone else, allowing to print a product that looks like, but not quite is, that original product.

Maybe the near future will bring a mighty new battle between those who want more control over the Internet (the right holders), and those who want to use it for the purpose of sharing and innovating (the 3D-printing communities).



# Trading Secrets



## Ninth Circuit Overturns \$172 Million Trade Secrets Award in Rival Toy Makers' Epic Dispute

*By Robert Milligan and Daniel Joshua Salinas (January 25th, 2013)*

After more than eight years of litigation and two jury trials over the Bratz doll line, rival toy makers Mattel, Inc. and MGA Entertainment, Inc. may be headed for a rubber match – a third jury trial. Yesterday, a Ninth Circuit panel consisting of Chief Judge Alex Kozinski, Judge Kim Wardlaw, and Judge Stephen Trott, overturned an award of \$172 million in damages (including attorneys' fees) to MGA for alleged trade secret misappropriation, holding that MGA's respective counterclaim-in-reply was not compulsory and should not have reached the jury. [\*Mattel, Inc. v. MGA Entertainment, Inc.\*, Case No. 11-56357 \(9th Cir. Jan. 24, 2013\).](#)

In 2006, Mattel sought leave to amend its complaint by adding a claim against MGA for alleged misappropriation of trade secrets. Then, in 2010, after the Ninth Circuit had decided the first appeal, MGA filed a counterclaim against Mattel for misappropriating its trade secrets.

To be compulsory, the counterclaim must "arise[] out of the transaction or occurrence that is the subject matter of the opposing party's claim." [FRCP 13\(a\)\(1\)\(A\).](#)

Mattel moved to dismiss MGA's claim, arguing that the statute of limitations had run because the events at issue happened more than three years earlier. Mattel argued that MGA's trade secrets claim did not arise out of the transaction or occurrence that was the subject of Mattel's trade secrets claim. Mattel argued that that each parties' claims involved different trade secrets that were allegedly stolen at different places and times; by different actors; and through different means.

The district court denied Mattel's motion and instead found that that MGA's counterclaim-in-reply for trade secret theft was compulsory because it was "logically related" to Mattel's trade secret theft claim. Specifically, the district court ruled that it was "more than reasonable to conclude at least some of the trade secret information allegedly misappropriated by [MGA] incorporated trade secret information" that Mattel had allegedly stolen from MGA.

MGA's trade claim proceeded to trial. The jury found for MGA, and awarded more than \$80 million in damages. The district court then awarded MGA an equal amount in exemplary damages under the California Uniform Trade Secrets Act, which authorizes exemplary damages if the misappropriation was "willful and malicious." Cal. Civ. Code § 3426.3(c). The court also awarded trade secret attorneys' fees and costs. In addition, because the jury found for MGA on Mattel's copyright claim, the district court awarded attorneys' fees and costs to MGA under the Copyright Act. Mattel appealed the trade secret award and the award of fees and costs on the Copyright claim. (See our prior posts on [Mattel's opening appellate brief](#) and the Judges' questions during [oral argument](#)).





# Trading Secrets



On appeal, the Ninth Circuit panel affirmed the award of fees and costs on the copyright claim but reversed on the trade secret award.

Relying on *In re Pegasus Gold*, 394 F.3d 1189 (9th Cir. 2005), the panel held that MGA's counterclaim-in-reply was not "logically related" to Mattel's counterclaim because it "did not rest on the same 'aggregate core of facts.'" The panel explained that opposing claims of trade secret theft are not enough to render a counterclaim compulsory: "[w]hat matters is not the legal theory but the facts."

Specifically, the Court reasoned that MGA's claim did not rest on the same "aggregate core of facts" as Mattel's claim:

"While Mattel asserted many claims that covered numerous interactions between Mattel and MGA, Mattel's specific allegations regarding trade secrets were that several of their employees ... defected to MGA and disclosed Mattel's trade secrets. By contrast, MGA's trade-secret claim rested on allegations that Mattel's employees stole MGA trade secrets by engaging in chicanery (such as masquerading as buyers) at toy fairs. That both Mattel and MGA claimed they stole each other's trade secrets isn't enough to render MGA's counterclaim compulsory."

The Court further reasoned that the claim would not have been compulsory if "the same information may have shuttled back and forth between Mattel and MGA... [because this] isn't a sufficient nexus to support a compulsory counterclaim."

Thus, the Court vacated the jury's verdict in favor of MGA because the claim was not compulsory and, thus should not have reached the jury. The Court instructed the district court to dismiss MGA's trade secret claim without prejudice.

This is the second time the same three-judge panel overturned a significant jury award in the case. In 2010, the same panel reversed a jury verdict that awarded Mattel nearly \$100 million in damages and the ownership rights to the Bratz doll brand.

The Court upheld the approximately \$137 million in attorneys' fees for MGA's defense against Mattel's copyright claims. The Court reasoned that the district court did not abuse its discretion in awarding fees and costs under the Copyright Act and that bad faith and frivolousness was not the applicable standard.

It does not appear that this case is over yet and [published reports](#) indicate that MGA intends to file a new lawsuit for the trade secret misappropriation claim. Regardless what happens, Chief Judge Kozinski had one final piece of advice for the parties, "play nice."

Apart from the size of the awards in this case, this case is also significant from a procedural standpoint because it reaffirms the importance of facts when determining whether a claim is compulsory or permissive. Indeed, the panel reiterated that the logical relationship test is based on the "aggregate core of facts" and not general inferences about similar legal theories.

We will keep you posted on any significant further developments.

# Trading Secrets



## Fashion Designer Resolves “Preppy Clothing” Trade Secrets Dispute

*By Jessica Mendelson (January 31st, 2013)*

In November 2012, we [first blogged](#) on the high profile trade secret dispute between Tory Burch, creator of the fashion line Tory Burch LLC, and her ex-husband, J. Christopher Burch.

In October 2012, Christopher Burch filed a breach-of-contract and tortious interference complaint against his ex-wife in which he alleged that his “ex-wife hijacked the bidding process for his 28 percent stake in the New York-headquartered luxury sportswear company the couple founded in 2003, when they were still married.” In response, Tory Burch filed counterclaims in early November, in which she accused Christopher of stealing trade secrets to establish stores which looked suspiciously like her own boutiques.



In late December 2012, the lawsuit officially settled, following the announcement that merchant bank BDT Capital Partners LLC (“BDT”) and private equity firm General Atlantic LLC (“General Atlantic”) would each purchase a minority stake in Tory Burch LLC. As part of the sale, Christopher Burch [agreed](#) that he would drop his lawsuit, Tory Burch, who retains a 28 percent share in the company, also agreed to drop her countersuit.]

The exact terms of the acquisition are unknown, and the parties did not disclose how much either BDT or General Atlantic would pay for their stakes in the company, nor the size of either company’s share. Nor is it clear whether the acquired shares will come directly from Christopher Burch’s shares of the company. Tory Burch did [reveal](#) that Christopher “will retain at least some of his stake in the business.”

In a joint statement, Tory Burch [stated](#), “We are thrilled to have BDT Capital Partners and General Atlantic join us as partners. They are completely aligned with our long-term approach to building our brand and share our vision for growth globally.” Christopher Burch agreed, stating, “I am pleased to see the company complete this milestone transaction. I am confident in its continued success, and I look forward to remaining a significant investor.”

Now that the legal dispute is history, [many industry insiders](#) believe that the next logical step for Tory Burch LLC is an IPO. Several [media](#) reports suggest a public offering may be in the pipeline, and Bloomberg analysts [estimate](#) market valuation may top \$3.4 billion. Whether this plays out remains to be seen, but now that the legal dispute is out of the way, things are clearly looking up for Tory Burch LLC.

# Trading Secrets



## Aleynikov Case Continues to Grab Headlines in Trade Secrets Community

*By Jessica Mendelson (February 1st, 2013)*

Last year, Sergey Aleynikov, a computer programmer, [beat federal charges](#) of trade secret theft under the Economic Espionage Act. Although Aleynikov was initially convicted, the Second Circuit Court of Appeals [overturned his conviction](#), finding that the trade secrets relating to the source code Aleynikov had taken were not related to a product “produced for . . . interstate or foreign commerce,” and thus, were not entitled to protection under the Act. See John Marsh’s [excellent blog post](#) for additional information on the Second Circuit case.



In response, Congress passed the [Trade Secrets Clarification Act](#), which expands the original Economic Espionage Act to include a trade secret “that is related to a product or service used in or intended for use in interstate or foreign commerce.” The change was intended to prevent results like the Second Circuit’s decision in Aleynikov.

Although his federal case is now completed, Aleynikov is now facing a [second prosecution](#) by Manhattan District Attorney Cyrus Vance. In New York state court on Friday January 18, 2013, Aleynikov reportedly [told](#) Judge Ronald A. Zweibel that the District Attorney was “trying to convict him of stealing the bank’s high-frequency trading computer code only because federal prosecutors couldn’t get him. Aleynikov’s lawyer, Kevin Marino, reportedly [explained](#) that the prosecution was “inhuman,” and that state prosecutors had simply regurgitated prior arguments from the federal prosecution, forcing Aleynikov to fight a “many-headed Hydra.” Marino reportedly expressed frustration with the case, arguing it amounted to double jeopardy, and that Aleynikov was unlikely to serve any time even if he were convicted, since he’d already spent a year in prison following the federal case.

According to Marino, the statutes Aleynikov is being prosecuted under don’t even apply to him. Marino alleges Aleynikov was authorized to access the computers, and therefore, his use was not unlawful. Assistant District Attorney Joanne Li reportedly [believes otherwise](#): “the misappropriation statutes cover exactly the type of wrongdoing Aleynikov is accused of.” [According to Li](#), the fact that Aleynikov was given access to the algorithm “didn’t give him a right to copy and transfer this data to his own benefit. Furthermore, the state criminalizes behavior like this as a deterrent, and as such, there is an interest in pursuing that objective through prosecution.”

Marino also [reportedly argued](#) that the state case lacked any real purpose: as he indicated that Aleynikov is already penniless and homeless, and since he was released from jail he has had to resort to living on friend’s couches. [According to Marino](#), the federal trial ended Aleynikov’s marriage, and Aleynikov is facing civil litigation with former employer. Marino [further argued](#) that the case should be dismissed in the interest of justice. Assistant District Attorney Li reportedly disagreed, arguing that the “interest of justice” exception did not apply to Aleynikov, who acted willfully and knowingly.

To alleviate his financial losses, Aleynikov [sued his former employer](#) in New Jersey federal district court in September 2012, arguing the company should pay the fees, which are now close to \$2.5 million,



# Trading Secrets



which Aleynikov has spent defending himself in the two prosecutions. In the complaint, Aleynikov pleads that he had exhausted his own financial resources, and should be entitled to “indemnification for the reasonable fees and expenses incurred in his defense,” as he allegedly was still an officer of the company at the time of the trial. On December 14, 2012, the court denied Aleynikov’s motion for summary judgment and motion for a preliminary injunction to require the company to pay his legal fees, finding that there was insufficient evidence on the record at the time of the filing to support either conclusion. Similarly, the court denied the company’s motion for summary judgment and motion to dismiss for the same reasons.

Both the indemnification case and the state criminal case continue to be litigated, and we will continue to keep you apprised of future developments. Similarly, Judge Zweibel is expected to rule on Aleynikov’s motion to dismiss based on double jeopardy within the next month.



*By Jessica Mendelson (February 7th, 2013)*

Interestingly enough, J. Crew's complaint for misappropriation [never explicitly uses](#) the phrase "trade secret." Instead, [J. Crew claims](#) Fenton misappropriated its "confidential and proprietary information [including] product designs, . . . productions schedules, manufacturing resources, and other information concerning [its] business operations," such as budgets and marketing strategies. As the Trade Secrets Institute [explains](#) it, New York has not yet adopted the Uniform Trade Secrets Act, instead, relying on common law. Under common law, misappropriation of trade secrets requires a showing of use. As such, many litigants will simply claim unfair competition, which allows a plaintiff to sue for unlawful misappropriation of property, in order for the defendant to compete with the plaintiff. The property at issue need not be tangible, and as such, is often applied to ideas as well. Here, the difficulty in proving that there was actual use may explain why the phrase "trade secret" is never explicitly mentioned in the complaint. The case also highlights the importance of careful pleading, particularly in states which have not adopted the Uniform Trade Secrets Act.

# Trading Secrets



## Recent California Supreme Court Decision Stokes Debate Over Scope of Trade Secret Preemption

By James McNairy (February 5th, 2013)

Cases defining the scope of the California Uniform Trade Secrets Act's ("CUTSA") preemptive effect have grown in recent years. Preemption (or "supersession" as the California Supreme Court prefers), increasingly is used by litigants to seek dismissal of non-trade secret causes of action pleaded alongside trade secret claims and which allegedly fall within the scope of CUTSA. This has been particularly so since the decision in *Silvaco Data Systems v. Intel Corporation*, 184 Cal. App. 4th 210 (2010), which interpreted broadly—albeit at times in dicta—the CUTSA's supersessive scope, finding among other things that "CUTSA bars [Bus. & Prof. § 17200] claims sounding in misappropriation of trade secrets."



The California Supreme Court has yet to determinatively address the supersessive scope of the CUTSA, but on January 24, 2013, issued an opinion that will likely be used in the ongoing debate over CUTSA supersession. In *Aryeh v. Canon Bus. Solutions, Inc.*, Case No. S184929, analyzing whether the "continuous accrual" rule properly may apply to bar under a statute of limitations theory an unfair competition claim, the court made the following observation:

The UCL affords relief from unlawful, unfair, or fraudulent acts; moreover, under the unlawful prong, the UCL "borrows violations of other laws and treats them as unlawful practices' that the unfair competition law **makes independently actionable**." [emphasis added.] Depending upon which prong is invoked, a UCL claim may most closely resemble, in terms of the right asserted, an action for...**misappropriation** [of trade secrets]... (citing *Glue-Fold, Inc. v. Slautterback Corp.*, 82 Cal. App. 4th 1018 (2000) (emphasis added)).

The court's citation to *Glue-Fold* is interesting. In *Glue-Fold*, the issue on appeal was "whether three different statutes of limitation have run on what are essentially three causes of action for the same wrong—misappropriation of a trade secret." The *Glue-Fold* plaintiff had asserted causes of action for breach of contract (a non-disclosure agreement), misappropriation of trade secrets under CUTSA, and violation of section 17200 of the California Business and Professions Code. *Id.* at 1023.

After expressly noting the non-trade secret claims before it, the *Glue-Fold* court expressly stated that "The Uniform [Trade Secrets] Act as adopted in California provides that its protection does not displace other contractual or civil remedies." (citing § 3426.7, subd. (b).). The court proceeded to analyze the statute of limitations issues before it.

While not too much should be read into *Aryeh*, neither should too little. Other California Supreme Court precedent supports that other civil remedies related to the taking of confidential business information properly may be pleaded alongside claims for misappropriation of trade secrets. See, e.g., *Reeves v. Hanlon*, 3 Cal. 4th 1140, 1155 (2004) (claim of tortious interference to gain unfair business advantage actionable alongside claim for misappropriation under CUTSA).





# Trading Secrets



In time (hopefully sooner rather than later) the California Supreme Court may provide clarification as to the supersessive scope of CUTSA. In the meantime, California businesses will continue to navigate the murky waters of California law related to the unlawful taking of confidential information.

# Trading Secrets



## Second Circuit Largely Affirms \$18.1 Million Trade Secrets Misappropriation Verdict

*By Scott Schaefer (February 14th, 2013)*

On February 6, 2013, the federal Second Circuit Court of Appeals affirmed \$15 million of a \$18.1 million dollar jury verdict (onto which the trial court tacked on an additional \$1.5 million in interest) in favor of a New York subway brake manufacturer on its trade secret misappropriation claim against a former licensee turned competitor. [\*Faively Transport USA, Inc. v. Wabtec Corp., No. 11-3518-cv, 2013 WL 440200 \(2nd Cir. Feb. 6, 2013\)\*](#). The legal issues are interesting, sure, but I'd like to focus on the more valuable lesson of the wisdom of settlement that this case screamed for.



The litigation lasted nearly five-and-a-half years, and involved a Swedish arbitration, two American district court cases and two 2nd Circuit appeals. The lawyers were from globally-renowned law firms. All told, the litigation involved no less than four trials (an arbitration, two preliminary injunction hearings, and a jury trial), two federal appeals, and mountains of briefing in all those proceedings. In the end, plaintiff got \$20 million in damages and interest, with apparently no fee awards. I have to ask: was it worth it?

Here's what happened. Faively claimed that Wabtec took its subway-car air-brake system technology, resulting in Wabtec's landing a subway modernization contract with the New York Transit Authority in 2007 (and perhaps other deals). Between 1993 and 2005, Wabtec designed brake systems under a license agreement with its sister company, SAB Wabco. Faively bought SAB Wabco in 2004, including its licensing agreements, and terminated Wabtec's license effective yearend 2005. Wabtec claimed to have "reverse engineered" its own air brake system prior to the end date, without using any of Faively's drawings or information to which it had access under the license agreement. No less than **seven times** was that claim rejected by an arbitration panel, two federal trial judges, two federal appellate panels, and a federal jury.

Plaintiff Faively European arm first sued Wabtec in October 2007 in Sweden for misappropriation of Faively's trade secret drawings. While the arbitration was pending, that same plaintiff sued in the New York Southern District for an injunction against further use of the Faively's subway brake secrets. The District Court agreed that Wabtec likely misused Faively's trade secrets, and granted the injunction. The Second Circuit also agreed that Wabtec likely misused the secrets, but vacated the injunction due to the absence of irreparable harm.

Back to Sweden, the arbitration panel's December 2009 award rejected Wabtec's claim (its third, by that time) that it properly reverse-engineered its brake system. The panel awarded Faively Europe a \$3.9 million royalty, based on projected profits through 2011. The panel's award apparently excluded any of Faively USA's claims against Wabtec, and the panel reportedly said that Faively USA was the primary victim of Wabtec's trade secret misuse. The award did not appear to include any attorneys' fees.



# Trading Secrets



So, in May 2010, Faively went back to New York, where its USA-arm filed a separate trade secret misappropriation suit based on the air brake system. Wabtec filed a motion to dismiss, which the court denied. Wabtec later filed a motion for summary judgment based in part on its reverse-engineering claim, which the court rejected for a fourth time. In fact, the court granted Faively's motion for summary judgment on Wabtec's trade secret misappropriation liability, and set the case for trial on damages.

Undeterred, Wabtec went to trial on Faively's damages in late June 2011. After trial, the jury rejected Wabtec's argument that it came up with its systems on its own (fifth rejection), and awarded Faively \$18.1 million in compensatory damages. No fees were awarded, probably because New York has not adopted the Uniform Trade Secrets Act, which in section 4 permits attorney fee awards for willful and malicious misappropriation.

On August 1, 2011, the district court denied Wabtec's post-trial motion in which it re-asserted its reverse engineering theory (sixth rejection), and entered judgment on the jury's verdict, plus \$1.5 million in pre-judgment interest. The Second Circuit's February 6th decision again rejected, for a seventh time, Wabtec's argument in its appellate brief that it properly reverse engineered its subway brakes (as well as Wabtec's other arguments).

What did we learn from this case? Protracted trade secret litigation can be very expensive. Only the parties can tell if it was worth it in this case.

# Trading Secrets



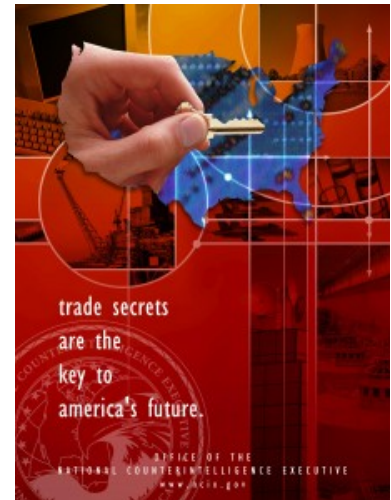
## United States Announces Multifaceted Plan To Combat Trade Secret Theft At Home And Abroad

*By Jessica Mendelson and Robert Milligan (February 21st, 2013)*

On Wednesday February 20, 2013, the White House [released](#) a five-point [plan](#) (“the Plan”) intended to combat trade secret theft of American trade secrets.

The plan is a collaboration between various federal agencies, including the Departments of Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence and the Office of the United States Trade Representative. As a part of the Plan, the Obama administration has pledged to increase diplomatic pressure, consider the possibility of additional legislation, and look to prosecute additional criminal cases in order to combat the theft of trade secrets.

“There are only two categories of companies affected by trade-secret theft: those that know they’ve been compromised and those that don’t know it yet,” Attorney General Eric Holder reportedly said at a White House conference Wednesday [according to the Wall Street Journal](#). “A hacker in China can acquire source code from a software company in Virginia without leaving his or her desk.”



The release of the Plan follows [allegations](#) of cyber hacking by the Chinese military, and [hopefully represents](#) the federal government’s effort to “respond to growing complaints by American companies about the theft of corporate trade secrets by other countries and foreign companies.”

### The Plan

The Plan’s official unveiling took place at the White House on Wednesday, when Obama administration officials from a variety of federal agencies unveiled a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies. The plan consists of five main points: (1) focusing diplomatic efforts to protect trade secrets overseas, (2) promoting voluntary best practices by private industry to protect trade secrets, (3) enhancing domestic law enforcement operations, (4) improving domestic legislation, and (5) promoting public awareness and stakeholder outreach.

### Diplomatic Efforts

Under the terms of the new plan, the State Department will take advantage of diplomatic meetings between countries in order to provide a platform to stress the importance of preventing theft of trade secrets. The Plan [would](#) “increase international engagement,” especially with countries which pose a significant threat of theft of trade secrets from American companies.



# Trading Secrets

## Industry Best Practices

In conjunction with the United States Intellectual Property Enforcement Coordinator (“IPEC”), the Obama administration also plans to assist private companies in developing industry best practices to protect against trade secret theft. According to the Plan, these best practices “should encompass a holistic approach to protect trade secrets from theft via a wide array of vulnerabilities.” Included are a variety of areas for companies to focus on in the development of best practices, such as research and development, human resources, and information and physical security policies.

## Domestic Law Enforcement Opportunities

Another goal of the plan is to enhance domestic law enforcement opportunities. Under the terms of the Plan, both the FBI and the Department of Justice will continue to prioritize the investigation and prosecution of corporate and state sponsored trade secret theft. Furthermore, the FBI will continue to expand its efforts to fight unauthorized computer access involving the theft of trade secrets. The Office of the Director of National Intelligence (ODNI) will also work to inform the private sector regarding prevention of trade secret theft, informing the private sector of industry specific threats, the types of information targeted, and the methods used to conduct such espionage. At the same time, the Department of Justice and the FBI will continue outreach and investigations to prevent and combat the theft of trade secrets.

## Potential New Legislation

The Plan also [includes](#) “a pledge to study whether new legislation is needed to combat trade secret theft.” This past year, President Obama signed two key pieces of legislation, [The Theft of Trade Secrets Clarification Act](#), and the [Foreign and Economic Espionage Penalty Enhancement Act](#), both of which will assist in the prosecution of trade secret theft. The administration will continue to evaluate current legislation, and will discuss the passage of additional legislation, if it is found to be necessary. The Plan may provide momentum for the [Protecting American Trade Secrets and Innovation Act \(“PATRIA”\)](#), which was introduced last year in Congress but did not get out of committee. PATRIA would provide a civil cause of action in federal court for certain trade secret cases.

## Promotion of Public Awareness

Finally, the government will promote public awareness of the growing threat of trade secret theft in the United States in order to mitigate losses. The government will conduct education and outreach through resources like the Department of Commerce’s [www.stopfakes.gov](http://www.stopfakes.gov), which provides useful information regarding trade secret theft, and how to protect trade secrets in priority markets. The United States Patent and Trademark Office will also provide trainings regarding protection of confidential and trade secret information, and the FBI will continue its current outreach programs.

## Impact of the Plan

The Obama administration’s Plan takes a strong stance on the protection of American trade secrets. [According to Robert Hormats](#), the Undersecretary of State for Economic Growth, Energy, and the Environment, the Obama administration’s “message is quite clear: The protection of intellectual property and trade secrets is critical to all intellectual property rights holders, whether they be from the United States or whether they be from Chinese companies or other companies around the world.” Attorney General Holder expressed his hope that the Plan would help combat the increasing threat of cyber-espionage, stating that the Justice Department would continue to make prosecution of



# Trading Secrets



trade secret theft a top priority. According to Holder, the department plans to bring additional economic cyber-espionage cases as a means of deterring foreign governments from hacking into American company's networks.

The Plan voices the Obama administration's displeasure with the theft of trade secrets by foreign governments. Furthermore, the Plan shows how the government can help private companies defend themselves against the sharing of trade secret information, and augment the Department of Justice's law enforcement efforts. [According to Victoria Espinel](#), the White House Intellectual Property Enforcement Coordinator, "Trade secret theft can cripple a company's competitive advantage in foreign markets, diminish export prospects around the globe and put American jobs in jeopardy. The strategy that we are releasing today coordinates and improves U.S. government efforts to protect the innovation that drives the American economy." Some believe that the Plan may lead to [greater cooperation](#) between the Department of Justice and US companies.

Whether the Plan will successfully reduce trade secret theft remains to be seen. [Critics have noted](#) that the Plan continues a number of pre-existing policies, and contains limited details regarding the implementation of new policies. However, regardless of how the details of the Plan play out, it clearly signals that the Obama administration is taking a strong public position against the theft of trade secrets, particularly by foreign governments and companies.



# Trading Secrets



## California Federal Court Allows Non-Signatory to Arbitration Agreement to Compel Arbitration in Trade Secrets Dispute

*By Paul Freehling (February 25th, 2013)*

A federal district court in the Northern District of California recently found that a non-signatory to an arbitration agreement may enforce that agreement against a signatory and compel arbitration under the doctrine of equitable estoppel.

Semin, a software developer, worked for Torbit, Inc. He signed an employment agreement containing a proprietary information non-disclosure provision, and a commitment not to compete while employed. The agreement mandated arbitration “of any dispute or claim relating to or arising out of the employment relationship.” Before resigning, Semin allegedly used Torbit’s computer network to download the company’s trade secrets onto his personal computer, and he created his own company to use Torbit’s proprietary information in competition with Torbit.



After he resigned, Torbit sued Semin and his company in a California federal court. The complaint alleged that he had violated the Computer Fraud and Abuse Act, and that he was liable for various common law causes of action. However, the only count directed at Semin’s company (also pleaded against Semin) claimed trade secret misappropriation.

Both defendants moved, citing the arbitration clause, to compel arbitration of the whole case. Torbit objected partly because Semin’s company, Datanyze was not a signatory to the employment agreement. Based on the doctrine of equitable estoppel, the court overruled the objection and granted the motion to compel. [Torbit, Inc. v. Datanyze, Inc., Case No. 5:12-CV-05889-EJD \(N.D. Cal., Feb. 13, 2013\).](#)

In the course of his employment, Semin helped to develop technology which, according to Torbit, constituted its “most valuable trade secret and one of its top competitive advantages.” The misconduct alleged against Semin alone included unauthorized computer activity and improper use of Torbit’s proprietary information. Torbit resisted Semin’s motion to compel arbitration of those claims, but the court granted the motion and held that the supposed CFAA violation and common law causes of action “touch matters” relating to and arising out of the parties’ agreement. Accordingly, those claims were deemed arbitrable.

The motion to compel arbitration of the trade secret misappropriation cause of action was more problematic because Torbit had not agreed to arbitrate disputes with Semin’s company, and courts ordinarily hold that arbitration is not required absent such an agreement. But the California federal court distinguished those holdings. Stressing that arbitration is a favored method of dispute resolution, the court cited several federal appellate rulings from outside the Ninth Circuit to the effect that a party is





# Trading Secrets



equitably estopped to claim “the benefits of a contract while simultaneously attempting to avoid the burdens that contract imposes.” Equitable estoppel was held to apply to the alleged trade secret misappropriation claims because they were “intertwined with,” “arise out of,” and “relate directly to” the contract providing for arbitration.

Although the Ninth Circuit apparently has not ordered arbitration based on equitable estoppel in a case like *Torbit*, the principle is described in a Ninth Circuit decision cited by the California court, *Mundi v. Union Sec. Life Ins. Co.*, 555 F.3d 1042 (2009). The language in *Mundi* is dicta because the non-signatory there failed to convince the court that the “intertwined with,” “arise out of,” and “relate directly to” standards were satisfied. Yet, the relevant pleadings in *Torbit* and in *Mundi* have some similarities, and so both courts might have reached the same conclusion.

It is difficult to predict, with respect to a specific factual scenario that may arise in the future, how courts in the Ninth Circuit (or elsewhere) will rule on a non-signatory’s motion to enforce an arbitration clause in an employment agreement. In fact, the 5th and 8th Circuits recently [reversed district court decisions](#) allowing non-signatories to compel arbitration.

To minimize the likelihood that the court will order the parties to arbitrate a case like *Torbit*, the complaint should emphasize that the alleged misconduct of the non-signatory fails the “intertwined with,” “arise out of,” and “relate directly to” tests.

# Trading Secrets



## Federal Court Rules That Government's Service Attempts Fail In Criminal Trade Secret Matter

*By Jessica Mendelson (March 4th, 2013)*

A federal judge in Virginia recently [held](#) that the United States Department of Justice's attempts to serve Kolon Industries, Inc. and five of its executives with criminal summons in a high profile criminal trade secrets action were ineffective, finding, among other things, that service on its U.S. subsidiary was not sufficient.

In the complaint, which was unsealed last October, the DOJ alleged Kolon engaged in a multi-year campaign to steal trade secrets from a competitor. Kolon [allegedly](#) poached its competitor's employees over a seven year period, intending to use its competitor's technology for its own research and development projects.

Additionally, Kolon allegedly retained five employees from its competitor for purposes of obtaining information about the company's R & D, pricing, and designs. Kolon's employees also allegedly attempted to obtain additional information regarding its competitor's products from current employees.



In last week's ruling Judge Robert E. Payne of the Eastern District of Virginia [rejected](#) "at least eight U.S. government efforts to serve Kolon," citing the DOJ's failure to serve the parent company, as well as inordinate delays in service.

According to Judge Payne, the government's service on Kolon's American subsidiary failed to meet legal service requirements. Generally, service on a subsidiary does not constitute process on the parent company. There are exceptions to this rule, including establishing that the subsidiary is acting as a "managing or general agent" for the parent. Here, however, Judge Payne found that the DOJ did not make a proper showing of this, since Kolon's subsidiary, not Kolon itself, contracts with American and Canadian customers. Similarly, Judge Payne found that the DOJ failed to successfully allege Kolon's subsidiary, KUSA, was merely an alter ego of Kolon. Here, the DOJ failed to show KUSA was merely a conduit for Kolon or that Kolon dominated KUSA. By contrast, KUSA functioned as a solvent organization with independently audited records and its own Board of Directors.

Furthermore, Judge Payne found the DOJ's service of Kolon failed under the Mutual Legal Assistance treaty between the United States and South Korea, since the service did not occur until a couple of days following the appearance date.

Despite the failure of service, Judge Payne denied Kolon's request to dismiss the indictment entirely, finding that the Department of Justice would probably be able to serve Kolon in the future under the Mutual Legal Assistance Treaty. The United States Attorney's office has already indicated plans to serve Kolon pursuant to the court's order. According to Judge Payne, a new proceeding could occur as soon as June 7th, so long as Kolon is served properly.

# Trading Secrets



## Nuts and Bolts for Terms Commonly Used in Trade Secret Computer Forensic Investigations

*By Guest Author Jonathan Karchmer (March 13th, 2013)*

*As a special feature of our blog – special guest postings by experts, clients, and other professionals – please enjoy this blog post by digital forensics expert Jonathan Karchmer, a Senior Manager with Intelligent Discovery Solutions.*

Computer forensic investigations are commonplace for matters dealing with allegations of trade secret theft. Forensic experts and IT security teams frequently use technological buzzwords and jargon to describe the steps and components of an investigation. Below are some commonly used terms and definitions that describe artifacts regularly examined during a forensic inspection, and also includes some conventional analyses that your forensic expert may provide as part of their report.



- **Computer forensics:** The preservation, examination, analysis, and reporting regarding digital media using methodologies and tools suitable for presentation in legal proceedings. Computer forensics is a specialized area of expertise, and has its own academic degree programs, professional certifications, and associated coursework.
- **Custodian:** A user of a computer system, and/or the owner of the data on a computer. The IT team may refer to the employees and staff as “users” – and the forensic examiners and legal team may use the term “custodians.”
- **Forensic Image:** A bit-for-bit complete copy of electronic data storage media, such as hard drives, USB drives, and optical disks. Also referred to as a “physical image,” these disk images contain all active (or non-deleted) data, as well as unallocated space (or “free space”) from a hard drive – which is where deleted files and their remnants can exist. Creating a forensic image for desktop or laptop systems used by key custodians is the standard in most forensic investigations.
- **Logical Image:** Unlike the above, a “logical image” refers to an image file that contains only a select set of files/folders from storage media. In contrast to a full physical image, a logical image can be created where a physical image may not be feasible, such as larger server disks.
- **Encryption:** Hardware or software encoding employed to secure confidential information. Encryption is enabled in various ways – it can protect entire hard drives, or it can be set to protect specific files or folders. Further, users can setup encrypted or hidden partitions on their own systems. Working with your client to understand what encryption their systems use is key for any collection/preservation effort as it directly impacts how the collection is performed. Frequently, the IT/Security team must work closely with the data collection team to ensure the data collected can be decrypted and reviewed.



# Trading Secrets



- **Hash Value:** Referred to as a “digital fingerprint,” a hash value is a string of alphanumeric characters that is the result of a mathematical algorithm. Hash values or “hashes” are unique to the original media or file from which they were derived. Hashes are used to authenticate evidence, and also used to identify known documents: suppose you have a key document you suspect of being copied to a hard drive. A search for known hashes can determine if that key document in fact resides on the hard drive, or on several hard drives.
- **System Registry:** On a Windows system, the system registry is a database that stores hardware and software configurations and options. From the standpoint of an investigation, the registry can help determine key information: a few examples include when the operating system was installed, which files were recently accessed, what USB devices may have been used recently, and what printers may have been connected to the computer. Corresponding artifacts on Mac systems may include “.plist” files, Preferences directories (folders containing configuration options), and log files. You use many terms in this paragraph that are not defined.
- **File table:** A database on a hard drive that tracks the files and folders stored on the hard drive. The file table is frequently analyzed to determine what files and folders exist, when they were created, and when they were modified. The specific details and operations of a file table vary from one system to another, or from a Mac system to a Windows system, to a Linux system – but the purpose is the same.
- **Shortcut or Link file:** On a Windows system, shortcuts are artifacts that are created when a user opens files, folders, and applications. Shortcut files contain information about the file or application that was opened, and can help pinpoint the source of a file – whether it exists on removable media, and when a file may have been moved or copied.
- **Internet History:** The history of user activity relating to web browsers used on particular devices. Often, analysis of the databases that are used with these applications can show what websites were accessed and when. If out-of-bound communications or file transfer / cloud services are among the results, it may provide new information to help direct an investigation.
- **De-duplication:** The removal of exact duplicate documents or emails from a data set.
- **De-duplication** reduces review time by ensuring that only one instance of any document is reviewed. Consider how many duplicates may exist in any data set as we all send and receive departmental or group emails. If only a fraction of the recipients are in your custodian set, there is a high probability you have duplicate documents across custodians.
- **De-duplication** is performed by hashing (see “Hash Value”) or mathematical algorithms that analyze the contents of data in a document; not its filename, nor the type of file – only the data content. This ensures that even if two or more identical documents have different names – they will still be reviewed only once.
- If you have multiple custodians, normally a **global de-duplication** is recommended: data processing technology exists to allow all custodians in possession of a document to be identified – even if duplicates are removed. A global de-duplication refers to removing duplicate docs from the entire data set, keeping just one “unique” document for review if duplicates are found. A custodian-level deduplication refers to removing only duplicate docs from a single custodian’s data. If a “hot” document is identified, a reviewer can simply look to see which custodians may have also been in possession of that same document. When using global de-duplication, consider using a custodian hierarchy to determine which custodians will have fewer duplicates removed, and which have more. For example: if no hierarchy is applied, a Tier 3 custodian may be in possession of a key “hot” document, while a Tier 1 custodian may not have the document in their data set. This is an unexpected result, and could result in issues or



# Trading Secrets



- delays if more resources are devoted to Tier 1 document review. Assign a custodian hierarchy based on custodian importance/relevance to keep more documents in Tier 1 and avoid surprises. What is a global de-duplication? Elaborate slightly on what a custodian hierarchy is.
- **Timeline:** a process by which multiple artifacts are consolidated and analyzed in order to determine a chronological order of events occurring on a given system. This allows examiners to combine date and time information from disparate areas, system logs, temporary files, and combine them into a uniform body where discrete activities can be sequentially organized.

*Mr. Karchmer is a digital forensics expert. Mr. Karchmer has extensive experience working on litigation and consulting matters involving computer forensics, e-discovery and other high technology issues. He serves his clients through the litigation or consulting lifecycle by assisting them with important issues like data scoping, preserving, gathering, processing, hosting, review and production, as well as deeper diving issues uncovered through the use of computer forensics. Mr. Karchmer can be contacted at [jkarchmer@idiscoverysolutions.com](mailto:jkarchmer@idiscoverysolutions.com). Please note that each case may be unique and this single blog post is not intended to fully cover everything related to trade secret investigations or constitute advice, legal or otherwise. It is always best to consult a qualified person to assist with any investigation.*

# Trading Secrets



## Preliminary Injunction Issued By Nebraska Federal District Court To Level The Playing Field in Trade Secrets Dispute

*By Paul Freehling (March 13th, 2013)*

A federal district court in Nebraska recently issued a significant preliminary injunction preventing trade secret misappropriation and unlawful competition in a contentious dispute between two freight companies. [West Plains, L.L.C. v. Retzlaff Grain Co.](#), Case No. 8:13CV47 (D. Neb., Feb. 26, 2013).



A group of freight forwarders employed by CT Freight allegedly resigned en masse and went to work for start-up RFG Logistics, a CT competitor. Before resigning, they allegedly communicated their intentions with each other and with some CT customers, and supposedly they secretly downloaded to their personal computers CT's marketing information (which they maintained was publicly available). Their departure allegedly decimated CT's freight forwarding department. The employees were bound by a trade secret confidentiality policy and, while employed by CT, a prohibition against competing, but they did not commit to post-employment non-competition or non-solicitation obligations.

CT sued the ex-employees in a Nebraska federal court and moved for a preliminary injunction. The court ruled that CT's compilation of marketing data was a protected trade secret under Nebraska law even if the data itself was not. In the court's view, in order to preserve the status quo and preclude unfair competition, a 60-day preliminary injunction against use of the compiled information would enable CT to rebuild its department and allow RFG to acquire the purloined information from public sources. The resulting playing field would be leveled without foreclosing competition indefinitely.

According to the court, as a result of their pre-resignation conduct, the defendants and their new employer achieved a competitive advantage at CT's expense because their "departure with CT Freight's Confidential Information [left CT] without the personnel to meet its customers' needs, while providing RFG Logistics with both the personnel and the information necessary to compete immediately for CT Freight's business." Consequently, CT demonstrated a likelihood of success on its claims for misappropriation and breach of the duty of loyalty. CT also showed that there was a threat of irreparable harm because of the absence of an easy or quantifiable remedy.

Balancing the harm and protecting the public interest was somewhat more problematic. There was no operative non-competition or non-solicitation agreement. A lengthy injunction would disable the individual defendants from competing for customers with whom the defendants previously had relationships. Further, although the resignations hindered CT from handling its prior volume of business immediately, it had notified its customers that it was working to mitigate the harm. The court reasoned that an injunction of limited duration "gives due regard to both CT Freight's interests and the public interest in free competition."

This case teaches that the victim of a misappropriation of trade secrets may be able to obtain a preliminary injunction against anti-competitive use of the data despite the absence of non-compete and non-solicitation agreements. However, a court might make the injunction period shorter than it typically would be if the parties had entered into a written agreement.



# Trading Secrets



## Trouble in Paradise? Trade Secret Theft Alleged in Hawaii Surrounding Zipline Technology

*By Robert Milligan and Grace Chuchla (March 15th, 2013)*

Ahhh, Hawaii. Crystal clear water, pristine beaches, warm weather – it's the perfect place to relax and enjoy some sun. Well, that is, it's the perfect place to relax until you disclose your trade secrets to a third party contractor who then allegedly breaks its business relationship with you and goes on to allegedly use your proprietary technology with two of your former alleged prospective business partners.

Such was the alleged situation that Cougar Mountain Adventures, Ltd. found itself in in February 2007. Cougar Mountain works in the zipline industry, designing and developing adventure courses that use their proprietary braking technology.



In July 2006, Cougar Mountain allegedly began negotiating with Experiential Resources, Inc. ("ERI"), a subcontractor that would assist in some of Cougar Mountain's zipline course installations and projects. On September 13, 2006, Cougar Mountain and ERI executed a Confidentiality Agreement, after which Cougar Mountain allegedly shared with ERI its confidential and proprietary zipline technology and trained ERI on how to install and operate its zipline courses. [\*Skyline Zipline Global, L.L.C. v. Domeck et al., Case No. 12-00450 JMS-BMK \(D. Hawaii\)\*](#) (the court clarified its initial order following a motion by plaintiff).

Enter two alleged prospective business partners interested in Cougar Mountain's zipline technology. Both allegedly met with a Cougar Mountain representative in late 2006 to discuss the possibilities of forming a zipline partnership and/or developing ziplines for their resorts. In October 2006, after delivering course design proposals to both prospective business partners, Cougar Mountain allegedly brought ERI into both of these deals, again allegedly sharing with ERI their proprietary technology and inside information regarding the negotiations.

Things were apparently going swimmingly and both projects were allegedly moving full steam ahead until February 2007, when one of the business partners allegedly cancelled its Letter of Intent with Cougar Mountain and the other partner allegedly abruptly and inexplicably stopped all communications. Three months later, in May 2007, a Cougar Mountain executive read a newspaper article about one of the partner's plan to develop a zipline course. With his suspicion allegedly raised, the Cougar Mountain executive emailed ERI and asked if they were involved in the partner's zipline course. ERI allegedly denied any involvement, and Cougar Mountain did not press the matter.

However, in September 2009, the Cougar Mountain executive allegedly saw photos of one of former alleged partner's zipline course and allegedly immediately recognized Cougar Mountain's proprietary braking system and patent-pending trolleys. Around this same time, the executive allegedly also learned from the other former alleged prospective partner's website that ERI was involved in the construction of its zipline. With this information, Skyline Zipline Global, LLC (a previously uninvolved fourth party that had assumed Cougar Mountain's intellectual property rights) filed a complaint against





# Trading Secrets



ERI and two business partners, on August 28, 2012, asserting patent infringement, breach of contract, trade secret misappropriation, fraudulent concealment, and tortious interference.

On October 31, a motion to dismiss was filed asserting that 1) Cougar Mountain did not take reasonable steps to keep its proprietary information secret and 2) Cougar Mountain's claim was time-barred because they should have discovered the alleged misappropriation in 2007.

Defendants' argument was based on the claim that Cougar Mountain's technology does not constitute a trade secret because they revealed their supposedly proprietary information to the alleged business prospective partners without obligating them to keep the information confidential. However, in its reply, Cougar Mountain disavowed that its misappropriation claim against the prospective business partners was based on the theory that Cougar Mountain disclosed trade secret information directly to them prior to having them sign a confidentiality agreement. Rather, it stated that it provided only general information and the basis of its trade secrets claim against them is that the alleged prospective business partners knew of Cougar Mountain's confidential relationship with ERI and used ERI as their vendor knowing that ERI was allegedly using Cougar Mountain's trade secrets. The court accepted this argument, and [denied](#) the motion with respect to the trade secret misappropriation claim. The court, however, narrowed the trade secret misappropriation claim to the allegation that the alleged prospective business partners obtained trade secret information through ERI and/or that one of the business partners obtained trade secret information after it signed a confidentiality agreement in connection with its letter of intent.

The court then turned to the statute of limitations argument. The Hawaii Uniform Trade Secrets Act states that all actions for misappropriation "must be brought within three years after [it] is discovered or by the exercise of reasonable diligence should have been discovered" (HRS §482B-7). More than three years had lapsed since Cougar Mountain questioned ERI about its involvement with the alleged prospective business partners, and thus, the court had to decide whether Cougar Mountain executive's inquiry to ERI and ERI's subsequent denial of any involvement with defendants' ziplines constituted "reasonable diligence." Although the Hawaii Supreme Court had never directly decided this issue, the court looked to other Hawaii and California court decisions and found it "plausible (at least at this pleadings stage) that ERI Defendants' assurances that they were not involved with [one of the business partners] would end a reasonable investigation."

Finally, the court ended with some good news for the defendants, and dismissed Skyline's claim for fraudulent concealment with leave to amend, finding that Skyline's general assertion that defendants made "false statements" was not enough to prove misrepresentation on part of the two alleged prospective business partners. Indeed, if any fraudulent misrepresentation or omission occurred, the court found that it was carried out by ERI, not the alleged prospective business partners.

So what does this glimpse into trouble in paradise demonstrate? First and foremost, if you do disclose trade secrets to third parties, make sure that you have NDAs with all the parties' involved and prohibit the sharing of such information outside the authorized individuals expressly provided for in the agreement. And don't disclose any trade secrets until you have a signed NDA. Think ahead, plan accordingly, and always look to close loopholes and backdoors through which competitors or erstwhile prospective business partners could misappropriate your confidential and trade secret information.

Regardless of the underlying merits of this case, the allegations in this case serve as a cautionary tale to always be vigilant, responsible, and proactive when it comes to protecting trade secrets and confidential information.

# Trading Secrets



## Growing California Trade Secret Preemption Doctrine May Thwart Efforts To Combat Employee Data Theft

*By Robert Milligan, Jessica Mendelson and Daniel Joshua Salinas  
(March 28th, 2013)*

Company information that is sensitive, but may not rise to the level of a trade secret is protectable in California, isn't it?

Not necessarily. Some recent California decisions have significantly limited an employer's ability to pursue certain claims and remedies based upon the theft of **mere** confidential or proprietary information by rogue employees.

Defendants (often individual former employees) who are sued in California for stealing a company's data are increasingly using the **trade secret preemption doctrine** to seek dismissal of non-trade secret claims, which are often pleaded alongside trade secret misappropriation claims, that allegedly fall within the scope of the [California Uniform Trade Secrets Act](#) ("CUTSA").

Non-trade secret claims advanced by the employer typically include:

- conversion
- interference with contract
- interference with prospective economic advantage
- breach of fiduciary duty
- unjust enrichment
- fraud
- statutory claims brought under Bus. & Prof. Code section 17200.

These claims are typically made because they are often easier to prove than the elements of trade secret misappropriation.

While trade secret preemption does not displace breach of contract claims, it can significantly limit the claims and remedies that companies may seek when their confidential or proprietary information is stolen.

### Differences Among the States:

**Other States:** The breadth and scope of trade secret preemption varies from state to state. While some states have held that preemption eliminates alternative causes of action for misuse or theft of confidential, proprietary or trade secret information, other states allow common law claims to be brought for the theft of confidential or proprietary information alone or along with trade secret misappropriation claims.





# Trading Secrets



**California state courts:** In California, CUTSA generally preempts causes of action that rely on the same “nucleus of facts” as a trade secret misappropriation claim. A recent California Court of Appeal decision reaffirmed that CUTSA provides the exclusive civil remedy for conduct falling within its terms, so as to supersede other civil remedies based upon misappropriation of a trade secret. Accordingly, California state courts typically do not allow both trade secret and non-trade secret claims to be brought for the theft of company information.

**California federal courts:** Some California federal courts have been more kind to employers, with some courts not forcing employers to choose until trial which of the claims they will ultimately pursue. A [recent California federal court decision](#), however, refused to permit a plaintiff to proceed on a tort theory for the theft of confidential information at the pleading stages, leaving the pursuit of tort claims for the theft of information not rising to the level of a trade secret unsettled.

Thus, variety is the only consistency when it comes to the application and breadth of preemption under CUTSA in California state and federal court. The California Supreme Court has yet to [determinatively address](#) the supersessive scope of CUTSA, but may eventually resolve this difference of opinion.

## Workplace Solutions:

California employers must be vigilant to ensure that their employees don't share their valuable information with competitors. Employers should employ well-drafted and well-communicated agreements and policies to best protect themselves should a dispute arise. Best practices for employers include:

- Identifying trade secrets or confidential information and adding confidentiality designations on the data
- Creating agreements and policies to protect the secrecy and confidentiality of company trade secret and proprietary information
- Effective employee education and training on importance of protecting company trade secrets
- Effective entrance and exit procedures, including employing exit interviews
- Tailoring non-disclosure of confidential information agreements to protect non-public and valuable information, and specifying examples of genuine confidential information
- Utilizing contractual agreements—not simply employee handbooks or policies—with employees as contractual remedies are not preempted by CUTSA
- Aggressive enforcement against breaches and prevention of data theft

Please see our recorded webinars on [2012 California Year in Review: What You Need to Know About the Recent Developments in Trade Secret, Non-Compete, and Computer Fraud Law](#) and [the Anatomy of a Trade Secret Audit](#) for more details on how to put your company in the best position.

# Trading Secrets



## If a Company in China Steals Your Trade Secrets, Do You Have to Litigate Your Lawsuit in China? Maybe...

*By Randy Bruchmiller (April 12th 2013)*

The theft of trade secrets by foreign companies, especially those in China, from American companies is a hot topic among lawmakers and in the press. A recent [opinion](#) from the Fifth Circuit Court of Appeals dealt a blow to the ability of American companies to bring lawsuits in the United States for trade secret theft in some circumstances, at least in the Fifth Circuit. The American companies that appear to be potentially susceptible to this ruling are those that have facilities in China or another country.



Innovation First International, Inc. ("Innovation"), an American toy manufacturer, filed suit in Dallas, Texas against Zuru, Inc. ("Zuru"), a British Virgin Islands toy manufacturer headquartered in China. It was alleged that a high level designer that worked at Innovation's China facility resigned his position, stole trade secrets, began working for Zuru in China, and used the trade secrets to produce the same robotic toy fish for Zuru that was being manufactured by Innovation. Innovation discovered that Zuru was marketing the same robotic fish when both Innovation and Zuru participated in the Fall Toy Preview in Dallas, Texas in 2011.

The trial court dismissed the case after Zuru filed a motion claiming China was a more convenient forum. The Fifth Circuit Court of Appeals affirmed.

Motions to dismiss based on convenience are rarely granted because courts generally give deference to the Plaintiff's choice of forum. The trial court found that "China has a far greater interest in regulating the conduct of companies doing business in China."

The Fifth Circuit observed:

"The district court recognized that Lu allegedly designed the toy fish at Innovations First's facility in China; Lu negotiated an agreement with Zuru in China; and the robotic fish produced according to that agreement was developed in China. The district court also reasonably concluded that most of the records and witnesses are located in China and their production or testimony can be compelled by Chinese courts."

The Court noted that neither party argued that the law of one forum or the other should apply or that there was an interest in avoiding a conflict with foreign law. Innovation also did not challenge that China is an available and adequate alternative forum. These issues are generally considered by courts when ruling on a motion to dismiss based on convenience. That leaves open the possibility that the ruling could have been different had these arguments been persuasively raised.

The bottom line is that, while some companies may enjoy lower costs to produce products abroad in addition to other benefits, companies run the risk of having to litigate claims such as theft of trade secrets in those same foreign forums.

# Trading Secrets



## Obama Administration's Request for Public Comment on Trade Secrets Law Underscores Importance for Companies to Protect Their Proprietary Assets Now

*By Robert Milligan (April 16th, 2013)*

Trade secrets and cybersecurity are on the national agenda.

Responsible corporate leaders are closely following the issue and must be concerned about the adequacy of their protections and the fallout should there be a breach.

"There are only two categories of companies affected by trade secret theft: those that know they've been compromised and those that don't know it yet," Attorney General Eric Holder recently [said](#).

With the Obama Administration's recent [plan](#) to combat increasing trade secret theft at home and abroad and an alarming new [study](#) concerning data theft, there has never been a time where companies' trade secret information are subject to greater risks and their security protections are subject to greater scrutiny.



This reality coupled with the ease with which information can be shared or stolen in this digital age requires that prudent companies employ effective strategies to combat trade secret theft.

The aptly entitled global study ["What's Yours Is Mine: How Employees Are Putting Your Intellectual Property At Risk"](#) found that over fifty percent of the departing employees surveyed retained their former company's confidential information and forty percent plan to use it in their new job. Most employees surveyed do not believe using confidential information taken from a previous employer is wrong and most also indicated that their organization does not take action when employees take confidential information. Further over sixty-five percent indicated that their organization does not take steps to ensure that employees do not use confidential competitive information from third parties. Over fifty percent of those surveyed in the United States believe that they should have a right to re-use source code for another company. A large percentage of employees surveyed admitted to transferring company confidential information to personal email, personal devices, or through file sharing applications.

According to recent government [reports](#), the theft of trade secrets from U.S. corporations impacts national security, undermines U.S. global competitiveness, diminishes U.S. export prospects, and puts American jobs at risk. Trade secrets play a crucial role in maintaining America's global competitiveness. The federal government has recently indicated that it wants to ensure that our laws are as effective as possible to address the threat to companies' trade secrets.





# Trading Secrets



The Obama Administration is presently reviewing applicable federal law related to enforcement against economic espionage and trade secret theft. This review is pursuant to its [plan](#) entitled "[Administration Strategy on Mitigating the Theft of U.S. Trade Secrets](#)" issued on February 20, 2013.

The U.S. Intellectual Property Enforcement Coordinator has recently requested public comment on what legislative changes should be in place to enhance enforcement against, or reduce the risk of, the misappropriation of trade secrets.

[Submissions](#) must be received on or before **April 22, 2013**.

While some may believe that no changes are necessary, among some of the suggestions that some companies are considering are supporting a federal civil cause of action for trade secret theft, clarifying that the Computer Fraud and Abuse Act applies to employee data theft, enhancing the penalties for violations of the Economic Espionage Act, clarifying the service requirements in EEA actions brought against foreign actors, and providing U.S. Customs with greater clarity concerning its ability to seize products containing misappropriated trade secrets.

I recently played a leading role in the ABA IP Section's passage of a [resolution](#) supporting a federal civil cause of action for trade secret theft when certain circumstances are present and certain specified requirements.

The resolution calls for a general framework with a federal civil cause of action for trade secret theft including:

- A definition of trade secret that is comprehensible and expansive versus restrictive and overly technical;
- The availability of remedies that is similar to the Uniform Trade Secrets Act, including injunctive relief, royalty damages, attorneys' fees, and exemplary damages;
- A comprehensible definition of what requirements must be met to trigger exclusive federal jurisdiction, which includes, at a minimum, claims involving the theft of trade secrets by or for the benefit of foreign governments, companies, or individuals;
- A seizure order provision that adequately addresses how seized information should be stored or protected, who will gather it, and who will have access to it; and
- A provision addressing the interplay between state trade secret claims brought under the UTSA adopted by the vast majority of states and common law claims when an action is brought under the proposed legislation which does not interfere with the pursuit of those claims under applicable state law.

If you are interested in making a submission by April 22nd, please contact your Seyfarth attorney.

Additionally, in light of this serious and growing threat, you may also consider evaluating your company's existing trade secret protections and updating your protections as needed.

We have found that a comprehensive [Trade Secret Audit](#) is an effective way to protect a company's trade secrets and provide some piece of mind in this challenging environment. According to the Obama



# Trading Secrets



Administration's [plan](#), best practices "should encompass a holistic approach to protect trade secrets from theft via a wide array of vulnerabilities" and the plan singled out areas for companies to focus in the development of best practices in research and development, human resources, and information and physical security policies.

A customized Trade Secret Audit helps your company in identifying valuable information assets and evaluating the strengths and weaknesses of your company's protections. Corrective measures, if needed, are then implemented to help ensure your company's assets are adequately protected, including assisting with effectively managing and protecting computer-stored data. The Trade Secret Audit assesses whether your company has adequate agreements and policies in place to ensure maximum protection and effective employee education and training programs in place. Audit members also work with IT security along with trusted IT specialists to assess the vulnerabilities of your computer network from insiders and outsiders.

A Trade Secret Audit provides your company with a thorough, proactive assessment of your company's information assets, as well as provides an assessment with recommendations for more effective processes. The cost of losing trade secrets and other intellectual property can be immense and an audit can help your company protect valuable assets, reduce exposure for trade secret theft claims, and maximize effectiveness in pursuing offensive claims, as well as keep your company up to date with emerging threats. For more information on a Trade Secret Audit, please see our webinar entitled the [Anatomy of a Trade Secret Audit](#) and [Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours](#).



# Trading Secrets



## California Court Tosses Idea Theft Suit Over LOST Television Show Out to Sea

*By Michael Baniak and Puya Partow-Navid (April 24th 2013)*

Arthur Quiller-Couch formulated seven basic plots for a conflict. Following his formula, every movie and television show can be narrowed down to one of seven basic plots. Although the number of plots may be limited, there are infinite ways to tell a story. In a town like Hollywood, where everyone seems to have a script, there is always a chance that your story may be new; or similar to a story that has already been told, or even worse, a story that has already been sold. Protection of “ideas” in Hollywood can literally be a big deal.



Intellectual property (property of the mind) is protected under copyright, trademark, patent, or trade secret law. Still, it is well known that none of the aforementioned laws protect ideas per se, such as ideas for television series or movies.

However, under California law, ideas still get some protection under the principles of an implied-in-fact contract. The disclosure and submission of an idea may be consideration for a promise to compensate for the disclosure/submission of the idea. Specifically, idea theft claims under California’s “implied-in-fact contract law” require proof of: (1) submission of the idea on an obligation to pay for use of the idea; (2) voluntary acceptance of the submission based on knowledge of the obligation to pay for the use of the idea; (3) use of the idea; and (4) damages. See *Desny v. Wilder*, 46 Cal. 2d 715 (1956) and *Mann v. Columbia Pictures, Inc.*, 128 Cal. 3d. 628 (1982).

In idea submission cases, the framework for proving use is nonetheless parallel to showing copying in a copyright claim. The elements of a copyright infringement are ownership of the copyright and actual copying by the defendant. *Meta-Film Associates, Inv. v. MCA, Inc.* 86 F. Supp. 1346, 1354 (1984).

Copyright protects the creative expression of an idea, the idea in and of itself is not copyrightable. Thus, if the author confides his idea to a friend and the friend uses the idea to make a movie, there is no copyright infringement. The exclusion of ideas from copyright protection may be found in 17 U.S.C. § 102(b).

In [\*Spinner v. American Broadcasting Companies, Inc. \(ABC\)\*](#), Spinner alleged that ABC developed and produced the television show *LOST* from a script Spinner submitted to ABC in 1977. The Court of Appeals affirmed the lower court’s finding of summary judgment, finding that Spinner failed to produce evidence that ABC used his materials. Furthermore, the Court of Appeals found that ABC established the independent creation of *LOST*, an absolute defense to idea theft.

Spinner was retained by ABC in 1977 to draft a pilot and entered into an agreement that was to pay Spinner \$30,000 for his services. Spinner submitted a script for a two-hour pilot titled *L.O.S.T.*. The show was based on people stranded in the Himalayas as a result of a plane crash. While in the Himalayas, the survivors entered a mountainside tunnel and were transported to a prehistoric



# Trading Secrets



world. The show centered on the survivors attempt to survive in the prehistoric world where they come up against creatures and primitive human beings.

ABC passed on the 1977 script. Time passes and in 1991 Spinner submitted a new treatment of the 1977 script to ABC. Spinner also submitted a third treatment in 1994. The updated treatments moved the story from the Himalayas/prehistoric world to outer space. Still, ABC passed on the updated treatments. More time passes.

In 2003, Lloyd Braun first thought of the concept of what would be the television show *LOST*. Braun stated that the concept was based on a marriage of the concepts from *Survivor* and *Cast Away*. At the time, Braun was the chairman of the ABC Entertainment Television Group. Braun pitched his idea of *LOST* to other ABC executives at an ABC retreat. After reviewing an initial draft by a contract writer, Braun hired J.J. Abrams and Damon Lindelof to draft a script. In 2004, a brainstorming session was held, and Lindelof drafted detailed notes based on the brainstorming session between Lindelof, Abrams, and ABC executives.

A script for the pilot was submitted on February 24, 2004. The script and the general format of the show were finalized by May 2004 and ABC premiered the pilot of *LOST* in September 2004. For *LOST*, the time between drafting the script and airing the pilot was very fast, even by Hollywood standards.

Spinner alleged that the concept of the *LOST* series that premiered in September 2004 was based on the idea he originally submitted to ABC in 1977, and that ABC could not possibly have been able to go from concept-to-premiere so fast without his 1977 script.

The *Spinner* Court first focused on the use element. Spinner did not have direct evidence that ABC used his script. Still, Spinner tried to infer use by alleging that ABC had access to his idea. Additionally, Spinner inferred use by alleging that the idea for *LOST* was similar to Spinner's script.

To show proof of access, and lack thereof, both Spinner and ABC relied on copyright infringement cases. Typically, copying is proven via circumstantial evidence of access and substantial similarity. *Meta-Film Associates, Inv. V. MCA, Inc.* 86 F. Supp. 1346, 1354-55 (1984). Access means that the defendants had an opportunity to view or to copy plaintiff's work. *Id.* at 1355.

Spinner predicated access on the theory that the development executives of *LOST* had a reasonable opportunity to view Spinner's 1977 script, because ABC had a policy of permanently retaining unreturned scripts; his script had not been returned. Spinner thus alleged that the script must have been accessible in an ABC "script library."

However, a search for Spinner's 1977 script yielded no results from ABC's drama development files. Moreover, ABC maintained that there was no centralized "script library" where executives can search and access scripts. Finally, the people that worked at ABC in 1977 and had knowledge of Spinner's script were long gone, and there was absolutely no evidence that any of them had ever talked to the creators of *LOST*.

Accordingly, the Court found that Spinner had only shown, at best, a bare possibility of access based on speculation, supposition, and guess work. Thus, any inference of use would have to be based only on substantial similarity. In an idea submission case, similarities that do not result from copying are



# Trading Secrets



“similarities... without legal significance.” *Teich* at 804. Therefore, any alleged similarity between *LOST* and Spinner’s idea was of legal insignificance.

The Court then focused on evidence that *LOST* had been independently created. When a plaintiff, such as Spinner, infers use of the idea, the inference can be negated by evidence that conclusively demonstrates that the defendant independently created the work. The evidence of independent creation must be “clear, positive, uncontradicted and of such a nature that it cannot rationally be disbelieved.” *Teich v. General Mill, Inc.*, 170 Cal. 2d 791, 797 (1959).

In *Spinner*, the evidence of independent creation included development notes from Braun’s initial pitch at the company retreat, the first draft of the script written by the contract writer, and notes from the brainstorming session attended by the ABC executives and the writers of *LOST*. In summary, the Court was able to see the evolution of the *LOST* television show, without any influence of Spinner’s idea. Therefore, the Court held that ABC established the independent creation defense as a matter of law.

The Court in *Spinner* nicely elucidated the framework for the use element of idea theft cases based on an implied-in-fact contract. Although *Spinner* was directed to the entertainment industry, implied-in-fact contracts exist in all industries, such as technology, advertising, and consumer products.

Those who produce “ideas” should document milestones in the development process. This applies to both sides, but perhaps with different objectives. As seen in *Spinner*, the documentation, such as meeting transcripts, brainstorming notes, and script outlines, were essential in ABC’s defense for independent creation. Contrast that with ABC’s policy for retaining unreturned scripts. Spinner predicated his use theory based on ABC’s retention policy. Had ABC retained Spinner’s 1977 script, and had it shown up in ABC’s drama development files, the story may have come out differently (at least on summary judgment) for Spinner.

Those who believe that their “idea” has been purloined, should remember that in an idea theft case based on the implied-in-fact contract, similarities that do not result from copying are similarities without legal significance. In most jurisdictions, ideas are as “free as air,” and being essentially “free,” courts look with a very jaundiced eye on those who would charge for the thought.

# Trading Secrets



## Illinois Federal Court Issues Preliminary Injunction Prohibiting Use Of Misappropriated Trade Secrets But Rejects Request For Expanded Injunction Based On Alleged “Inevitable Disclosure”

*By Paul Freehling (April 28th, 2013)*

A recent Illinois trade secrets and non-compete decision involving a 3D printing salesman serves as a reminder that some Illinois courts will scrutinize overly broad non-compete provisions and may limit injunctive relief to the territory that the employee actually serviced for their former employer. [\*Fisher/Unitech, Inc. v. Computer Aided Technology, Inc.\*, Case No. 13 C 2090 \(N.D.Ill., 4/9/13\).](#)

**Preliminary injunction granted.** The salesman signed an employment agreement containing confidentiality and non-compete provisions. Subsequently, after accepting a position with a competitor, he allegedly misappropriated his former employer’s trade secrets and provided them to his new employer. His former employer filed suit in an Illinois federal court. On the plaintiff’s motion, the court entered a preliminary injunction barring the salesman, while the case was pending, from (a) using or disclosing his former employer’s confidential information in his former territory, and (b) selling his new employer’s competitive products or services to any customer or potential customer with whom he had contact during his previous employment. But his former employer was not satisfied.



**Expanded preliminary injunction denied.** The salesman’s non-competition covenant purported to apply, for two years after termination of his employment, anywhere within 200 miles from any office or territory of his former employer. Relying on the “inevitable disclosure” doctrine and the terms of the covenant, his former employer asked the court to enter an expanded preliminary injunction prohibiting him during the pendency of the lawsuit from competing anywhere within that 200-mile area. The court denied the request.

**Inevitable disclosure of what?** The inevitable disclosure doctrine provides that an employee who had access to the former employer’s confidential information invariably will make use of it, consciously or subconsciously, in the course of subsequent employment. The judge asked the attorney for the former employer to describe what had been provided to the salesman, other than confidential information (which was covered by the existing injunction), that warranted protection. The attorney’s response was: “field experience” and “on the job training.” The judge concluded that this type of generalized knowledge is not subject to restriction and, therefore, the scope of the non-compete covenant was “greater than is reasonably necessary to protect the employer’s business interests.”

**Unreasonable geographic area contemplated.** The 200-mile area referenced in the non-compete covenant extended far beyond the salesman’s territory and even into places where the former



# Trading Secrets



employer did not do business. According to the court, there was no showing of a likelihood that the former employer would succeed on the merits, and no demonstration that irreparable harm would result, regardless of where the salesman competed for business while the litigation was pending, so long as the current preliminary injunction was not violated.

**Blue-penciling.** Lastly, the judge considered “blue-penciling” the non-compete covenant to narrow it within reasonable confines. Having found that the ex-employee “will not ‘inevitably’ disclose any information as to which [the former employer] has a protectable interest,” the court refused to blue-pencil.

**What this opinion teaches.** The judge seems to have had two reasons for refusing to expand the preliminary injunction’s territorial scope to coincide with the provisions of the non-compete clause. First, the area purportedly encompassed by the clause was held to be too large, particularly because it dwarfed the salesman’s territory. Second, the court held that the only relief the former employer needed and was entitled to during the pendency of the lawsuit was protection of its confidential information. This second reason seems to have rendered the non-competition clause superfluous. But confidentiality and non-compete covenants can serve quite different purposes. For example, a former employer may be blind-sided by the sudden defection of one or more employees who immediately launch a sales blitz on behalf of the new employer, and in order to compete effectively the former employer may need some breathing room in order to recruit one or more replacements. In the *Fisher/Unitech* case, perhaps a more expansive preliminary injunction would have been entered if the employment agreement had set forth carefully drafted, explicit and separate rationales for each of the two covenants.

# Trading Secrets



## Is Your Company's Customer List Still A Trade Secret If Your Company Uses Labeled Delivery Trucks?

*By Jessica Mendelson (May 4th, 2013)*

Does using a labeled truck identifying your company to deliver products to your clients make your client list publicly available? Will doing so undermine protecting your client list as a trade secret? Last month, the defendant in a case before a federal district judge in California tried to make that argument, and while the case was decided on other grounds, it does pose some interesting questions for trade secret litigants attempting to protect customer lists. While many businesses do not necessarily consider the identity of their clients trade secrets in the Internet and social media age, some still closely guard the identity of their customers and believe that at a minimum such information is confidential or proprietary, if not a trade secret.



On April 8, 2013, the court in [\*Magic Laundry Services, Inc. v. Workers United Service Employees International Union\*](#) granted the defendant's special motion to strike four claims, including misappropriation of trade secrets, interference with contract, defamation, and trespass. The case poses an interesting question, namely, whether the use of labeled delivery trucks for deliveries to clients prevents a company from gaining trade secret protection for their client list. Magic Laundry Services, Inc.'s ("Magic Laundry") lawsuit stemmed from the defendant Workers United Service Employees International Union's ("WUSEIU") alleged attempts to unionize its employees. According to Magic Laundry, Defendant allegedly created flyers describing the poor working conditions at the company, spoke to its customers and sent them letters regarding these conditions. Defendant also allegedly organized a secondary boycott of Magic Laundry's customers, and petitioned both local and national political entities regarding working conditions.

In deciding the motion to strike, the court addressed the following causes of action:

### **Interference with Contract**

Magic Laundry alleged that WUSEIU's actions were designed to disrupt Magic Laundry's contracts with third parties, which made the performance of contracts challenging. Defendant's however, alleged that Section 7 and 8 of the National Labor Relations Act (NLRA) permitted their actions, as it provided the right to unionize. The court agreed, finding that the defendant's actions were "squarely within the purview of the NLRA." Furthermore, there were no allegations of violence which would remove the claim from the purview of the NLRB.

### **Defamation**

Magic Laundry alleged that WUSEIU's actions were defamatory in nature. However, the court found otherwise, holding that Magic Laundry had not made any showing of malice. According to the court, "Magic Laundry apparently concedes that it does not have evidence" to show that some of the statements were false.





# Trading Secrets



## Trespass

Magic Laundry alleged that defendant's members entered their private property. However, Defendant denied the allegations of trespassing, and argued that even if they did enter the property, their actions are exempt under the California law which exempts those engaging in lawful union activity from its trespass statutes. The court agreed, finding Defendant's conduct was exempt, and dismissing the claim.

## Misappropriation of Trade Secrets

Magic Laundry alleged that its customer list, which WUSEIU used to send letters regarding working conditions, was a trade secret, and had been improperly acquired by WUSEIU. The Defendant argued that the information was not a trade secret, since Magic Laundry's market trucks publicly delivered to their clients' locations, and therefore, the clients' locations were public knowledge. The court found no evidence that the list had been acquired via improper means, or that Plaintiff's had properly proved damages. Furthermore, there was no evidence that the disclosure of the client's locations harmed Magic Laundry in any manner. Magic Laundry narrowed the claim to encompass only prospective employees, however, the court still found that there was insufficient evidence to support Magic Laundry's contention that the Defendant was aware of the potential client list was improperly disclosed. Accordingly, the court found that Plaintiff had failed to make a prima facie showing of trade secret misappropriation.

## RICO Claims

Magic Laundry also asserted a number of Racketeer Influenced and Corrupt Organizations ("RICO") claims against the Defendant. The court appeared skeptical of these claims, stating in the order that it "is dubious that Magic Laundry can allege a proper RICO claim." Nonetheless, the court permitted Magic Laundry to amend its claims, but warned that there would be no subsequent amendment of the complaint. The case was subsequently dismissed without prejudice.

## Takeaway

From a trade secret litigation perspective, Defendant's argument that Plaintiff's well-labeled delivery trucks appear in public at the location of their clients was sufficient to render Plaintiff's customer list public knowledge is interesting, particularly since businesses often like to advertise some of their significant customers on their websites or otherwise. The court never specifically adopted this argument, yet it did not reject it either in deciding to strike the claim. Instead, the court found that Plaintiff failed to show damages or improper disclosure. As one [expert](#) points out, the argument "seems like a stretch" and "could place any company that delivers its products to or services its customers using marked vehicles in jeopardy of losing trade secret protection for its client list." Whether courts will adopt this reasoning in future trade secret cases involving customer lists remains to be seen. It serves as a reminder that companies should be careful about their public disclosures to or regarding customers particularly if they consider their customers identity trade secret or confidential information.



# Trading Secrets



## New York State Court Rejects Double Jeopardy Argument In Data Theft Case

*By Jessica Mendelson (May 10th, 2013)*

We have previously [written about](#) Sergey Aleynikov, a former computer programmer for an investment bank who beat federal charges of trade secret theft under the Economic Espionage Act in 2012. Although Aleynikov was initially convicted of these charges, the Second Circuit Court of Appeals overturned his conviction, finding that the trade secrets relating to the source code Aleynikov had taken were not related to a product “produced for. . . interstate or foreign commerce,” and thus, were not entitled to protection under the Act. In response to this decision, Congress passed the Trade Secrets Clarification Act (see [our prior post](#) for additional coverage), which expands the original Economic Espionage Act to include a trade secret related to a product or service used in or intended for use in interstate or foreign commerce. The change was intended to prevent results like the Second Circuit’s decision in Aleynikov.



Although the federal case against Aleynikov has long since ended, Aleynikov is now [facing a second prosecution](#) in the New York state courts. In January 2013, Aleynikov and his attorney argued that these charges were similar to the original federal charges, and were being [brought](#) “only because federal prosecutors couldn’t get him.” Aleynikov’s lawyer, Kevin Marino, argued that the state prosecution amounted to double jeopardy, and violated his client’s Fifth Amendment rights. However, in a ruling [last month](#), Judge Ronald Zweibel rejected this argument, finding successive prosecutions in federal and state court were not prohibited. Furthermore, the successive prosecutions were not barred because the federal and state cases had been filed under separate statutes: the federal charges were filed under the National Stolen Property Act and the Economic Espionage Act, while the state cases were filed under the New York Code. As a result, Judge Zweibel found that this was not a case of double jeopardy.

Additionally, [Judge Zweibel](#) rejected Aleynikov’s argument that the prosecution was “inhuman,” stating, “unfortunately for the defendant, his character does not warrant a dismissal in the furtherance of justice. Judge Zweibel also rejected Aleynikov’s claims that the state charges against him were barred by collateral estoppel. Aleynikov’s attorney, Kevin Marino, [expressed](#) disappointment in the ruling, but “remain[ed] confident Mr. Aleynikov is not guilty and will again be exonerated.”

We will continue to keep you apprised of future developments as the case continues.

# Trading Secrets



## Pennsylvania Appellate Court Orders Sanctions for Plaintiff's Bad-Faith Trade Secret Misappropriation Claims

*By Scott Schaefer (May 28th, 2013)*

On May 17, 2013, a Pennsylvania appellate court, with one of its judges dissenting, ordered that the trial court award attorneys' fees to a married couple whose neighbors wrongfully accused them of trade secret misappropriation regarding flagstone artwork. [\*Krafft v. Downey\*](#), Pa. Sup. Ct. No. 476 WDA 2012 (Donohue, J.).



According to the majority, plaintiffs Jack and Linda Krafft must have known that they did not have protectable trade secrets in their flagstone imaging processes when they alleged that their neighbors, Larry and Jane Downey, violated the Pennsylvania Uniform Trade Secrets Act (PUTSA) by using those processes in their own business. Thus, the court held, the trial court should have made the Kraffts pay the Downeys' attorneys' fees spent in defending against the Kraffts' PUTSA claims for which, by making them, the Kraffts engaged in "subjective misconduct."

**The facts and the trial court's decision.** Between 1995 and 2004, Linda Krafft learned how to transfer artwork images onto flagstone, and refined that process through extensive trial-and-error. In 2004, the Kraffts signed a license agreement with their neighbors, the Downeys, under which the Kraffts taught the Downeys the flagstone imaging process and licensed to them the "Framing on Stone" name. In exchange, the Downeys paid the Kraffts \$20,000, and also agreed to pay 10% of the net sales. The agreement prohibited the Downeys from disclosing the imaging process. After the Downeys stopped paying commissions in 2007 and coined their own imaging brand ("Rock of Ages"), the Kraffts sued the Downers in December 2007 in Pennsylvania state court for breach of contract.

In February 2008, the trial court denied the Kraffts preliminary injunction motion, which apparently hinged on whether the Kraffts' imaging process was confidential. In its written order, the court said that the Kraffts' process was not secret, was in the public domain, and "is not new or unique to" the Kraffts. The Downeys presented extensive evidence during the injunction proceedings showing that prior flagstone imaging patents had expired, and that a number of books and articles available on the internet described the flagstone imaging process.

Undeterred, the Kraffts subsequently filed an amended complaint, including a PUTSA misappropriation claim. The Downeys filed a counterclaim shortly thereafter under PUTSA section 5(1) for the Kraffts having made a bad-faith claim in light of the court's prior order. Just under two years later, not long after the Downeys filed a motion for summary judgment on their PUTSA claim, the Kraffts agreed to withdraw it. Nevertheless, the Downeys asked the trial court to award them their attorneys' fees for having to defend against the PUTSA claim, which the Kraffts knew had no merit. The trial court denied that initial request. The Downeys later renewed that request after the Kraffts obtained a jury verdict against the Downeys for breach of contract (I could not locate the amount of that verdict). The court



# Trading Secrets



refused, holding that the Kraffts did not subjectively know they had no viable trade secrets, apparently relying on the two-prong bad-faith test of “objective speciousness” and “subjective misconduct” first used in California federal court in *Stilwell Dev. Inc. v. Chen*, 1989 WL 418783 (C.D. Cal. Apr. 25, 1989) and applied by a number of federal courts since.

**The appeal, majority decision, and dissent.** On appeal, the appellate court majority refused to adopt that two-pronged approach. The court pointed out that except for California, the few other UTSA state courts which interpreted bad faith under section 5(1) (Oklahoma, Alabama, and Maryland) had not applied the two-pronged test, but instead looked to their own internal law for guidance. Because there was no ‘uniform’ test for that section, the court would not adopt the test for the P[‘Uniform’]TSA.

Even so, the court applied the two-prong test to the Downeys’ counterclaim, because apparently it made no difference. The Kraffts could not have in good faith believed, in light of the trial court’s prior injunction-denial order, that their PUTSA claims had any merit. The court sent the case back to the trial court to determine the appropriate fee award.

Appellate Judge Strassburger [dissented](#). He wrote that under the appropriate standard of review, which requires in part that the appellate court give significant deference to the trial court’s first-hand observations of the party’s conduct and credibility, the appellate court should have upheld the denial of PUTSA Section 5(1) attorneys’ fees. The trial judge was in the best position to determine the Kraffts’ subjective intent regarding their PUTSA claim, and just because they lost their preliminary injunction motion early in the case did not necessarily mean they would lose on their PUTSA claim at trial. Indeed, the Krafft’s succeeded at trial on their breach of contract claim, so the trial court’s finding that the PUTSA claim was not brought in bad faith, Judge Strassburger wrote, did not contradict the evidence so much so as to require the appellate court’s reversal.

**What this means.** The majority opinion did not resolve anything. It extensively examined the two-pronged test, refused to adopt it, but nevertheless applied it. Perhaps the Kraffts will ask the Pennsylvania Supreme Court to review. Or maybe they will settle the case and walk away from their verdict. We will keep an eye out, and update you with any useful developments.

# Trading Secrets



## Hey, I Thought We Had An Agreement: California Appellate Court Allows Party To Seek Attorney's Fees In Trade Secret Case

By Mark Hansen (June 6th, 2013)

### The Agreement

Congratulations! You've just entered into an agreement to settle your trade secret misappropriation case.

Defendants will pay you money damages, and agree that you may move the court for fees and costs under Civil Code section 3426.4, based upon their alleged willful and malicious misappropriation. Defendants reserve the right to oppose and to tax your costs. Under the agreement, the trial court is to retain jurisdiction over the case to enforce the settlement agreement. You and defendants then dismiss the action, noting "Plaintiff to separately seek recovery of fees and costs, subject to opposition."



You may now proceed to seek an award of attorney's fees and costs from the trial court, right?

### Agreement? What Agreement?

This was the situation presented in the recent case of [\*Khavarian Enterprises, Inc. v. Commline, Inc., et al.\* \(May 14, 2013\) \(Case No. B243467\)](#). After entering into this agreement, plaintiff moved for attorney's fees and costs. It also submitted evidence that defendants' misappropriation was willful and malicious. Defendants filed an opposition and a motion to strike the memorandum of costs.

At the hearing, the trial court refused to consider plaintiff's motion. The court held that the settlement of the case effectively barred plaintiff from seeking attorney's fees and costs, thereby nullifying that part of the settlement agreement. The court rejected the notion that, under these circumstances, it could or should review the record to make a finding as to whether defendants' misappropriation was willful and malicious.

Even with plaintiff's monetary recovery and the language of the agreement, the court found that plaintiff was not the prevailing party under the provision of California Code of Civil Procedure section 1032(a)(4) defining "prevailing party" as "the party with a net monetary recovery, [or] a defendant in whose favor dismissal is entered."

Despite having entered into the agreement, defendants argued that the provision was unenforceable because there was no authority or procedure for plaintiff to settle a case under Civil Code section 3426.4, and then ask the court to make a finding of willful and malicious misappropriation.

The court denied plaintiff's motion for fees and granted defendants' motion to strike.



# Trading Secrets



## Oh, That Agreement . . .

The Second District Court of Appeal [reversed](#).

The Court ruled that the parties' settlement agreement was legally permissible and required the trial court to exercise its discretion to determine whether plaintiff is the prevailing party and, if so, whether defendants' acts of misappropriation were willful and malicious, thereby justifying an award of attorney's fees and costs under Civil Code section 3426.4.

The Court observed that in determining which side was the prevailing party, the parties were not bound by the definition relied upon by the trial court. Instead, under Code of Civil Procedure section 1032(c), in crafting a settlement, parties may agree to standards and procedures to which they wish to adhere regarding recovery of attorney fees and costs — which the Court of Appeal pointed out is exactly what the parties in this case did.

The Court added that there is nothing that legally proscribes a plaintiff, who voluntarily dismisses its case after obtaining a net monetary recovery through settlement, from being the prevailing party. Indeed, the Court pointed out that the language in the agreement, authorizing plaintiff to apply to the court for an award of attorney's fees and costs, after dismissing the action, could only mean that the parties agreed that plaintiff was the sole potential prevailing party.

The Court went on to find that the only reasonable interpretation of this language in the settlement agreement was that the parties had agreed to submit to a procedure by which the court would use its discretion to determine whether plaintiff was the prevailing party, and if so, whether defendants committed willful and malicious misappropriation. It added that this approach is neither unlawful nor procedurally impossible; and a contrary interpretation would render that portion of the agreement "empty" and "ineffectual."

Thus, under these circumstances, a trial court may be required to act as fact finder on a post-settlement motion for attorney's fees. Here, because the dismissal was an action in compliance with and required by the stipulated settlement, it did not deprive the court of jurisdiction to consider the fee and cost motions that were specifically contemplated by the settlement agreement. In fact, the language of the agreement obligated it to do so, even if it meant that the trial court would have to engage in considerable fact finding to make such determinations.

## Conclusion

This decision is likely to pave the way for more parties to include provisions in settlement agreements calling for post-settlement determinations by courts as to the right of one side to recover attorney's fees, not just in the trade secret misappropriation context, but in other areas as well.



# Trading Secrets



## In Setting Genes Free, Supreme Court Decision Will Put Greater Emphasis on Trade Secret Protection in Biotech

*By Michael Baniak (June 14th, 2013)*

In a decision awaited with considerable trepidation by the biotech world, among others, the Supreme Court Thursday (June 13) handed down its unanimous decision (9-0) in [Association for Molecular Pathology v. Myriad Genetics, Inc.](#) The Court held “that genes and the information they encode are not patent eligible... simply because they have been isolated from the surrounding genetic material.”

Myriad discovered the precise location and sequence of what are known as the BRCA1 and BRCA2 genes. That information in turn enabled Myriad to develop medical tests useful for detecting mutations in patient’s genes, and therefore determine likelihood for certain cancers. Myriad obtained patents directed to “an isolated DNA coding” for those genes. Other Myriad patent claims were directed to “complementary DNA,” called “cDNA,” which omits portions of the genetic sequence within the naturally occurring DNA. Plainly stated, cDNA is a synthetic creation not present in nature.



As to the naturally occurring DNA patent claims, the court held “[i]t is undisputed that Myriad did not create or alter the genetic information” encoded in the naturally occurring genes. Determining the location and order of the nucleotides merely discovered what existed in nature. “[S]eparating that gene from its surrounding genetic material is not an act of invention,” Justice Thomas wrote for the Court. To hold otherwise “would be at odds with the very point of patents, which exist to promote creation.”

What this means is that a company willing to expend the substantial time and millions dollars, if not tens or hundreds of millions, in seeking to discover some aspect of genetic coding that may, or may not, yield a useful product or treatment, will need to think harder about keeping that discovery secret. The Supreme Court decision takes the heart of the target search- -the isolated gene for instance—and dedicates it to the public, if exposed, as would occur in a patent disclosure. A company therefore may consider commercializing the basic discovery in some form but retaining it as a trade secret (if the commercialization does not itself reveal the discovery).

As to the cDNA (i.e. synthetic creation) patent claims, the Court had little difficulty affirming their patent eligibility. “[T]he lab technician unquestionably creates something new when cDNA is made.” Therefore, it is not a product of nature.

The Court acknowledged that the case did not involve method patents on “new applications” of knowledge about mutated genes or gene sequences that have diagnostic or therapeutic value. The Court noted in its decision that “as the first party with knowledge of the BRCA1 and BRCA2 sequences, Myriad was in an excellent position to claim applications of that knowledge.” Myriad’s patent claims to new applications of knowledge about mutated genes remain viable, as they were not challenged.



# Trading Secrets



The concurring opinion of Justice Scalia also highlights what may be considered a drawback of the patent system. His one paragraph concurrence, in essence, states that he really did not understand any of the molecular biology going on, but nonetheless felt the decision sounded right. Jurists untrained in technology, let alone cutting-edge technology, are called upon to make critical decisions on patentability, and judges freely admit the difficulties they face in grappling with some technologies. Trade secrets, on the other hand, rarely see the light of day in a courtroom as to protectability of the technology itself under trade secret law.

Justice Thomas concluded the majority opinion, saying “[i]t is important to note what is *not* implicated by this decision.” First, he noted, method claims were not involved, which could, for instance “involve an innovative method of manipulating genes while searching for” a particular gene. Nor does this case “involve patents on new applications of knowledge about” some gene discovery. Further, the Court did “not consider the patentability of DNA in which the order of the naturally occurring nucleotides has been altered.” The latter may not be viewed as naturally occurring. “We merely hold that genes and the information they encode are not patent eligible under §101 simply because they have been isolated from the surrounding genetic material.” Whether any of the foregoing would also pass muster under the patentability standards of novelty and unobviousness was likewise not before the Court. This bundle of potentially patentable spin-offs from the basic discovery will have to be weighed against the prospect of keeping the fundamental discovery a secret, as a patent directed to such an application of the isolated gene would invariably require the disclosure of the isolated gene itself.

The decision is being viewed by many as something of a victory for both sides. Myriad lost its isolated DNA patent claims, but maintained its patent coverage on the non-naturally occurring cDNA and its unchallenged claims directed to methods of using genetic sequences to aid in the diagnosis and treatment of diseases. cDNA, the synthetic creation not present in nature, is becoming increasingly important in experimentation, testing and the evolving use of synthetic DNA sequences for novel therapeutics. On the other hand, the victory for the parties opposing Myriad is that isolated DNA may have been freed as unpatentable subject matter by today’s decision, for anyone to use and build upon such discoveries. New and unobvious methods and applications that surround those discoveries, and clearly changes made to that isolated DNA not found in nature, remain as fertile ground for possible patent protection.



# Trading Secrets



## Foreign Engineer Arrested For Trade Secret Theft Involving Medical Technology

*By Jessica Mendelson (June 24th, 2013)*

The U.S. Attorney's Office in New Jersey recently [charged](#) a former employee with stealing trade secrets from a New Jersey medical technology company.

The former employee, an Indian national, worked in a group at his former employer responsible for the manufacture of pen injectors and pre-fillable syringes. He resigned from the company last month, and [in the weeks leading up to his resignation](#), "allegedly downloaded 8,000 files containing step-by-step assembly instructions and invoices for equipment to create self-administered disposable pens." [According](#) to the company's own internal probe, he also "forwarded about 60 documents containing trade secrets from his work email account to one of his personal email accounts." He also allegedly called in sick the day before he resigned, but he was "busily downloading" company files using his work laptop, the [complaint](#) says.



Company representatives noticed the suspicious downloads and the authorities were alerted. The FBI then [executed a search warrant](#) for his hotel room, where he was staying prior to returning to India. The FBI seized hard drives, computer storage devices, and computers. The employee also informed agents of his plans to return to India in the next couple days. The agents also discovered evidence that he may have intended to use the trade secrets in future employment, [including](#) "a résumé and an 'entrepreneurial finance book.'" [According to FBI Agent](#) Laurie A. Allen, "The numerous documents containing BD trade-secret information downloaded by defendant Maniar collectively constitute a veritable tool-kit for mass producing the disposable pen," Allen said. This stolen information could be used to set up a competing business.

The U.S. Attorney's Office has charged the former employee with theft of trade secrets for his own economic benefit, and if convicted, he could face up to 10 years in prison and a \$250,000 fine. The employee has [also been sued](#) by his former employer in civil court for trade secret misappropriation in violation of New Jersey's Trade Secrets Act. The criminal case against the employee was temporarily placed on hold by Magistrate Judge Steven Mannion on Thursday June 12, as plea negotiations are currently in progress.

The case highlights the [growing use of criminal prosecution](#) as a tool to dissuade theft of trade secrets. The case also highlights the importance of monitoring employee access to secure company databases and limiting access to important data to a need know basis. Furthermore, companies should consider using additional preventive means to prohibit employees from stealing trade secrets, such as configuring computers to restrict access to external devices, blocking a user from uploading information to a web-based site, and/or utilizing software that blocks employees from sending emails to certain domain names and either highlights or restricts the amount of data that can be sent out by a user. In an era in which data is becoming increasingly portable, companies must increase their vigilance in monitoring the use and export of their data and trade secrets.

# Trading Secrets



## Obama Administration Issues Joint Strategic Plan To Protect America's Intellectual Property

By Misty Blair (June 29th, 2013)

The Obama Administration recently issued its [2013 Joint Strategic Plan on Intellectual Property Enforcement](#), building on the Joint Strategic Plan [issued three years ago](#). In its 88 pages, the 2013 Plan outlines steps for federal agencies to take over the next three years to combat "[IP] infringement that has a significant impact on the economy, the global economic competitiveness of the United States, the security of our Nation, and the health and safety of the American public."



U.S. Intellectual Property Enforcement Coordinator, Victoria Espinel, lauds "a number of accomplishments" achieved since the first Plan (pp. 1-3): increased law enforcement activity against infringers in terms of investigations and seizures; enactment of legislation heightening the penalties for **trade secret theft** and counterfeit drug trafficking; private sector companies' adoption of "best practices" for curbing online piracy and the sale of counterfeit goods; and negotiations of agreements with trading partners for greater protection and enforcement abroad. She notes that "the Administration will continue to improve upon these efforts" to protect an industry that in 2010 reportedly accounted for more than one-third of the U.S. gross domestic product, 60 percent of all U.S. exports, and more than 27 million jobs. She then focuses on three specific issues for ongoing discussion (pp. 5-7): "troubling patent litigation tactics that present a significant and growing challenge to innovation"; "efforts by foreign governments to condition market access or the ability to do business on the transfer of trade secrets or proprietary transfer" ("forced technology transfer"); and the challenges and opportunities presented by "trends and innovations" such as "cloud computing, mobile computing... and 3D printing."

The heart of the 2013 Plan includes 26 specific action items, divided into six goal-oriented categories, to guide the agencies through 2016 and beyond. These items and goals include:

- *Leading by Example* (pp. 13-15): secure the U.S. Government supply chain against counterfeits; and ensure the Government's software use complies with its license agreements.
- *Improving Transparency and Public Outreach* (pp. 15-19): increase openness in enforcement policy-making and international negotiations; maintain communications between federal law enforcement and IP stakeholders; organize an interagency group to evaluate issuance of exclusion orders by the International Trade Commission; educate authors about the fair use doctrine; and raise public awareness both here and abroad of the dangers of counterfeiting and piracy.
- *Ensuring Efficiency and Coordination* (pp. 19-25): increase cooperation of federal, state, and local law enforcement; organize an interagency group to identify new technology for use in border enforcement and other areas; continue the work of key U.S. Embassy IP Working Groups and diplomatic officials abroad; coordinate agencies in the delivery of IP-related



# Trading Secrets



- training and capacity-building programs to foreign judges and other authorities; and consider the institution of copyright and patent small claims court proceedings.
- *Enforcing Our Rights Abroad* (pp. 25-34): expand partnerships between federal law enforcement and international counterparts; strengthen enforcement through international programs such as the World Customs Organization's Cargo Target System; leverage trade policy tools such as Special 301 reviews of the IP protection schemes of trading partners; combat infringing foreign-based and foreign-controlled websites; ensure the continued protection of IP at ICANN as new generic top-level domains are implemented; educate and support small and medium-size enterprises in foreign markets; and study the nexus between counterfeiting activities and unacceptable labor conditions.
  - *Securing the Supply Chain* (pp. 34-39): support efforts to expand the information-sharing authority of the Department of Homeland Security and Customs and Border Patrol; work with international postal operators and private sector-based express carriers to better identify shipments of counterfeit goods; encourage voluntary initiatives in the private sector to curb online IP infringement and illegal internet pharmacies; and combat counterfeit pharmaceuticals and medical devices through track-and-trace systems and destruction of counterfeits.
  - *Creating a Data-Driven Government* (pp. 40-41): coordinate an interagency review of existing legislation, to be completed within 120 days of submission of the 2013 Plan; issue annual reports on the number of jobs and percentage of GDP attributable to IP, with the next such report due in December 2013; and issue annual reports on the agencies' expenditure of resources for IP enforcement.

One blogger at BNA Bloomberg has generated a [comparison of these action items with those listed in the 2010 Plan](#). There are **seven new proposals** in the 2013 Plan, including the one for consideration of small claims proceedings in patent and copyright matters and the one for examination of labor conditions associated with infringing goods.

The remainder of the 2013 Plan focuses on the recent major enforcement activities of the individual agencies (pp. 43-86), including the U.S. Patent and Trademark Office, U.S. Copyright Office, International Trade Administration, Commercial Law Development Program, Department of Homeland Security, Department of Health and Human Services, Department of Justice, and U.S. Trade Representative.

The 2013 Plan was issued on the heels of [another report late last month by the Commission on the Theft of American Intellectual Property](#), an advisory group formed to provide recommendations to the U.S. Congress. The 89-page report outlines the staggering blow that IP theft deals to the American economy, roughly \$300 billion worth of damage per year, with 50 to 80 percent of the blame attributed to theft originating in China. The report also outlines various measures that the U.S. Government may take to remedy the situation, and while some bloggers (see [here](#) and [here](#)) cheered these recommendations, the report was largely criticized by others (see [here](#), [here](#), and [here](#)) who could not get past [two paragraphs in the report](#) (p. 81); the Commission recommended the potential use of certain files — dubbed “ransomware” by the latter group — to “recover or render inoperable intellectual property stolen through cyber means.” **Notably, the Commission recommends the creation of a private civil cause action for trade secret theft under the Economic Espionage Act.**

The 2013 Plan does not address trade secrets in any great detail which is a bit of a surprise as IPEC [published a Notice in the Federal Register soliciting public comments for a legislative review](#) related to economic espionage and trade secret theft earlier this year as part of the [“five point plan”](#)



# Trading Secrets



intended to combat the theft of U.S. trade secrets. One explanation may be that the two plans have different focuses. The ABA IP Section and AIPLA, as well some legal commentators (e.g. [John Marsh](#), [Peter Toren](#), [Ken Vanko](#) and Seyfarth's [Robert Milligan](#)), have come out in support of creating a civil claim in federal court for trade secret theft in some form. Hopefully, we will see more from the Administration on the trade secrets front later this summer to address trade secret theft, particularly by foreign governments, companies, or individuals or for their benefit.

We will continue to monitor developments the Administration and others take in the war against IP theft worldwide with a focus on trade secret protection.



*By Robert Milligan (July 3rd, 2013)*

In coordination with legal counsel, the Company will need to undertake an immediate internal investigation of the employee's activities. The Company should review the information that was taken and determine whether the information was already publically available or whether it contains Company confidential or trade secret information. Additionally, the Company should determine whether multiple copies of the stolen documents exist and whether they have been designated or labeled as confidential or trade secret. The Company should evaluate its internal policies and procedures as well as its agreements with the employee to determine the scope of the employee's violations as well as determine whether the employee has a history of similar violations or conduct. If so, hopefully those prior violations are documented.

The Company should contact the employee and conduct an immediate in-person interview. During the interview, the employee should be confronted regarding the data transfers. The Company should determine whether there is an innocent explanation for the activity, as well as staying mindful of and adhering to its own whistleblower protection policies. The Company should probe the extent of the personal transfers, transfers from others, and whether the employee has disclosed the documents to third parties. The Company should also question the employee concerning the employee's motivations





# Trading Secrets



as well as the employee's awareness of Company policies and agreements prohibiting such activities. The Company should attempt to obtain concessions that the employee's actions violate the Company's policies/agreements. The Company should ask for the employee's immediate cooperation in returning the data and request access to the employee's personal email account as well as any other electronic devices or accounts that contain Company information to accomplish the same. It is important that the Company obtain the return of the data, particularly if the information is confidential or trade secret, so that the Company can attempt to preserve its confidential nature.

Assuming that there is no legitimate reason for the employee's actions, the Company will need to consider appropriate discipline for the situation, including considering suspension or termination of the employee. The Company should have written documentation clearly demonstrating the reason for such discipline was for violation(s) of particular policies or agreements, not in retaliation for any purported whistleblowing. Civil legal theories against the employee may include, among other claims, breach of contract, breach of loyalty, conversion, trade secret misappropriation, and/or a violation of the Computer Fraud and Abuse Act (depending upon the jurisdiction) or similar state computer data protection or access laws. Depending upon the gravity of the situation, the Company may also want to consider approaching law enforcement to consider pressing charges against the employee. If the employee refuses to return the documents and make the employee's accounts and other electronic devices/accounts containing Company data available for inspection to obtain the return of the purloined data, the Company may need to consider seeking immediate injunctive relief in court.

***Before taking any adverse actions against the employee, however, the Company needs to evaluate the employee's potential claims against the Company and any whistleblower protections for self-help discovery in the particular jurisdiction.*** For instance, in the SOX whistleblower case *Vannoy v. Celanese Corp.*, No. 09-1118, 2011 DOLSOX LEXIS 68 (ARB Sept. 28, 2011), the Department of Labor's Administrative Review Board recognized the tension between legitimate employer confidential policies and employee whistleblower bounty programs, like the provisions in Dodd-Frank that preclude companies from enforcing or threatening to enforce confidentiality agreements to prevent whistleblowers from cooperating with the SEC. The ARB, relying on Internal Revenue Service and SEC whistleblower bounty programs, reversed an ALJ's finding in favor of the employer and remanded the matter for evidentiary hearing to determine whether the employee's taking of company documents by sending them to his personal email account was protected lawful conduct within the scope of SOX.

Similarly in, *Quinlan v. Curtiss-Wright Corp.*, 204 N.J. 239 (N.J. Dec. 2, 2010), the New Jersey Supreme Court, employed a seven factor test to determine the propriety of an employee's taking of company documents to support her legal claims. "The ultimate question under the balancing test is whether the employee's dissemination of confidential documents was reasonable under the circumstances. This type of test is consistent with the general notion that oppositional activity must be reasonable in order to receive protection under Title VII and other similar statutes." In upholding a ten million dollar verdict against the employer, the court found that employer could have terminated plaintiff for taking the documents but not for her counsel's use of the performance review in deposition. The court further found that the plaintiff's attorney's use of the comparator's performance review at deposition was the actual reason for her discharge, and thus plaintiff was indeed discharged for engaging in protected activity. In reaching its decision, the court found the factors supporting plaintiff's position were that plaintiff gave the performance review only to her attorneys, it was directly relevant to her claim, she had a colorable basis to believe that the performance review would not have been disclosed during discovery, and the disclosure of the document was not disruptive because its disclosure did not threaten the operation of the company in any way.





# Trading Secrets



In contrast, in *O'Day v. McDonnell Douglas Helicopter Co.*, 79 F.3d 756 (9th Cir. 1996), the Ninth Circuit rejected the plaintiff's age discrimination claim based upon plaintiff's theft of documents he found by rummaging through files in his supervisor's office on the night he was denied the promotion. "In balancing an employer's interest in maintaining a 'harmonious and efficient' workplace with the protections of the anti-discrimination laws, we are loathe to provide employees an incentive to rifle through confidential files looking for evidence that might come in handy in later litigation. The opposition clause protects reasonable attempts to contest an employer's discriminatory practices; it is not an insurance policy, a license to flaunt company rules or an invitation to dishonest behavior." The Sixth Circuit reached a similar result in *Niswander v. Cincinnati Ins. Co.*, 529 F.3d 714, 718 (6th Cir. 2008).

In sum, courts addressing employee self-help discovery in whistleblower cases have reached differing results across the country. This reality provides Companies with a cautionary message: don't accept the theft of Company documents in violation of Company policies and agreements but tailor your approach to fit the employee's specific claims and your jurisdiction's discovery self-help laws. Courts in whistleblower cases have generally analyzed six factors to determine whether the self-help taking of Company confidential documents is reasonable: (1) how the documents were obtained; (2) to whom the documents were given; (3) the content of the documents; (4) whether the documents were produced in response to a discovery request; (5) the scope of the employer's confidentiality policies/agreements; and (6) the necessity to preserve the evidence by the employee. As evidenced by *Vannoy*, special attention should be given to the employee's specific potential whistleblower claims as certain claims such as SOX claims may provide protection to take Company documents (or at a minimum divulge Company information), particularly if such information is shared with the SEC. Companies should have broad and comprehensive confidentiality policies, which are widely communicated and uniformly enforced and specific care should be given to mark documents as confidential and limit confidential documents on a need to know basis. Careful screening of job candidates and the consistent use of effective entrance and exit interviews are essential. Companies should also consider using data protection software which provide alerts regarding large data transfers by employees, limits the size of data transfers, and blocks specified computer activities, including access to select websites, including file-sharing sites, and/or placing limits or restricting use of USB devices. Also depending upon the jurisdiction, employers may consider computer monitoring and extra technical safeguards to protect mission critical data.

For more information on this important topic, please see our previously recorded webinar entitled [Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing](#). Also, see the [Fairly Competing Podcast](#) on the topic as well.

Today's blog post is part of [Seyfarth's Workplace Whistleblower Microblog Series](#). You can sign up for the entire series [here](#).

# Trading Secrets



## Words Matter: Your Non-Disclosure Agreement May Trump Governing Trade Secret Law

By Jason Stiehl (July 12th, 2013)

Reaching back over a decade, the *Convolve and MIT v. Compaq and Seagate* litigation involves a dispute between MIT, the owner of intellectual property related to signal shaping technology, and Compaq and Seagate.

While the dispute involves many facets, and the Federal Circuit's most recent [ruling](#) included a reversal of a non-infringement finding, notable for current purposes is the portion of the decision holding that the parties' negotiated non-disclosure language served to override any governing state law related to trade secret misappropriation.



### Factual Background

Convolve, through its founder Dr. Neil Singer (then a graduate student at MIT), developed technology to move equipment quickly while minimizing the resultant vibrations. Through its 2000 lawsuit, Convolve alleges that, in 1998, Convolve and Compaq engaged in license negotiations related to the hard drive technology developed by Dr. Singer's research, entering into a non-disclosure agreement ("NDA") to facilitate those discussions. *Opinion*, pg. 8. The agreement specifically identified the confidential information as "storage peripheral market information and technology information" from Compaq and "algorithms and processes for enhancing positioning systems" from Convolve. The NDA further states that the disclosed information must be: (1) marked as confidential at the time of disclosure; or (2) unmarked, but treated as confidential at the time of disclosure, and later designated confidential in a written memorandum summarizing and identifying the confidential information. *Id.* at \* 8-9. Convolve entered into a similar agreement, with similar terms, with Seagate. *Id.* at 9. The parties engaged in several meetings and negotiations. During the first meeting, the information provided by Convolve was clearly identified as confidential, and a subsequent memorandum was sent confirming that all information discussed was confidential. However, on two subsequent meetings, Convolve did not state in writing that any of the disclosures were confidential. *Id.* at \*10.

### The Federal Circuit's Ruling

As required under California law, Convolve identified numerous trade secrets, 15 of which remained at issue at the time of the lower court's summary judgment ruling. *Id.* at \* 11. The lower court ultimately held that several of the claim trade secrets were revealed during these subsequent meetings, and, therefore, Convolve could not seek trade secret protection. *Id.* at \*12-14. On appeal, Convolve argued: (1) enough evidence existed that the information was presented under the protection of the NDA; (2) the parties course of conduct allowed for a broad interpretation of the NDA, not requiring specific identification of trade secrets as confidential; and (3) a claim still existed, regardless of the NDA, for the tort of trade secret misappropriation. *Id.* at \*19. After rejecting the "sufficient evidence" argument, *id.* at \*21, the Court undertook an analysis of the "broad construction" argument. The Court likewise rejected this argument, holding that the intent of the parties was clear not only from the plain



# Trading Secrets



language of the mutually drafted agreement, but also by their conduct. Specifically, because the parties followed-up the first meeting with a written memorandum identifying all discussions as confidential, the Court found that the intent of the parties was clear that such memorandum was required. *Id.* at \* 25. Finally, and perhaps most notably, the Court rejected the argument that trade secret law supplements any obligations under the NDA. The Court noted that, under general principles of contract law, a written memorandum supplants any oral or implied understanding, citing *Union Pacific R.R. Co. v. Mower*, 219 F. 3d 1069, 1076 (9th Cir. 2000). *Id.* at \* 26. Further, the Court noted that the California Uniform Trade Secret Act required a similar finding, as misappropriation only occurs under circumstances that give rise to a duty to maintain secrecy. Cal. Civ. Code § 3426.1(b). The Court concluded that those circumstances, here, were governed by the NDA. *Id.* at \* 27.

## Implications

While this decision applies to a specifically negotiated license agreement, the ruling may have broad implications as to any contractual relationship between parties, including an employee-employer relationship. As most non-competition agreements contain paragraphs defining confidentiality obligations, companies should take care to ensure that they do not place obligations upon themselves greater than those required under governing trade secret law, as the Court found Compaq, Seagate and Convolv did here. While some courts ultimately may require appropriate markings for confidential information, by placing such a strong ongoing obligation on the parties via their NDA, Convolv was found to have involuntarily revealed what it believed was protected.

# Trading Secrets



## Are Sunny Skies Ahead for Plaintiff After Clearing An Early Hurdle in A Trade Secret Case Involving Weather Service?

*By Jessica Mendelson (July 25th, 2013)*

A New Jersey district court judge recently declined to dismiss trade secret claims against the Weather Channel, finding that the plaintiff Events Media Network Inc. (“EMNI”) had alleged sufficient facts to state a claim of trade secret misappropriation under the Georgia Trade Secrets Act.



The parties first entered into a licensing agreement in the spring of 2008. EMNI agreed that it would provide the Weather Channel with access to a continually updated database of information, including schedules for events and attractions throughout the United States. This information was compiled based on publicly available information. The Weather Channel was given broad rights to use and distribute this information, [however](#), “EMNI retained proprietary rights to the information and imposed confidentiality requirements on its use.” Following the expiration of the agreement in 2011, some of these confidentiality provisions survived, and EMNI filed suit, alleging that the Weather Channel had misappropriated the information, and used it for purposes beyond those permitted by the contract, such as building maps and creating weather products.

The Weather Channel filed a motion to dismiss the claims, [alleging](#) that EMNI was “attempting to expand a simple contract dispute into a tort action for conversion and misappropriation of trade secrets.” Defendants also argued that the fact that the information at issue was publicly available and could be displayed publicly under the terms of the licensing agreement demonstrated that it was not a trade secret. The court, however, found otherwise, finding the pleadings sufficiently alleged a violation of the Georgia Trade Secrets Act to survive a motion to dismiss. Here, the plaintiff allegedly [earned](#) a “competitive advantage from compiling publicly available information,” and thus, “those public domain elements may be considered to have been integrated into a finished product that is deserving of trade secret protection.” The court found that EMNI had sufficiently alleged that it maintained the confidentiality of a database of information it had licensed to the Weather Channel, and had placed clear limits on the Weather Channel’s dissemination of EMNI’s information.

Defendants in trade secret litigation should use caution in relying on the defense that information is not a trade secret because it is publicly available. While this defense may be applicable in many cases, where the information is compiled into a finished product which provides the plaintiff with a competitive advantage, the court may be wary of this defense (at least made on the pleadings).

In addition, the case raises the issue of whether the terms of a written contract can establish the elements of a trade secret. Here, the parties contractually agreed the information supplied by EMNI was proprietary. EMNI used that provision to argue the Weather Channel had conceded that the information was proprietary, and the court agreed. As [John Marsh](#) points out in his own blog post on the case, “[i]n written agreements negotiated between sophisticated commercial parties, courts will



# Trading Secrets



frequently defer to the language of the agreement.” This is consistent with the recent [Convolve](#) case in which the Federal Circuit found that the parties’ negotiated non-disclosure language served to override any governing state law related to trade secret misappropriation. We will continue to keep you posted with any material developments in this case.

# Trading Secrets



## Pennsylvania Federal Court Affirms Broad Pleading Standard for Uniform Trade Secrets Act and Ability to Plead Preempted Claims in the Alternative

By Rebecca Woods (July 26th, 2013)

According to the allegations in a recently filed complaint, Defendant Implementation Management Assistance, Inc. (“IMA”) hired a long-time employee, Liana Hans, away from competitor Plaintiff Triage Consulting Group, Inc. (“Triage”). Hans allegedly had intimate knowledge of Triage’s proprietary systems and allegedly shared that knowledge with IMA, in derogation of her confidentiality agreement with Triage. IMA thereafter recruited another Triage employee, Sara Lewis, with the expressly stated purpose of allegedly seeking to use Triage’s proprietary information and to steal Triage’s clients. Hans and Lewis allegedly assisted in the development of IMA’s own version of Triage’s proprietary software.



After Triage notified IMA that it believed IMA possessed its proprietary information, IMA allegedly agreed to allow Triage to investigate, to remove any Triage information on its systems, and to pay for the investigation and any removal. Rather than proceeding, however, IMA terminated Hans and allegedly recanted on its agreement to remove Triage’s proprietary information from its system and to pay for the investigation. IMA also continued to employ Lewis.

Triage then brought suit. [Triage Consulting Group, Inc., v. Implementation Management Assistance, Inc., No. 12-4266 \(E.D. Pa.\)](#)

IMA sought dismissal of Triage’s Pennsylvania Uniform Trade Secrets Act (“PUTSA”) and breach of contract claims against Lewis and intentional interference with contractual relations claim against IMA. IMA argued that Lewis’s mere knowledge or acquiescence of Hans’ alleged improper use of Triage’s information did not amount to “misappropriation” under the PUTSA. The court concluded that Triage adequately alleged that Lewis knew or should have known that she was using Triage’s proprietary information to assist IMA in creating copycat systems, and that, in the ordinary course of her business with IMA, Lewis knew or had reason to know that she used Triage’s proprietary information and whoever divulged it had a duty of secrecy to Triage.

The court also denied the motion to dismiss as to the breach of contract claim and tort claim on the grounds that, although the PUTSA generally preempts “tort, restitutionary, and other Pennsylvania law,” the PUTSA does not preempt breach contract claims against Lewis, and the tort claim was properly pled in the alternative.

This case is a cautionary tale for employers seeking to hire competitors’ employees. It also serves to demonstrate the variety of opinion across the country regarding trade secret preemption.



# Trading Secrets



## Conversion Claim for Theft of Confidential Information Not Preempted By Trade Secrets Act

*By Robert Milligan (August 4th, 2013)*

Can Oregon employers bring conversion claims against employees who misappropriate confidential information without having their claims preempted by the state's Uniform Trade Secrets Act? According to a recent Oregon federal district court opinion, the answer is “**yes**”; however, in several other states, the answer is “**no**”.

This result highlights the continued divergence of opinion across the nation concerning the viability of tort or statutory claims based upon the theft of information that may not rise to the level of a trade secret.

It matters because such claims are often easier to prove than trade secret claims, particularly before juries who may have high expectations for trade secret classification. They also provide a wider variety of remedies than contract claims, exposing defendants to liability for all harm proximately caused by the defendants' conduct. Additionally, such claims may not be subject to the stringent discovery requirements for trade secret claims in some states which require the identification of the stolen information with particularity before discovery commences.



Simply put, theft of information claims (whether based upon common law business torts or statute) provide employers with additional leverage to protect their companies from employees and competitors that may use such information but arguably are inconsistent with the preemption provisions found in many states' Uniform Trade Secrets Acts.

In [\*KF Jacobsen v. Gaylor\*](#), Case No. 3:12-cv-02062-AC, — F.Supp.2d —, 2013 WL 2318853 (D. Or. 2013), an employer filed suit against its former employee alleging that, when he departed, he took with him a variety of confidential and proprietary files. The employer's complaint included claims for violation of the Oregon Trade Secrets Act (“OTSA”), the Computer Fraud and Abuse Act, the Stored Communications Act, and conversion.

The employee then brought a motion to dismiss arguing that the employer's conversion claim was preempted by its claim under the OTSA and that a plaintiff may not base a conversion claim on taking copies of information. The employer argued that its conversion claim was not preempted by the OTSA to the extent it sought damages for the conversion of information other than trade secrets and that it had adequately alleged that the employee exercised control over the copied information in a manner inconsistent with the employer's rights as owner of the information. In its complaint, the employer described the documents allegedly misappropriated by employee as “some of which may be additional misappropriated trade secrets of plaintiff *or confidential and proprietary information of plaintiff.*” (emphasis added).



# Trading Secrets



The OTSA supersedes “conflicting tort, restitution or other law of Oregon providing civil remedies for misappropriation of a trade secret.” OR. REV. STAT. 646.473(1). Actions seeking contractual and criminal remedies are not affected by the Trade Secrets Act. OR. REV. STAT. 646.473(2)(a) and (c). Additionally, a plaintiff may still pursue an action for “civil remedies that are not based upon misappropriation of a trade secret.” OR. REV. STAT. 646.473(b).

The court indicated that Oregon courts have not addressed the extent to which the OTSA preempts civil remedies. The court acknowledged that a number of courts in other states have extended the preemptive effect of the language found in OR. REV. STAT. 646.473 to claims that are based on the same operative facts as a claim for trade secret misappropriation. *See id.* (citing *Penalty Kick Mgmt. Ltd. v. Coca Cola Co.*, 318 F.3d 1284, 1297-98 (11th Cir. 2003) and *Hutchinson v. KFC Corp.*, 809 F.Supp. 68, 72 (D. Nev. 1992)). The court further acknowledged that an Oregon federal district court had specifically held that the OTSA preempts conversion claims *based on alleged misappropriation of trade secrets*. *See id.* (citing *Kante v. Nike, Inc.*, No. CV 07-1407-HU, 2008 WL5246090, \*4 (D. Or. Dec. 16, 2008)). (emphasis added).

The employer argued that its allegations were broad enough, when read together to allege that employee may have in his possession information that is not trade secret information and, therefore, not covered by the OTSA. The court found that the term “confidential and proprietary information” could be construed broadly enough to include information that does not fall with the definition of “trade secret” under the OTSA. Consequently, the court found that the conversion claim seeks damages for the conversion of information other than trade secrets, and thus **was not** preempted by the OTSA.

The employee also argued that, even if the employer’s claim were not preempted, the employer still could not assert conversion because he did not interfere with the employer’s ability to access or control their documents. The employee argued that he “merely copied documents...at a time when he had the authority to do so.” The court did not find this argument persuasive. It stated that the “the gravamen of the tort [of conversion] is the defendant’s intent to exercise control over the chattel inconsistently with the plaintiff’s rights.” The court found that employee’s alleged copying, retaining, and sharing of the information with third parties, without the employer’s consent, was inconsistent with the employer’s control over the documents and the information in the documents, and its right to keep the information confidential. Accordingly, the court found that the employer had sufficiently alleged in its pleading that the employee “exercised control over the chattel inconsistently” with employer’s rights to maintain the confidentiality of the information.

With the court’s rejection of the employee’s arguments against the conversion claim, the court **confirmed** that the employer could state a claim based upon the theft of confidential information. There is, however, an interesting footnote in the court’s opinion that could limit the applicability of its analysis. In this footnote, the court stated that conversion “generally covers only chattel or tangible property.” According to the court, neither party raised the issue of whether the employee misappropriated tangible property, rather than intangible property “not subject to conversion.” Accordingly, whether the confidential information at issue (either in hard copy or electronic form) qualifies for protection remains an open question in the case. With the prevalence of information sharing/transfer through email, Drop Box, social media, and flash drives, this is an important distinction to keep in mind and is worth following as the case progresses. Nevertheless for Oregon employers who face the situation of an employee who walks out the door with confidential information, this decision lays out a path to plead a claim for conversion (at least for now).

This decision comes in the wake of several other preemption rulings which have reached different results.



# Trading Secrets



A federal district court in California, for example, [recently held](#) claims for intentional interference with contractual relations, intentional interference with prospective economic advantage, unfair competition, breach of fiduciary duty were preempted or subject to supersession. Other California courts have reached different [results](#).

Additionally, another California federal district court [recently found](#) that a return of personal property claim based on the taking of “confidential, proprietary, and/or trade secret information” was preempted. In that case, the court analyzed three different approaches to preemption employed by California courts. Under one approach, a claim has been found exempt from supersession so long as the claim requires the allegation of “something more” than just trade secrets misappropriation. Another approach has found a claim exempt from supersession unless it is based on the taking of information that is ultimately adjudged to be a trade secret. Lastly, other courts have found information theft claims are only saved from supersession if a plaintiff “assert[s] some other basis” beside trade secrets law for a property right in the information at issue.” In the case, the court granted the motion to dismiss and adopted the third approach “given CUTSA’s breadth and structure, its purpose of promoting uniformity, and the broad superseding effect of the narrower uniform trade secrets.”

The California Supreme Court has yet to [determinatively address](#) the supersessive scope of CUTSA, but may eventually resolve this difference of opinion.

Courts in western states such as [Arizona](#), [Hawaii](#), [Nevada](#), [Utah](#), and [Washington](#) have reached similar results preempting “confidential information” theft claims under their respective trade secret preemption statutes. A Pennsylvania federal court, however, recently [found](#) that preemption should not be determined on the pleadings and a [New Jersey state court](#) determined that common law claims were not displaced by New Jersey’s new trade secret statute.

The only certainty in this area appears to be its variety (even within states). For some best practices to protect confidential information in light of this uncertainty, please see our [previous blog post](#). Additionally, I will be leading a presentation at the [ABA Annual Meeting in San Francisco, California](#) this Friday, August 9, 2013 at 2:00 p.m.-3:30 p.m. p.s.t. on [Hot Topics in Trade Secrets Law Across the Country](#). Please consider attending to learn more about the latest in trade secret preemption and other hot topics in trade secrets law.

# Trading Secrets



## California Federal Court Finds Specific Jurisdiction Over South Dakota Company For Alleged Involvement in Misappropriation of Trade Secrets

By Daniel Joshua Salinas (August 12th, 2013)

A South Dakota company recently found itself subject to personal jurisdiction in California by a California federal court despite its arguments that it lacked sufficient “minimum contacts” to establish such jurisdiction. The district court held that the company’s alleged knowledge of and involvement with a new employee’s alleged misappropriation of trade secrets in California purposefully availed the company to jurisdiction in California. ([\*Integrated Practice Solutions, Inc. v. Wilson\*, 3:13-cv-00088-BTM-WMC, \(S.D. Cal., July 31, 2013\)](#)).



Plaintiff Integrated Practice Solutions, Inc. is a Washington corporation with its principal place of business in San Diego County, California. IPS designs, sells, and services practice management computer software for chiropractors and other healthcare professionals, including features to aid with billing, scheduling patient visits, managing patient records, and tracking inventory.

IPS alleged that it maintains a list of current and prospective customers that it alleges would be extremely valuable to competitors. A dispute arose when a former IPS sales representative and Vice President of Sales joined competitor Future Health Acquisition, Inc. (“Future Health”) and allegedly misappropriated about 6,000 “leads” from IPS’s customer list.

IPS brought action against the former employee and Future Health for, *inter alia*, misappropriation of trade secrets. Future Health subsequently filed a motion to dismiss for, *inter alia*, lack of personal jurisdiction. Additionally, IPS filed a motion to dismiss for jurisdictional discovery.

Future Health contended in its motion to dismiss that it was a South Dakota based company and IPS did not establish sufficient minimum contacts between Future Health and California. Future Health argued that IPS provided no allegations that Future Health had any California residents as employees, any sales to California customers, or any California offices. Moreover, Future Health argued that it did not meet the former employee in California or negotiate his employment contract in California and hiring a California resident alone is insufficient to establish minimum contacts.

The district court rejected Future Health’s arguments and found the court had specific jurisdiction over Future Health based on its involvement with the alleged actions of the former employee misappropriating IPS’s customer list. The district court reasoned that misappropriation of trade secrets is an intentional tort and:

“if [the former employee] did misappropriate the customer list and Future Health did somehow take advantage of that, then Future Health would have purposefully availed itself of doing activities in or directed towards California. It would have committed an intentional act, namely using IPS’s customer



# Trading Secrets



list, an act expressly aimed at California, since that is where IPS is based, knowing that IPS would likely suffer competitive harm as a result.”

The district court further reasoned that IPS offered correspondence from Future Health that implies that Future Health was aware that the sales representative allegedly misappropriated IPS’s customer list. Thus, the court denied Future Health’s motion to dismiss and granted IPS’s motion for jurisdictional discovery, but limited such discovery to the specific issue of Future Health’s knowledge of and possible ratification of the former employee’s alleged misappropriation.

This case illustrates that out of state companies who do not conduct business in California but hire California residents may be subject to personal jurisdiction in the state should a dispute later arise regarding their knowledge of and involvement with a new employee’s misappropriation of trade secrets. This case is similar to the [Vance’s Foods, Inc. v. Special Diets Europe Ltd.](#) case we blogged on last year where a California federal court found personal jurisdiction over a corporate officer who was a citizen of Ireland and his Ireland based corporation based on his alleged international trade secret misappropriation activities. This case also reminds of us the importance of employers expressly explaining to new employees and obtaining their written acknowledgement during the hiring and onboarding process not to bring over, utilize, or otherwise disclose their former employer’s trade secrets. For additional best practices regarding hiring competitors’ employees, check out our Nov. 28, 2012 [webinar](#).



# Trading Secrets



## U.S. Senators Propose Legislation To Strengthen Federal Criminal Trade Secret Laws

*By Robert Milligan (August 13th, 2013)*

Senators Sheldon Whitehouse (D-R.I.) and Lindsey Graham (R-S.C.) recently proposed [a draft discussion bill](#) to amend the federal Economic Espionage Act and enhance criminal trade secret protections.

The amendments would expand the Economic Espionage Act to expressly cover trade secret misappropriation sponsored by foreign governments and theft taken at their request, provide victims with additional procedures to protect their trade secrets in court, protect “strategies” and “negotiating positions” as trade secrets, prohibit hacking of U.S. assets by computers used abroad, and add trade secret theft as a predicate for a RICO claim.

In introducing the draft [legislation](#), Senators Whitehouse and Graham made the following statements stressing the importance of trade secrets and protecting the United States from economic espionage.

“Trade-secret theft and economic espionage threaten American companies and our nation’s economic competitiveness. Foreign thieves and hackers must not be allowed to escape accountability through loopholes in our criminal laws,” Whitehouse [said](#).

“There are different ways people can steal from you: a guy can walk up to you with a gun or he can just hack your computer while sitting on his couch in another country,” Graham [said](#). “Trade-secret theft and economic espionage can become forms of financial warfare.”

Whitehouse and Graham, who serve as chairman and ranking member of the Judiciary Committee’s Crime and Terrorism Subcommittee, indicated in their joint statement that they plan to hold a hearing in the fall regarding the draft legislation.

According to Senator Whitehouse’s [summary](#), the draft bill would make seven key changes to the Act:

(1) **Cover government sponsored hacking** – This proposal would clarify that the statute covers instances in which (a) a foreign government agent steals and relays a trade secret to a private company; or (b) a private thief steals a trade secret at the request of a foreign government and relays the stolen trade secret to a private company.

Proposal: Amend § 1831(a) by adding after “agent,” “or intending or knowing that the offense is committed at the request, under the direction, or on behalf of any foreign government, foreign instrumentality, or foreign agent,”.







# Trading Secrets



(2) **Enhance intervention of interested parties** – This proposal would enhance the opportunity of owners of trade secrets to weigh in on any assessment of the importance of keeping trade secrets confidential.

Proposal: Create a new 18 U.S.C. § 1835(b) “Interested Owners.—The court shall allow an owner of a trade secret at issue in a prosecution under this chapter to file a submission under seal that describes the interest of the owner in a trade secret remaining confidential, and shall consider such submission before issuing an order under subsection (a). The record for an interlocutory appeal brought by the Government shall include the submission made under seal to the court by the owner of the trade secret, and may be supplemented on appeal by a further submission under seal by the owner of the trade secret. No submission under seal made pursuant to this subsection may be entered into evidence in a prosecution.”

(3) **Clarify that the statute covers trade secret theft accomplished through the use of means or facilities within the United States** – This proposal would ensure that the statute would apply to a hacker whose code passes through American computers but who is never physically present in the United States.

Proposal: Amend 18 U.S.C. § 1837 by adding “(3) an act in furtherance of the offense was committed through means or facilities located in the United States and the offense resulted in an injury to an individual or entity located in the United States.”

(4) **Clarify definition of “foreign instrumentality”** – This proposal would ensure that companies that are substantially subsidized by foreign government entities fall within the definition of “foreign instrumentality,” and that a foreign entity led by a foreign agent can meet the definition of “foreign instrumentality.”

Proposal: Amend 18 U.S.C. § 1839(1) by adding “subsidized,” after “sponsored,” and adding “or foreign agent” after “government”.

(5) **Cover theft of negotiating positions or strategies** – This proposal would ensure that stealing negotiating positions or strategies (e.g. from a company or its law firm) is covered by the statute.

Proposal: Amend 18 U.S.C. § 1839(3) by adding “strategies, negotiating positions,” after “plans,”.

(6) **Clarify definition of “benefit” to include any conveyance of a trade secret to a foreign government** – This proposal would ensure criminal liability for all the trade secrets the thief knowingly conveys to a foreign government, not just the ones the thief knows will benefit a foreign government.

Proposal: Amend 18 U.S.C. § 1839 by adding “(5) the term ‘benefit any foreign government, foreign instrumentality, or foreign agent,’ shall include the conveyance of any trade secret to any foreign government, foreign instrumentality, or foreign agent.”

(7) **Make Trade Secret Theft a RICO predicate** – This proposal would ensure that RICO tools are available in trade secret and economic espionage investigations.

Proposal: Amend Section 18 U.S.C. § 1961(1) by inserting “sections 1831 and 1832 (relating to economic espionage and theft of trade secrets),” before “section 1951”.



# Trading Secrets



The Information Technology and Innovation Foundation (ITIF) has praised the bi-partisan efforts of Senators Whitehouse and Graham.

“This bill will enhance the efforts of the U.S. government to create a broader policy framework for addressing cyber espionage and intellectual property theft, which will protect American businesses and jobs and promote the continued growth of the knowledge-based economy,” ITIF President Robert Atkinson [said](#). “It will also serve notice to other nations that efforts to promote hacking of U.S. enterprises and theft of American IP will not be tolerated.”

Unfortunately, the discussion draft does not currently contain language creating a civil claim in federal court for trade secret misappropriation. Senator Whitehouse was a sponsor of the [PATRIA legislation](#) introduced last year which would create such a claim. Both the AIPLA and ABA Intellectual Property Section, as well as some [legal commentators](#), have [supported](#) the creation of a civil claim.

Rep. Zoe Lofgren, D-Calif., however, recently [introduced](#) in the House of Representatives the Private Right of Action Against Theft of Trade Secrets Act, which would create a federal civil claim for trade secret theft, but it is much more limited than the previous PATRIA legislation.

In addition to adding a civil claim, Congress may also want to consider adding legislation making it easier to [serve](#) foreign entities/individuals accused of misappropriating trade secrets, including [revising](#) the Criminal Rules of Civil Procedure, as several high-profile trade secret cases have recently been slowed by [service challenges](#).

Congress has shown the ability to work in a bi-partisan manner to [pass legislation](#) to protect American trade secrets with the passage last year of legislation to expand the definition of protectable trade secrets and increase the penalties for violations of the Economic Espionage Act. It remains to be seen whether Congress will be able to do the same this year but the clock is ticking...We will keep you posted on any material legislative developments.

# Trading Secrets



## Best Practices and Latest Developments in Trade Secret Law

*By Robert Milligan (August 27th, 2013)*

I recently presented on “Hot Topics In Trade Secret Law Across the Nation” at the [ABA Annual Meeting](#) in San Francisco, California.

Here are seven key takeaways regarding best practices and latest developments from the event that you may find useful:

### **Understanding the Importance of Trade Secret Preemption**

Simply put, [trade secret preemption or supersession](#) is the concept that the Uniform Trade Secrets Act (adopted in 47 states) preempts or supersedes all other civil claims for the theft and/or wrongful use of information, except for breach of contract claims. Such claims are typically conversion, unfair competition (common law or statutory), tortious interference with contractual relations or business expectancy, breach of fiduciary duty or breach of duty of loyalty. Additionally, some states do not even permit such claims based upon the theft of confidential information that does not rise to the level of a trade secret. These non-UTSA claims can often be easier to prove than trade secret claims and can provide for tort remedies, rather than mere contract remedies.



In many states, non-UTSA claims are preempted by the UTSA and its preemption provision. [Some states](#), however, still permit plaintiffs to bring such non-UTSA claims along with the trade secret claim and only preclude plaintiffs from pursuing the non-UTSA claims if a determination has been made that the information at issue is a trade secret. There is even variety within states, such as California, where [three separate approaches](#) have been followed by various courts.

While typically viewed as a “lawyers’ topic,” trade secret preemption is a much more significant and important topic that companies must be educated about to effectively protect their information assets. Many are surprised that some courts (following the strict preemption approach) view the UTSA as statute that actually “limits liability” for information theft. In those states following the strict preemption approach, companies are typically left with only two potential claims for the theft of information by former employees or other third parties, breach of contract and trade secret misappropriation. This reality underscores that employers should use confidentiality and non-disclosure agreements, rather than merely employee handbook policies to protect their proprietary information, **so that they are not left with only one claim against a misappropriator.**

Additionally, juries typically have high standards for what information qualifies for trade secret protection so trade secret preemption places added importance on companies thoughtfully classify their information assets and ensuring that valuable information is properly protected through reasonable secrecy measures. It also highlights that companies must have effective onboarding and termination procedures to ensure that employees are effectively educated regarding the importance of protecting company information and to ensure that companies obtain the return of their valuable information when



# Trading Secrets



employees leave. Valuable information assets that are not adequately protected **will leave companies with little to no legal recourse if they are later stolen**. Please see our previous [webinar](#) concerning best practices for protecting trade secrets in the hiring and termination of employees.

## **Importance of Protecting Trade Secrets Throughout Litigation**

Companies often need to be reminded when they initiate a trade secret lawsuit that the information at issue must be protected throughout the litigation process. The parties to the litigation will typically enter into a protective order which limits who may obtain access to documents and information exchanged in the litigation subject to strict confidentiality and non-disclosure obligations. Additionally, the protective order, court rules, and applicable case authority provide the requirements for filing or lodging documents in the litigation under seal when they are submitted to the court in connection with the determination of particular case issues.

While some litigants may view such sealing motions as perfunctory, some courts scrutinize sealing motions and generally evaluate whether it is in the public interest to seal such documents and whether there are other significant interests. The recent *Apple v. Samsung* case in the Northern District of California provides a reminder [that courts independently evaluate](#) whether documents should be sealed regardless of agreements between the parties to the litigation. Parties need to understand that these motions often must be brought to preserve the confidentiality of the information, that they are not inexpensive, and there is also some risk that the court will not always grant the motion.

The importance and cost of preserving confidentiality through the litigation is part of the checklist that plaintiffs should take into account before filing suit. Sensible counsel understand that they must continue to educate the judge throughout the litigation regarding the importance of keeping documents and information sealed in the case. Parties to contracts should also be cognizant that confidential documents and information exchanged during the relationship may later be subject to first party or third party discovery. They should require notification provisions in their contracts providing sufficient time to seek a protective order to protect the confidentiality of information or documents called for in discovery prior to disclosure.

## **Is the Computer Fraud and Abuse Act Still a Viable Weapon in Employee Mobility Litigation?**

Is the Computer Fraud and Abuse Act dead for employers that want to use it against employees who misuse their computer systems? The [Ninth Circuit](#) and [Fourth Circuit](#) have significantly pared down the utility of using the Act in the typical employee data theft scenario. Violations of computer use policies are not typically actionable in these jurisdictions if the employee was provided access to the computer network and the data at issue. Some [jurisdictions](#) still allow plaintiffs to bring CFAA claims for such violations demonstrating that analyzing the individual state and circuit authorities are essential in properly evaluating such claims. Even in the Ninth Circuit, [violations of computer access policies](#), [unauthorized password sharing to obtain unauthorized access to a protected computer](#), and [violations of access revocation](#) restrictions have recently been found actionable. Legislation has [recently been proposed](#) to “reform” the Computer Fraud and Abuse Act which would limit its applicability to pure hacker scenarios. For more information on the debate concerning whether violations of internet terms of service should constitute a violation of the Computer Fraud and Abuse Act, please see our [webinar](#) on “How Big Data Impacts Trade Secret, Computer Fraud and Privacy Law.”



# Trading Secrets

## **Dealing with the Employee Whistleblower Who Takes Company Data**

Employee whistleblowers are one of the [more challenging areas](#) that companies must face. A swift investigation is necessary to get a handle on the situation. The employee should be immediately interviewed and the company should make immediate efforts to obtain the return of any truly proprietary data. Civil and criminal remedies will need to be considered, particularly if proprietary company data has been stolen or compromised. All the while the employer will need to comply with its whistleblower compliance program and not retaliate against the employee for engaging in any protected activity. It is not an easy process to balance even for the most diligent employers. Strategies for avoiding these scenarios include, employing hiring best practices, restricting access to key information on a need-to-know basis to only trusted employees, watching for employees who are downloading, transferring, or printing large amounts of documents/information and employing software solutions to prevent such actions, and having a thorough action plan on the shelf to employ for a rainy day. For more information on this topic, please see our webinar entitled "[Employee Theft of Trade Secrets or Confidential Information in Name of Protected Whistleblowing.](#)"

## **BYOD Explosion and Data Security**

More companies are adopting [BYOD policies](#) to permit employees to use their own personal computing devices to access the company network. Companies must institute BYOD policies that protect company information, provide clear limits on access, and provide for clear protocols at termination. As employees can access work and personal email accounts on the same mobile devices, employers must be vigilant that employees do not rapidly transmit company files to their personal accounts. There are also greater risks for data security breaches with the greater accessibility provided by BYOD. Employee education regarding security, including precautions to take outside the office and abroad, file encryption, and the use of secured computer networks is essential.

## **Effectively Conducting a Computer Forensic Investigation**

Companies must keep up to date with the latest ways that valuable information is leaked or otherwise compromised. Such information can be compromised by hard copy theft, emailing of company information to personal accounts, CD burning, and the transfer of data to thumb drives and FTP sites. Companies must respond to the latest threats such as the unauthorized storage of valuable information in the cloud with [third party file sharing sites](#). Many sophisticated companies use software to detect and prevent large data transfers either via email, USB, or third party file sharing sites. Additionally, it is essential to understand what data can be stored on specific electronic devices to understand what may be recoverable in a computer forensic investigation. For example, the iPhone 5, when compared to other smart phones or electronic storage devices, may have material differences in what may be stored and recovered in a computer forensic investigation. Lastly, [social media evidence](#) is becoming more useful in establishing non-compete and trade secret violations, but employers must be cognizant of employee privacy considerations in using and demanding access to social media accounts. Prudent employers [should utilize compliant social media policies and social media ownership agreements](#).

## **Annual Review of Significant Trade Secret Cases Across the Nation**

The ABA Trade Secrets Committee also provided the audience with its [Annual Case Law Review](#). The Review summarizes the most significant trade secret cases in the nation in 2012 and early 2013.



# Trading Secrets

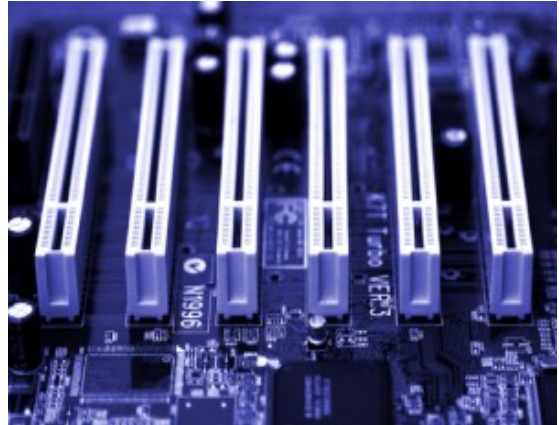


## Court Awards Attorney's Fees for "Bad Faith" Trade Secret Misappropriation Claim

*By Erik von Zeipel (September 5th, 2013)*

The [California Uniform Trade Secrets Act](#) ("CUTSA") allows for an award of attorney's fees to the prevailing party on a trade secret misappropriation claim. The statute permits award of attorney's fees to a plaintiff for a defendant's "willful and malicious" misappropriation and to a defendant when a plaintiff makes a claim in "bad faith":

"If a claim of misappropriation is made in bad faith, a motion to terminate an injunction is made or resisted in bad faith, or willful and malicious misappropriation exists, the court may award reasonable attorney's fees and costs to the prevailing party...."



*Civil Code* section 3426.4.

Since there are relatively few published decisions addressing attorney's fees awards to defendants under the statute, a review of the recent unpublished decision in [All American Semiconductor, LLC v. APX Technology Corp., No. G 046605, 2013 Cal. App. Unpub. LEXIS 5718, \(Cal. App. 4 Dist. Aug 18, 2013\)](#) may serve as a good opportunity to remind prospective plaintiffs of the need to ensure they have a good faith basis for any misappropriation claim before filing suit.

The plaintiff in *All American Semiconductor* had purchased all the assets of a bankrupt company, and, based on statements in the bankruptcy bid solicitation materials, erroneously believed it had purchased the rights to certain proprietary memory module designs. When the plaintiff was unable to locate any design plans for the memory modules among the bankrupt company's assets, and no paper files whatsoever, the plaintiff grew suspicious. Upon finding empty directories on the bankrupt company's computers, the plaintiff concluded that those empty directories must have contained data related to the designs and someone must have erased the data. Based on these mistaken beliefs, the plaintiff filed a nine-count complaint against Richard McCauley, the bankrupt company's former general manager and vice president, his new company, and APX Technology Corporation — the company that *actually* designed the memory modules. Among other things, the complaint alleged misappropriation of trade secrets based on the defendants' supposed misappropriation of the memory module designs.

Discovery, including several depositions, revealed no evidence that the bankrupt company had ever designed any memory modules, let alone had any trade secrets. To the contrary, McCauley testified the bankrupt company did not and could not design the memory modules, as it did not have the software or electrical engineers to do so. Instead, McCauley testified it merely assembled the modules based on designs provided by APX. APX's president testified that APX owned the designs and provided them to memory module assemblers, including the bankrupt company, on a non-exclusive basis. Finally, an electrical engineer at APX testified he had designed the memory modules using complex computer software.





# Trading Secrets



Based on this evidence, APX moved for summary adjudication on the misappropriation claim. The plaintiff opposed, citing testimony from a former shipping clerk of the bankrupt company stating he believed, without foundation, another employee at the bankrupt company designed memory modules. That employee, however, testified he was not an engineer and did not design the modules. The plaintiff also claimed to have found some evidence on the bankrupt company's computers of software that *could* have been used to design memory modules, and offered other speculative testimony suggesting it would have been *possible* for the bankrupt company to design memory modules if it had the right software and tools, but that he had no knowledge of it ever doing so. Finally, the plaintiff blamed McCauley for its lack of evidence, arguing his new company controlled the bankrupt company's employees and suggested that they therefore would not provide evidence adverse to their new employer.

Having failed to offer any evidence the bankrupt company ever designed memory modules, the plaintiff submitted a supplemental opposition claiming instead the bankrupt company had *purchased* the designs from APX citing vague invoices for nonrecurring engineering charges.

The trial court granted summary adjudication in favor of APX and awarded attorney's fees for the plaintiff's bad faith prosecution of the misappropriation claim. On appeal, the Court held that the trial court correctly found that the plaintiff failed to provide any evidence it owned a trade secret. Specifically, the plaintiff failed to identify what constituted a trade secret in any alleged memory module design. Instead, the Court held, the plaintiff attempted to show it could have designed memory modules, based on an inference that some scrubbed data *could* have been software that *could* be used to design memory modules, and that former engineers *could* have designed such modules. Missing was any evidence the bankrupt company actually designed the memory modules, or evidence of what part of the design was trade secret and unknown to the public and competitors.

In affirming the attorney's fee award, the Court explained that the statute does not define "bad faith" and recited case law holding it requires both "objective speciousness" and "subjective bad faith." "Objective speciousness exists where the action superficially appears to have merit but there is a complete lack of evidence to support the claim." *FLIR Systems, Inc. v. Parrish*, 174 Cal. App. 4th 1270 (2009). "Subjective bad faith" will "rarely be susceptible of direct proof; usually the trial court will be required to infer it from circumstantial evidence." *Gemini Aluminum Corp. v. California Custom Shapes, Inc.*, 96 Cal. App. 4th 1249, 1263 (2002). Further, subjective bad faith "may be inferred where the specific shortcomings of the case are identified by opposing counsel, and the decision is made to go forward despite the inability to respond to the arguments raised." *Id.* at 1264. Subjective bad faith exists where a plaintiff intends to cause unnecessary delay, filed the action to harass, or harbored other improper motives. *FLIR Systems*, 174 Cal. App. 4th at 1278. Finally, "[a] court may find subjective misconduct by relying on direct evidence of [the] plaintiff's knowledge during certain points in the litigation and may also infer it from the speciousness of [the] plaintiff's trade secret claim and its conduct during litigation." *Computer Econs., Inc. v. Gartner Group, Inc.*, No. 98-CV-0312 TW (CGA), 1999 U.S. Dist. LEXIS 22204, at \*18-19 (S.D. Cal. Dec. 14, 1999).

In its analysis, the Court found the trial court could reasonably infer objective speciousness from the plaintiff's lack of evidence of what constituted its alleged trade secret designs and that the designs were not known to the public or others in the industry. In addition, APX repeatedly argued from the outset that the plaintiff could not identify any trade secrets because the bankrupt company never designed memory modules. Further, the trial court could reasonably infer subjective bad faith from the plaintiff's prosecution of its claims without evidence, and its shifting theories in opposition to summary adjudication. Finally, the Court dismissed the plaintiff's argument that the trial court erred in not considering self-serving declaratory statements from its president claiming that it filed the lawsuit "in good faith and without improper motive." Bad faith cannot be avoided simply by claiming "it appeared at



# Trading Secrets



the time of the filing of the action some evidence would be obtained in discovery that would support a misappropriation claim.” *SASCO v. Rosendin Electric, Inc.*, 207 Cal. App. 4th 837 (2012).

## Tips for Avoiding “Bad Faith” Misappropriation Claims

*All American Semiconductor* is an unusual case in that the plaintiff was unable to identify its alleged trade secrets because it never actually received the assets it believed it purchased from the bankrupt company. However, there are still lessons prospective plaintiffs can learn from this case to avoid a similar unpleasant fate.

Most trade secret misappropriation claims arise when an employee with access to trade secrets leaves an employer to go to work for a competitor. Fearing the departed employee will use the former employer’s trade secrets to compete, the initial reaction is often to quickly file suit and seek injunctive relief. Before doing so, it is important to recognize that California has rejected the “inevitable disclosure” doctrine. *Schlage Lock Co. v. Whyte*, 101 Cal. App. 4th 1443, 1447 (2002). Thus, mere suspicion of misappropriation is not enough. *SASCO*, 207 Cal. App. 4th at 844. It is therefore essential to do a thorough factual and legal investigation before filing any misappropriation claim. Such investigation should identify any evidence showing: (1) what specific trade secrets are at issue; (2) what reasonable measures were taken to maintain their secrecy; (3) how the departed employee was able to acquire the trade secrets; (4) any threat of misappropriation or damages arising from the misappropriation. If it is suspected the trade secrets were transferred electronically, it is important that a forensic examination of relevant computers and/or other electronic devices be performed by experienced experts. Be mindful that using in-house IT personnel may create potential spoliation issues. Finally, if a defendant identifies alleged problems with a trade secret claim, plaintiffs would be wise to recognize that continuing to pursue the claims without being able to address the identified problems may expose them to bad faith claims if things go south. *Gemini Aluminum Corp.*, 96 Cal. App. 4th at 1264.

# Trading Secrets



## What's for Lunch? Trade Secrets!

*By Jessica Mendelson (September 9th, 2013)*

With the end of summer fast approaching, a new trade secret case filing caught our attention regarding one of the staples of the summer barbecue...the hot dog.

Who doesn't love a good, old fashioned hot dog? It just so happens that a pair of litigants agree with this sentiment! In a case filed in Los Angeles this summer, Dog Haus LLC sued W.S.H Enterprise and its business, King Hot Dog, alleging that confidential information, including the recipes for hamburgers and secret sauces, had been misappropriated. Dog Haus alleges that King Hot Dog convinced two former Dog Haus employees to leave the company and begin working for King Hot Dog. In doing so, the former employees allegedly utilized Dog Haus' proprietary information in violation of their written employment agreements, resulting in economic injury and harm to Dog Haus' reputation and goodwill.



Dog Haus is a California based company with three restaurants in the Los Angeles area specializing in hot dogs and hamburgers. The phrase "Dog Haus" is a registered trademark and trade name. In November 2010, the company hired defendant Asuncion Cruz ("Cruz") as a line cook. Through the course of his employment, Cruz allegedly had access to significant proprietary information, including recipes for the company's sauces and burgers, as well as vendor information. At the time of his hire, Cruz signed an employment agreement prohibiting the dissemination of proprietary information. Similarly, Luis Miguel Cruz Martinez ("Martinez"), a prep cook, also allegedly had access to proprietary information, including the sauces used by the company. Under the terms of their employment agreement, both men were restricted from taking confidential information and sharing it with a third party. However, according to the complaint, Cruz and Martinez allegedly agreed to implement a scheme to secretly misappropriate Dog Haus' proprietary information, as well as its business opportunities, and to sell this information to King Hot Dog. Allegedly, King Hot Dog then began making unauthorized use of Dog Haus' trade dress and trade secrets, including the restaurant décor, the floor plan, the menu, and the serving style. Based on defendants' actions, Dog Haus alleged claims of breach of contract, intentional interference with Dog Haus' business relationships and prospective economic advantage, as well as unfair competition, misappropriation of trade secrets, and trade dress infringement.

From a legal standpoint, it remains to be seen whether and to what extent Dog Haus's recipes, sauces, and décor are a protectable interest or sufficiently distinctive and famous in its look to entitle Dog Haus to injunctive relief against any misappropriation, trade dress infringement or dilution claims arising from a competitor's alleged use of the same or similar products. This is not the first [wiener war](#) that we have seen. The case serves as a reminder that those in the restaurant industry must closely guard their cooking secrets and employ effective non-disclosure and confidentiality agreements. The case is scheduled for a status conference on October 7, 2013. No other hearings have been scheduled as of yet, but we will continue to keep you updated with any material developments in this juicy case.

# Trading Secrets



## Are the Last Episodes of “Breaking Bad” Trade Secrets?

*By Jessica Mendelson (September 11th, 2013)*

Breaking Bad is seemingly everywhere this month. With only a few episodes remaining, die-hard fans of the television show have gone into overdrive. We too, have caught Breaking Bad fever, and started to wonder, do the final episodes qualify as trade secrets? If one of the show's employees were to release the general plot narrative, would the show's owners be able to sue for trade secret misappropriation? For more information, please see [Kenneth Vanko's excellent blog post](#) on the subject.



In order to show that information is a trade secret, the owner must show that (1) it has instituted reasonable measures to maintain the secrecy of the information, and (2) the information is economically valuable because of its secrecy. We will address these factors in turn.

### Secrecy Measures

Although our knowledge of the exact security measures employed to keep Breaking Bad's scripts a secret are somewhat unclear, rumor has it that the show's creator has gone to great lengths to ensure secrecy. [According to Dean Norris](#), the actor who plays Hank on the hit show, “By the end of show, when we were about halfway through, all the scripts had all the juicy parts redacted, they were blacked out. It was like working for the CIA.” Similarly, [according to Laura Fraser](#), who plays Lydia, she received the entire script, but some of the pages had been “redacted, like an FBI document with pages and pages of blackness” so that only her lines were visible, and “if you wanted to read the redacted stuff you went into the office and read it on one computer.”

According to Kenneth [Vanko](#), “the scripts created by the show's writers generally contain code names (they're not labeled, for instance, Breaking Bad), ostensibly to guard against the impact of some accidental disclosure.” Furthermore, the show's contracts with outside vendors also involve an air of secrecy: many of the vendors don't even know they're supplying goods or services used by the show. Furthermore, the creator refuses to allow previews of the show before it airs. Additionally, those with access to the script were likely required to sign non-disclosure agreements. Such measures indicate that the show's producers have taken significant steps to ensure the secrecy of the show.

### Is the Information Economically Valuable Because of Its Secrecy?

In determining whether the episodes of Breaking Bad can be considered trade secrets, we must consider what makes the scripts themselves valuable: is it their secrecy or their novelty?



# Trading Secrets



Considering novelty first, in the wake of shows like *Mad Men* and *the Sopranos*, it is difficult to consider a drama with a male “anti-hero” for a protagonist to be a novel creation. As an [early review of the series put it](#), the show “lacks [*Mad Men*]’s originality and . . . is in many ways a bleaker male version of ‘*Weeds*,’ Showtime’s comedy about a widowed soccer mom who sells pot to keep up with the Joneses.” The lack of novelty strengthens the argument that the show gains value because of its secrecy. Furthermore, the fact that the main plot points (namely Walt’s methamphetamine manufacturing and his cancer) have been consistent since the show first began and that the show plays out over a period of two years means that viewers are constantly speculating about how the show will end, suggesting there is value in knowing how the show will end. Additionally, the rapid increase in viewership between the end of season 5 and season 6, due to the show’s availability on DVDs and Netflix and word-of mouth, suggest that people have grown increasingly interested in the show as the end nears, possibly because of the fact that the show is about to conclude. This has led to increased ratings and revenue, and suggests that the final episodes have significant economic value.

## **Are the Final Episodes of *Breaking Bad* Trade Secrets?**

Based on the economic value of the scripts, as well as the intense efforts to maintain the secrecy, the final episodes of *Breaking Bad* would likely be considered trade secrets until they enter the public domain. While their trade secret status is temporary, those in the know should keep this information confidential until the show’s final episodes officially air.



# Trading Secrets



## Careful, that Slice of Pizza You're Eating Might Be Full of Trade Secrets...

*By Jessica Mendelson (September 30th, 2013)*

It's time for yet another meal filled with trade secrets!

Earlier this month, New York Pizzeria, Inc., a pizzeria chain with over thirty restaurants in the United States and the Middle East, filed a complaint in federal court in Texas alleging trade secret misappropriation. New York Pizzeria alleged that a former employee, as well as individual restaurant owners, were conspiring to misappropriate its trade secrets for the purposes of creating a competing business. [According to New York Pizzeria's](#) allegations, a former employee and the owner of a competing business conspired to steal and use the company's trade secrets. The defendants allegedly used this unlawfully obtained information to start a competing franchise chain.



According to [the complaint](#), the former employee previously owned a New York Pizza franchise. His employment with the company was terminated in March 2011, and in October of that same year, the company sought to terminate his franchise as well. The parties allegedly agreed that New York Pizzeria would assume ownership of the restaurant, and would buy the former employee out. However, the former employee allegedly failed to honor certain obligations from this contract, and sued for breach of contract. In response, New York Pizzeria filed a counterclaim, alleging misappropriation of trade secrets. The suit eventually settled, however, after the settlement, New York Pizzeria alleged that the former employee continued to steal New York Pizzeria's product, and the company filed a second lawsuit, asserting independent trade secret misappropriation claims.

[According to Plaintiff's](#) allegations, the former employee "had access to . . . confidential, proprietary information, including NYPI's recipes, 'plate specifications,' supplier and ingredient lists, and training and restaurant operations manuals. . . [and the former employee] provided that information to the . . . [the other] defendants, without privilege to do so." Additionally, Plaintiff alleges that the former employee and cohorts illegally accessed New York Pizzeria's online portal by using one of New York Pizzeria's company user names and passwords. This login information allegedly enabled defendants to obtain New York Pizzeria's confidential and proprietary information, including special recipes and concepts for pizza, eggplant parmesan, baked ziti and pizza.

From a legal standpoint, it remains to be seen whether and to what extent New York Pizzeria has a protectable interest in the recipes and concepts and whether it will be successful in obtaining injunctive relief for their alleged use. This case, like the previous recipe case that we [recently blogged about](#), serves as a reminder that those in the restaurant industry must closely guard their cooking secrets and employ effective non-disclosure and confidentiality agreements. Additionally, franchisors must carefully guard the proprietary aspect of their franchise systems through appropriate agreements. No other hearings have been scheduled as of yet, but we will continue to keep you updated with any material developments in this tasty case.



# Trading Secrets



## Federal Court Rules Trade Secret Misappropriation Sufficiently Alleged Based on Improper Acquisition, Even in Absence of Use or Disclosure

*By Erik von Zeipel (October 8th, 2013)*

The United States District Court for the Eastern District of Virginia recently [denied a motion to dismiss a counterclaim for violation of Virginia's Uniform Trade Secrets Act \("VUTSA"\)](#), holding that the counterclaim sufficiently alleged trade secret misappropriation based on *improper acquisition* of a trade secret, even in the absence of allegations of use or disclosure.

### Factual allegations:

Plaintiff Jacqueline Marsteller was a Senior Vice President and Account Executive employed by defendant Electronic Consulting Services, Inc. ("ECS"). On November 3, 2011 ECS informed Marsteller that she was being terminated and that her last day of employment would be December 31, 2011 in order that she would be eligible to receive a \$95,000 bonus. The bonus was indeed paid to Marsteller on December 30, 2011. Marsteller began work for a competitor to ECS in December 2011.



### Procedural history:

Almost a year and a half after Marsteller left ECS, she sued her former employer on grounds not identified in the court's opinion. ECS filed a six-count counterclaim alleging, among other things, that after Marsteller was notified she was being terminated, she misappropriated various trade secrets by transferring information to an external storage device as well as e-mailing information to her personal e-mail account in violation of VUTSA.

### Motion to dismiss:

Marsteller moved to dismiss the counterclaims, including the VUTSA claim on the grounds that ECS failed to allege that: (1) the alleged trade secrets derived independent economic value; and (2) Marsteller *used* the trade secret information.

In ruling on the motion, the court explained that a claim for violation of VUTSA must allege that: (1) the information in question constitutes a trade secret, and (2) the defendant misappropriated it.

The court further explained that to constitute a "trade secret" under VUTSA, information must: (1) derive independent economic value; (2) not be known or readily ascertainable by proper means; and (3) be subject to reasonable efforts to maintain its secrecy. The court concluded that ECS validly pleaded the information allegedly taken by Marsteller was trade secret because it alleged that: (1) the information derives independent economic value because ECS spent time, effort and money developing the information and the information would allow a competitor to know ECS's business



# Trading Secrets



development and bidding plans, target its contracts and access its unique format for summarizing contract opportunities; (2) the information is not readily ascertainable by proper means as it reflects ECS's internal strategies and plans not publicly available; and (3) ECS took reasonable steps to protect the information by storing it on an internal password protected server.

With respect to “misappropriation,” the court stated that VUTSA recognizes two kinds: (1) improper acquisition of a trade secret; and (2) disclosure or use of a trade secret. Improper acquisition means “acquisition of a trade secret by a person who knows or has reason to know that the trade secret was acquired by improper means.” “Improper means” is defined under VUTSA as including “theft, bribery, misrepresentation, use of a computer or computer network without authority, breach of a duty or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means.” The court also cited case law for the proposition that “[u]nder the VUTSA, improper acquisition of a trade secret, even in the absence of allegations of use or disclosure, is sufficient to state a claim.” *Systems 4, Inc. v. Landis & Gyr, Inc.*, 8 Fed. Appx. 196, 2000 (4th Cir. 2001) (improper means alone can give rise to misappropriation claim) (unpublished).

In analyzing the counterclaim, the court concluded that ECS's allegation that Marsteller transferred and retained ECS's internal documents outside of the scope permitted by her employment, including transferring proprietary documents to an external storage device, sufficiently stated a claim for “misappropriation” through improper acquisition.

## **Alternative basis for ruling:**

Interestingly, the court also noted (in what is arguably dicta) that ECS's VUTSA claim contained “plausible allegations” that Marsteller also *used* certain misappropriated ECS information. The court apparently reached this opinion based on ECS's allegations that: (1) the ECS information in question was developed in order to obtain ISO certification; (2) ISO certification requires development and implementation of “business processes” required by ISO standards; (3) Marsteller began working for her new employer as the Vice President of Business Process Engineering in December 2011; and (4) Marsteller's new employer obtained ISO certification in July 2012.

The court stated that these allegations raised a “reasonable inference” that Marsteller used ECS's information and that it was “plausible, not just possible, that Marsteller used or disclosed” ECS information to benefit her new employer.

As a somewhat related side note, Virginia does not recognize the doctrine of inevitable disclosure. *Gov't Tech. Servs. v. IntelliSys Tech. Corp.*, 1999 WL 1499548 (Va. Cir. Ct. Oct. 20, 1999).

## **Takeaway:**

Having survived the motion to dismiss, it is unclear where ECS goes from here. Given that ECS waited more than a year and a half after Marsteller's departure (and her new employer's ISO certification) to raise its allegations, ECS will likely have an uphill battle obtaining any injunctive relief. The court will presumably also be unlikely to award damages if there is no evidence Marsteller used any of ECS's information.

What can employers do to avoid ending up in this situation? There are a number of safeguards and procedures that companies should consider as part of “best practices” in preventing trade secret misappropriation: (1) emphasizing to workers the importance of protecting the company's confidential, proprietary and trade secret information; (2) using non-disclosure and trade secret protection



# Trading Secrets



agreements to protect sensitive information; (3) continued education to remind workers regarding their obligations to protect company information; (4) employing reasonable protective measures to safeguard trade secrets; and (5) using exit interviews and certifications requiring departing workers to confirm they do not have any company trade secrets or confidential or proprietary information.

When misappropriation is suspected, it is essential not to delay to do a thorough factual and legal investigation before filing any misappropriation claim. Such investigation should identify any evidence showing: (1) what specific trade secrets are at issue; (2) what reasonable measures were taken to maintain their secrecy; (3) how the departed employee was able to acquire the trade secrets; (4) any threat of misappropriation or damages arising from the misappropriation. If it is suspected the trade secrets were transferred electronically, it is important that a forensic examination of relevant computers and/or other electronic devices be performed by experienced experts. Be mindful that using in-house IT personnel may create evidence spoliation issues.

Finally, if evidence of misappropriation is found, delaying legal action is likely to reduce the chances of obtaining injunctive relief to stop impermissible use of the misappropriated trade secrets, and thereby reduce your chances of preventing harm to your company.

# Trading Secrets



## Judgment on Willful And Malicious Trade Secret Claim Is Not Dischargeable In Bankruptcy

*By Paul Freehling (October 9th, 2013)*

Bankruptcy is intended to provide a fresh start and discharge outstanding debt. But some debt is not dischargeable in bankruptcy. A Virginia bankruptcy court [held](#) last week that a judgment against the debtor for intentional trade secret misappropriation is not dischargeable.



**Summary of the case.** La Bella Dona Skin Care, Inc. obtained a \$207,000 judgment in a Virginia state court against its ex-employee Harton for conduct that the court held to be willful and malicious misappropriation of La Bella Dona's trade secrets. Thereafter, she filed a voluntary petition for a Chapter 13 bankruptcy adjudication. In the bankruptcy proceeding, La Bella Dona filed an adversary proceeding seeking a determination that the judgment debt was not dischargeable in bankruptcy. After Harton answered the adversary complaint, admitting most of the salient facts but asserting that the debt was dischargeable, La Bella Dona moved for judgment on the pleadings. The motion argued that the doctrine of *res judicata* precluded her from challenging the state court holding that the misappropriation was willful and malicious, and that such conduct is not dischargeable under the Bankruptcy Code. Last week, the bankruptcy court granted the motion and held that the findings made and judgment entered by the state court could not be re-litigated by Harton in the bankruptcy court. [In re Harton \(La Bella Dona Skin Care, Inc. v. Harton\), Ch. 13 Case No. 12-36221-KRH](#) (Adversary Proceeding No. 13-3028-KRH) (Bkrcty Court, E.D. Va., Oct. 1, 2013).

**State court decision.** The bankruptcy court found that the following facts were uncontested: La Bella Dona conducted what the bankruptcy court called a "med-spa business." While Harton still was employed by La Bella Dona, she incorporated a competing salon. A few days later, after La Bella Dona's salon had closed for the day, she entered the salon and accessed her employer's computer. She printed out both the appointment schedule for the next 60 days and contact information for her employer's clients. Then, Harton opened her own salon nearby. Using La Bella Dona's contact list, she mailed postcards to 2,000 of its clients and stated on the postcards: "We've Moved – same faces – new location." She also phoned or emailed each client who had a confirmed, upcoming appointment. Many cancelled their appointments with La Bella Dona and came to Harton's salon. La Bella Dona sued her in state court which concluded that she had willfully and maliciously misappropriated her former employer's trade secrets.

**The Bankruptcy Code.** Section 523(a)(6) of the Code (11 U.S.C. §523(a)(6)) provides that "a debt for willful and malicious injury by the debtor" is excepted from the discharge provisions. However, that section has been held not to apply to Chapter 13 bankruptcies. Section 523(a)(4), which has been held to apply in any bankruptcy proceeding, states that a debt resulting from embezzlement or larceny is not dischargeable, but the state court did not find that Harton committed "embezzlement or larceny."



# Trading Secrets



**The bankruptcy court's decision.** Citing bankruptcy court cases from other jurisdictions, the Virginia bankruptcy court [held](#) that a state court judgment for knowing misappropriation of trade secrets constitutes “larceny” as that word is used in §523(a)(4). Consequently, the judgment debt against Harton is enforceable notwithstanding her adjudication as a bankrupt.

**Takeaways.** The decision in *La Bella Dona* is harsh but understandable. The Bankruptcy Code does not relieve all intentional wrongdoers from the consequences of their misconduct. When a victim of trade secret misappropriation obtains a money judgment (in addition to or in lieu of injunctive relief), a finding that the miscreant acted willfully and maliciously may serve to protect the money judgment against being discharged by the debtor's bankruptcy adjudication.

# Trading Secrets



## Neglect of Cloud Computing Policies In Workplace Can Provide Perfect Storm for Trade Secret Theft

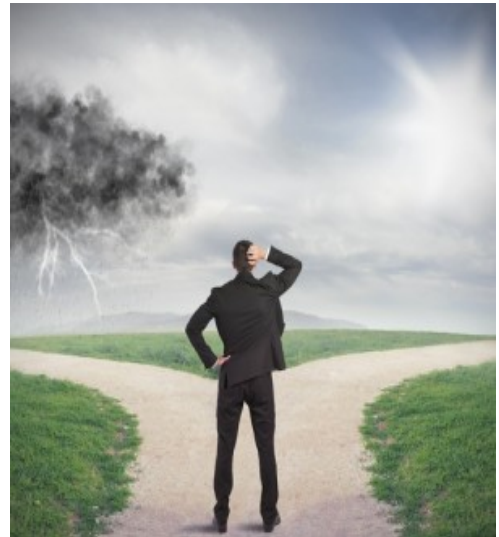
*By Robert Milligan, Jessica Mendelson and Daniel Joshua Salinas (October 10th, 2013)*

Prudent employers are often looking for areas in their business where valuable company data may not be adequately protected.

Enter the growing prevalence of third party online data storage for professional and personal use in the workplace, coupled with the increasing accessibility provided by employers to access company data remotely.

While the benefits of cloud computing are well documented, the growth of third party online data storage has facilitated the ability for rogue employees to take valuable trade secrets and other proprietary company files, in the matter of minutes, if not seconds.

There have been [several high profile cases](#) in California recently addressing the alleged theft of company data by employees through the use of third party online data storage.



To address this technology and threat to companies, employers must be vigilant to ensure that they have robust agreements and policies with their employees as well as other sound trade secret protections, including employee training and IT security, to protect their valuable trade secrets and company data before they are compromised and stolen. This is particularly important in California because California law can provide limited protection for employers—compared to other jurisdictions—because of its general prohibition of non-compete agreements and growing trade secret preemption or supersession doctrine.

As we have [previously discussed](#), one of the notorious employment laws separating California from other states is its [long-standing and draconian prohibition of employee non-compete agreements](#). Additionally, [some recent California decisions](#) have significantly limited an employer's ability to pursue certain claims and remedies based upon the theft of mere confidential or proprietary information by rogue employees. Employers may have limited recourse under California law if the stolen data does not rise to the level of a trade secret at least under a tort theory of recovery.

Further, a recent [article](#) in *The Recorder* entitled “Trade Secrets Spat Center on Cloud,” observed that the existence of cloud computing services within the workplace makes it “harder for companies to distinguish true data breaches from false alarms.”

Given these challenges, employers should implement policies and agreements to restrict or clarify the use of cloud computing services for storing and sharing company data by employees. Some employers may prefer to simply block all access to such cloud computing services and document the same in their





# Trading Secrets



policies and agreements. Also employers should provide education and training regarding the company's policy regarding employee use of cloud storage services.

Additionally, certain key steps should also be taken to protect against the theft of trade secrets and confidential information by departing employees with this new threat in mind:

- Collect and preserve all company property issued to the departing employee (e.g. desktops, laptops, cell phones, iPads, notebooks, flash memory drives/devices).
- Consider having the electronic devices forensically imaged and analyzed by a competent computer forensic investigator.
- Confirm that no unauthorized information, file, document, or e-mail transfers have occurred.
- Review computer access and print logs to determine if there has been any unusual or unauthorized use.
- Review internet history to determine whether third party storage sites were used.
- Review employee's work email to determine whether third party storages sites were registered for and used.
- Ensure ongoing access by the departing employee (remotely or otherwise) to information, documents, computer servers, offices, etc. is cut off.
- Ensure that the company has obtained all cloud computing and/or social media passwords and user information for company owned accounts and that passwords are subsequently changed.
- Provide the departing employee with any previously signed agreements pertaining to company property and confidential and trade secret information, including agreements/policies relating to cloud storage.
- Question employee during formal exit interview regarding the return of company property and any use of online data storage.
- To the extent that employee acknowledges online data storage, make arrangements with the employee to have the information returned or otherwise disposed of.
- Request that the departing employee sign a statement acknowledging continuing obligations in signed agreements as well as an acknowledgement that employee has returned all company property, including all electronic files.

A carefully thought out plan to trade secret protection, including third party online data storage issues, while taking into account business needs and realities, can help employers protect their valuable trade secrets and company data before they are compromised and stolen and help avoid costly litigation down the road. Please see our recorded webinars on [Trade Secret Protection Best Practices: Hiring Competitors' Employees and Protecting the Company When Competitors Hire Yours](#) and [Trade Secret Audits](#) for more details on how to put your company in the best position to protect valuable company information.

# Trading Secrets



## Federal Appellate Court Finds Motion To Enjoin Disclosure Of Confidential Information Should Not Be Denied Merely Because The Same Information Could Have Been Acquired Lawfully

By Paul Freehling (October 28th, 2013)

The United States Court of Appeals for the *Fifth Circuit*, reversing a trial court's refusal to enter an order enjoining disclosure of confidential information, recently [held](#) that the lower court erred when it (a) ruled that the moving party must satisfy all six trade secret balancing test factors, (b) rejected a party's request for an evidentiary hearing with respect to a key factual dispute as to which the parties submitted conflicting affidavits, and (c) applied federal rather than state law in determining that the moving party's potential injury from the alleged misappropriation could be adequately compensated with money.



### Summary of the case

While still employed by Heil Trailer International Company, Kula allegedly sent emails to Troxell, a Heil competitor. The emails allegedly contained certain information relating to Heil's business. Thereafter, Kula went to work for Troxell. Heil sued Kula, Troxell and others in a Texas federal court for, among other alleged wrongdoing, misappropriation of trade secrets. Heil's motion for a preliminary injunction was denied for three reasons: the lower court said the information Kula allegedly provided Heil could have been easily duplicated or acquired by others in the industry; any injuries Heil sustained could be adequately compensated by monetary damages; and the balance of hardships weighed in the defendants' favor. On interlocutory review, the Fifth Circuit reversed and remanded because of a variety of errors. [Heil Trailer Int'l Co. v. Kula](#), No. 13-10046 (5th Cir., Oct. 16, 2013) (unpublished *per curiam* opinion; limited precedent).

### Errors held to have been made by the trial court

1. *Failure to conduct an evidentiary hearing with regard to trade secret issues.* Texas courts recognize a six-factor balancing test in determining whether misappropriated information qualifies as trade secret. Here, Heil and Kula submitted directly conflicting affidavits concerning one of those factors: how difficult it would be for competitors to duplicate or acquire the information. Heil requested an evidentiary hearing on the issue. The trial court denied the request and, based solely on the affidavits, concluded that the information could have been easily duplicated or acquired by others in the industry. The Fifth Circuit held that the difficulty of duplicating or acquiring information claimed by one party to be confidential "is relevant to that information's status as a trade secret [but] by itself is unlikely to be dispositive." Further, quoting its own 1971 decision, the appellate tribunal stated that "where the parties' affidavit testimony is in direct contradiction as to material questions of fact, 'the propriety of proceeding upon affidavits becomes the most questionable.'" Accordingly, an evidentiary hearing should have been held.



# Trading Secrets



2. *Failure to demonstrate irreparable harm.* The appeals court observed that, under Texas law, injury to goodwill and to competitive position presumptively is irreparable where trade secrets have been misappropriated. Therefore, the trial court, which failed to articulate any facts or circumstances in support of its conclusion that Heil did not demonstrate irreparable harm, committed an error which must be remedied on remand.

3. *Balance of hardships.* According to the Fifth Circuit, the district court must determine whether the balance of hardships favors Heil, the party seeking the injunction, or the defendants. On remand, in the words of the U.S. Supreme Court, the trial court should identify and consider “the most serious possible injury’ that can be claimed by either party” if the injunction is granted or if it is denied.

4. *Other bases for an injunction.* In support of its motion for an injunction, Heil explicitly asserted both several common law bases, in addition to trade secret misappropriation, and some statutory provisions. The Fifth Circuit stated that the trial court did not — but must on remand — consider all of those assertions, not just misappropriation.

## Takeaways

Many courts would concur with the Fifth Circuit’s teaching that, on appeal from a decision with respect to a motion for a preliminary injunction in a case with allegations like those in *Heil*, a “clearly erroneous” standard applies to the findings of fact below while the conclusions of law are subject to *de novo* review. In a diversity jurisdiction case such as *Heil*, state law determines whether information constitutes a trade secret for purposes of ruling on a motion for preliminary injunction. A trial court making that determination based on Texas law must evaluate and weigh all of the relevant facts and circumstances, balancing the relative strength of the parties’ competing positions. In the face of a demand for an evidentiary hearing, resolving a genuine dispute concerning material facts solely on a paper record is problematic. Further, Texas courts hold that irreparable harm usually is presumed where there is a threat to disclose trade secrets.

# Trading Secrets



## The Romance of Trade Secrets: Competing Speed Dating Companies Engaged in Trade Secret Misappropriation Battle

*By Jessica Mendelson (November 5th, 2013)*

Dating comes with its own set of challenges, and apparently, these now include trade secrets! This month, a speed dating service provider, Speed Date USA Inc. ("Speed Date") [filed](#) a multi-million dollar lawsuit against Match.com ("Match") in Pennsylvania federal court.



According to the [Complaint](#), the parties had an agreement under which Speed Date would operate and manage speed dating events for Match for a period of two years. Match would then allegedly pay Speed Date \$25 for each ticket the company sold, as well as an additional fee per person for events with more than twenty participants. Under the terms of the agreement, each party was required to give sixty days written notice in order to terminate the event. [Furthermore](#), for termination purposes, no "agreed upon events" could be "outstanding," and scheduled events could only be canceled with five days' notice. However, Match allegedly terminated the agreement a year before its scheduled termination, and in the process, cancelled more than 80 scheduled speed dating events.

Speed Date also alleges Match illegally misappropriated Speed Date's trade secrets, which Match then used to run its own speed dating events. According to the terms of the [complaint](#), Match "agreed to keep in confidence and not to disclose to a third party the others' confidential or proprietary information." Speed Date alleges it spent years creating the formulas and patterns for marketing and running speed dating events, and that the information had significant independent economic value, as it was not generally known. Furthermore, Speed Date alleges the information and successful business model it developed were the very reason Match sought to partner with Speed Date. Speed Date alleges that following the termination of the contract, Match then used this confidential information to compete with Speed Date, and to begin to run their own speed dating events. Ultimately, [as a result](#) of the "early termination of the agreement" Speed Date alleges that they have suffered and may continue to suffer the loss of "clients, business, profits and revenue." Speed Date has requested damages totaling \$1.65 million from the loss of the contract, as well as \$4 million in punitive damages.

The case is still in its infancy, but whether Speed Date is successful in proving its trade secrets claim will likely turn on whether it can show that (1) it has instituted reasonable measures to maintain the secrecy of the information, (2) the information is economically valuable because of its secrecy, and (3) any evidence of misappropriation. Here, the parties had a non-disclosure agreement, suggesting that there were at least some efforts made to maintain the secrecy of Speed Date's confidential information. However, the protectability of this information will likely turn on whether it is economically valuable because of its secrecy. Here, it is not clear from the complaint what sort of confidential information Speed Date considers a trade secret, and whether its information that could be easily duplicated or required considerable effort to compile. While business plans, customer lists, and financial information are [frequently alleged to be](#) trade secrets, it is not clear that the formula for



# Trading Secrets



running a speed dating event would necessarily fall under the realm of trade secret protection. Further, Speed Date will need to establish that the information was actually misappropriated. We will continue to keep you updated on this lovely case as it continues to progress.

# Trading Secrets



## A Whale of A Trade Secret. . . Or Not?

*By Jessica Mendelson (December 4th, 2013)*

Last month, the Occupational Safety and Health Review Commission (“OSHRC”) refused to release SeaWorld’s new safety protocols for trainers interacting with killer whales, despite a recent court ruling that such protocols do not qualify for trade secret protection. The new protocols include new safety measures taken by SeaWorld in the wake of the death of trainer Dawn Brancheau, who was killed by an orca in February 2010.



In August, a federal judge held that the protocols were not trade secrets, and gave OSHRC a month to review the order before making the protocols publicly available. [According to Judge Welsch](#), “The protocols that SeaWorld wants to remain under seal reflect the training methods and techniques its trainers implement poolside with the killer whales. . . An observer knowledgeable in the behavior and training of killer whales could likely ascertain the information contained in the written protocols by watching the trainers interact with the killer whales.”

Judge Welsch’s ruling suggests that information must fall clearly into the definition of a trade secret to merit protection. In order to show that information is a trade secret, the owner must show that (1) it has instituted reasonable measures to maintain the secrecy of the information, and (2) the information is economically valuable because of its secrecy. Here, Judge Welsch’s ruling suggests that Seaworld has not kept the information at issue secret, because it is publicly available and can be easily ascertained by an observer. Thus, Welsch holds that the information cannot qualify for trade secret protection.

Despite Judge Welsch’s ruling that the information at issue is not protected as a trade secret, OSHRC has not made the information available to the public. [According to the Associated Press](#), OSHRC was supposed to provide the protocols in late September, but has failed to do so, apparently because OSHRC officials fear criminal liability for releasing trade secrets. [According to an agency spokesman](#), “A few of the lawyers here were concerned about whether the agency could potentially be held liable for releasing the protocols.” As of this writing, the agency does not appear to have released the documents to the public.

The case is currently on appeal before the DC Circuit. SeaWorld, however, is not contesting the trade secret determination, instead, choosing to focus its appeal on the Court’s broad application of the Occupational Safety and Health Act, a federal safety law meant to protect workers in unusual circumstances.



# Trading Secrets



## Protected Status Of Trade Secrets May Be Lost By Not Insisting On Confidentiality

*By Paul Freehling (December 11th, 2013)*

A recent decision of the U.S. Court of Federal Claims highlights the difficulty the owner of trade secrets faces in trying to market products while simultaneously preserving confidentiality. The Court dismissed a trade secret owner's misappropriation lawsuit against the U.S. Government because of a failure to insist on trade secret protections.



Summary of the case. Gal-Or, an Israeli scientist, invented various products which embodied his inventions and were used in the military aerospace industry. In the course of his efforts to sell his inventions, he disclosed confidential information to the Government and others, but he did not always insist on a non-disclosure agreement or place a legend on documents or prototypes. The Government allegedly misappropriated his trade secrets and infringed his patents. He sued in the Court of Federal Claims, alleging a violation of the Takings Clause of the Fifth Amendment and seeking \$71 million in damages. The Government then moved to dismiss the trade secret misappropriation counts on the ground that he revealed the confidential information without always imposing an obligation to maintain secrecy. The motion was granted. *Gal-Or v. U.S.*, Case No. 09-869C (U.S. Court of Fed. Claims, Nov. 21, 2013) (Braden, J.).

Gal-Or's sales efforts. Various branches of the military, as well as government contractors, expressed an interest in Gal-Or's products and then, allegedly, used the technology without permission. In some instances he had obtained non-disclosure commitments. In some others, he had disclosed documents bearing restrictive legends. However, he apparently revealed some information without receiving confidentiality commitments or including a legend.

In Gal-Or's complaint, he alleged that the Government made unauthorized use or disclosures of his trade secrets. In response to the Government's contention that the case should be dismissed because some of his disclosures were unrestricted, he insisted that the only way to obtain classified work from the Government or its contractors, and to market his inventions, was to share this information.

The court's ruling. Relying on judicial precedent, which holds trade secret protection is waived if confidentiality is not maintained, Judge Braden rejected Gal-Or's contention that he did enough to warrant trade secret protection: "[I]nstances in which Mr. Gal-Or took proactive steps to protect the confidentiality of his trade secrets are simply overwhelmed by the number of times he did not. More fundamentally, . . . Mr. Gal-Or's submissions [to the court] make it impossible to identify the trade secrets that were protected from those that were not."

Gal-Or insisted that disclosure to persons with classified security clearance did not require a specific confidentiality commitment or legend, but the court held that "their obligation as to secrecy was to the Government, not Mr. Gal-Or." Therefore, Gal-Or lost his property interest, and the court found that without a property interest, there can be no taking in violation of the Fifth Amendment.



# Trading Secrets



Takeaways. Whenever the owner of a trade secret discloses it, directly or indirectly, without imposing an obligation to maintain confidentiality, the owner risks loss of secrecy protection. Gal-Or allegedly revealed his confidential information in documents, videotapes, lectures, meetings and flight tests. This case holds that, regardless of the medium, there is no substitute for universally insisting on non-disclosure. For additional information on this issue, please see our prior blog post on [Convolve and MIT v. Compaq and Seagate litigation](#).



# Trading Secrets



## Computer Fraud and Abuse Act

# Trading Secrets



## Computer Fraud and Abuse Act Circuit Split Remains Unresolved: United States Supreme Court Challenge Dismissed

*By Robert Milligan (January 7th, 2013)*

The parties in the *WEC Carolina Energy Solutions LLC v. Miller* matter recently [agreed](#) to dismiss the petition for writ of certiorari filed with the United States Supreme Court, and as a result, the Court has [dismissed](#) the case.

Accordingly, the circuit split regarding the ability of employers to use the Computer Fraud and Abuse Act (CFAA) to sue former employees in typical employee data theft cases remains unresolved.



In early 2012, a Ninth Circuit *en banc* panel in *United States v. Nosal* [adopted](#) a narrow interpretation of the CFAA and found that an employee's violation of his/her employer's computer usage policies to steal company data was not a violation of the CFAA. The Court focused on whether the employee originally had access to the information, not whether the employee misused the employer's confidential information in violation of usage policies.

Later in 2012, the Fourth Circuit in *WEC Carolina Energy Solutions LLC v. Miller* [joined](#) the Ninth Circuit and adopted this narrow interpretation of the CFAA.

The First, Fifth, Seventh, and Eleventh Circuits have adopted a broader interpretation of the CFAA based on either common-law agency principles or computer usage policies. Under the agency theory, when an employee accesses a computer to further interests adverse to the employer, such actions terminate his or her agency relationship and, thus the employee loses any authority to access the computer. Under the computer usage theory, a violation of a computer usage policy can serve as a basis for holding an employee liable under the CFAA. Thus, an employee who is authorized to access a company computer, but uses that access to steal or damage valuable company data in violation of a computer usage policy, would be liable for his or her wrongful conduct under the CFAA.

As a result, employers can still pursue CFAA claims in the First, Fifth, Seventh, and Eleventh Circuits against rogue employees who steal data, whereas such claims remain very difficult to pursue in the Fourth and Ninth Circuits.

WEC Carolina Energy Solutions LLC had previously filed a [petition for writ of certiorari](#), [asking](#) the Court to determine whether the CFAA applies to employees who violate employer-imposed computer access and data use restrictions to steal company data.

The question posed by the [petition for writ of certiorari](#) was "whether the CFAA applies to employees who violate employer-imposed computer access and data use restrictions to steal company data." Please see [Thomas O'Toole's](#) and [Russell Beck's](#) discussion regarding the issue, as well as a nice [summary](#) of the CFAA split in the recent Florida Bar Journal.



# Trading Secrets



Accordingly, in those circuits that do not recognize CFAA claims in the typical employee data theft scenario, employers should consider the following: 1) consider revising your company's computer use policies and incorporate the concept of computer [access](#) policies instead (please see our previous post about the importance of computer access policies, [even in the Ninth Circuit](#)); 2) review the access employees are provided to company information on your company's computer servers and devices and narrow access to such information to need to know (e.g. lower level employees should not have access to highly valuable company information); and 3) the circuit split highlights the importance of contractual restrictions with employees requiring employees to return all company property and information upon termination, as well as employing robust and detailed exit interviews, which probe departing employees regarding the return of all company information, including information that may reside on personal computers and devices and securing the return of the same.

While there was proposed CFAA legislation in 2012, including [one bill](#) that would narrow its application and another that would [expand its scope](#), it is unclear whether similar legislation will be proposed in 2013. If you are interested in a legislative fix to the CFAA split, please contact your Seyfarth attorney or let us know [here](#). In the meantime, we will continue to keep you posted on any new significant CFAA decisions.

# Trading Secrets



## Computer Fraud and Abuse Act Claims Subject to Heightened Pleading Requirements

*By Jessica Mendelson (January 14th, 2013)*

In a recent Northern District of California [decision](#), Judge Sandra Brown Armstrong upheld the Ninth Circuit's ruling in *Nosal*, and at the same time, held that fraudulent conduct claims under the Computer Fraud and Abuse Act are subject to the heightened pleading requirements of Rule 9 of the Federal Rules of Civil Procedure.

Plaintiff is a computer technology company that supplies customers with enterprise hardware and software systems, and provides updates, including patches and fixes for its proprietary firmware and operating system software. Customers who purchase a technical support agreement are given access credentials that allow them to download support software from the plaintiff's websites. Access to these websites is subject to the plaintiff's terms of use, and customers are not permitted to share access credentials with unauthorized users.



In February 2011, DLT Federal Business Systems Corp ("DLT") became a member of plaintiff's membership program, which provides for third party companies interested in reselling plaintiff's hardware and software. DLT allegedly fraudulently used its access to obtain plaintiff's proprietary software patches and updates, which it then provided to customers, even though those customers lacked support agreements with plaintiff. In November 2011, plaintiff terminated DLT's membership due to alleged violations of the agreement. Plaintiff [alleged](#) that DLT and Service Key LLC were engaged in a "gray market conspiracy" and allegedly took "vast quantities of software patches and updates for plaintiff's proprietary operating system and other technical support files. In February 2012, plaintiff filed a complaint in the Northern District of California, alleging various causes of action. DLT subsequently filed a motion to dismiss plaintiff's claims for violation of the CFAA, inducing breach of contract, fraudulent inducement, unfair competition, intentional interference with prospective economic relations, and an accounting.

In December 2012, Judge Armstrong dismissed plaintiff's allegations that the defendants violated the Computer Fraud and Abuse Act ("CFAA") via unauthorized access and induced breach of contract. According to Judge Armstrong, DLT's conduct, "using legitimate access credentials to access websites and then distributing information obtained from such access to third parties who have no right to receive such information – is precisely the type of conduct that *Nosal* held was beyond the scope of the CFAA." In *Nosal*, which we previously blogged about [here](#), the Ninth Circuit held that the CFAA was intended to punish hacking, not the misappropriation of trade secrets or misuse of information.

Judge Armstrong allowed plaintiff to amend its claims against defendants for fraudulent conduct under the CFAA, finding that section 1030(a)(6) of the CFAA prohibits a party from fraudulently trafficking in "any password or similar information through which a computer may be accessed without authorization" where such trafficking affects interstate commerce. In amending the complaint, the court directed plaintiff to conform with Rule 9(b) of the Federal Rules of Civil Procedure and to "allege with specificity each incident of fraudulent conduct." Judge Armstrong reasoned that CFAA claims are subject to the





# Trading Secrets



heightened pleading requirements of Rule 9(b) when the allegations are “grounded in fraud” or otherwise “sound in fraud.” Judge Armstrong cited *Kearns v. Ford Motor Co*, where the Ninth Circuit held that even when fraud is not a necessary element of a claim, Rule 9(b) applies where a unified course of fraudulent conduct is alleged.” Accordingly, Judge Armstrong found *Kearns* applicable to the instant case because plaintiff alleged that DLT had accessed plaintiff’s support websites and engaged in fraudulent trafficking of passwords to facilitate third party access.

Judge Armstrong’s ruling provides another case reaffirming the ruling in *Nosal* – that a person who is authorized to access a password protected website does not violate the CFAA by downloading and distributing the materials to unauthorized persons. More importantly, the ruling is notable because Judge Armstrong found that the heightened pleading requirements of Rule 9 apply to the CFAA. Companies would be wise to take this into account in asserting fraudulent conduct claims under the CFAA, and make sure their pleadings are sufficiently detailed and particularized to meet the heightened pleading standard.

# Trading Secrets



## Activist's Death May Spur Legislative Changes To The Computer Fraud and Abuse Act

*By Jessica Mendelson and Robert Milligan (January 16th, 2013)*

The death of Aaron Swartz, a well-known coder, entrepreneur and political activist, has resulted in increased scrutiny of the federal Computer Fraud and Abuse Act ("CFAA"), a law some condemn as arcane and draconian but supported by others as necessary to combat illegal hacking and data theft.



Mr. Swartz [helped](#) to create RSS, a tool which allows users to subscribe to online information. He was also a [digital activist and innovator](#) and pushed to make information on the internet free and publicly accessible. Mr. Swartz was found dead in his New York apartment on January 11.

At the time of his death, Mr. Swartz was facing federal prosecution for allegedly gaining illegal access to JSTOR, a subscription service allowing users to access a variety of academic journals. Mr. Swartz allegedly wanted to "liberate" the journals in the database and make them publicly accessible. According to [various reports](#), Mr. Swartz allegedly initially downloaded articles from JSTOR through a guest account on the Massachusetts Institute of Technology ("MIT") network. Through the use of a program called "keepgrabbing," Mr. Swartz allegedly was able to circumvent JSTOR's limits on the number of articles a single person could download. However, after MIT and JSTOR caught on and disabled his access multiple times, Mr. Swartz allegedly broke into a utility closet on MIT's campus where he was able to connect his computer directly to the university network. In total, Mr. Swartz allegedly [downloaded](#) around 4.8 million articles from JSTOR. In July 2011, Mr. Swartz was indicted on federal charges, including wire fraud and thirteen separate violations of the CFAA. For these crimes, Mr. Swartz [faced](#) up to thirty-five years in prison, as well as millions of dollars worth of fines.

The specific charges that Mr. Swartz violated the CFAA alleged Mr. Swartz "intentionally accessed a computer without authorization or exceeded authorized access." 18 U.S.C. 1020(a)(2)(c). As we have previously mentioned, under this section of the CFAA, there are two main theories of liability: [the agency theory, and the computer usage theory](#). Under the agency theory, which is typically used in the employment context, when the employee accesses a computer or network to further interests adverse to the employer, such actions terminate his or her agency relationship and, thus the person loses any authority to access the computer. Under the computer usage theory, a violation of a computer usage policy or internet terms of service can serve as a basis for holding someone liable under the CFAA. Thus, for example, a person who is authorized to access a company computer, but uses that access to steal or damage valuable company data in violation of a computer usage policy, would be liable for his or her wrongful conduct, under the CFAA.

Mr. Swartz's family [reportedly blames](#) his death on "intimidation" from an overzealous prosecutor. [A petition to remove](#) the U.S. Attorney prosecuting the case, already has 25,000 signatures, and is awaiting a response from the White House.



# Trading Secrets



Some see Mr. Swartz's death as the [result](#) of prosecutorial intimidation. Others express [frustration](#) with the current state of the CFAA, arguing it has been amended so many times that it no longer makes sense. In the past, others have supported a [stronger and more robust CFAA](#).

Although the law may be broad, and the associated penalties severe, some experts argue that prosecutors acted in accordance with the law in bringing charges against him. [According to a recent post on a legal blog](#), Orin Kerr, a law professor at George Washington University and frequent contributor to the blog The Volokh Conspiracy, "the charges were based on established caselaw" and did not involve aggressive prosecutorial overreach. In Swartz's case, Mr. Kerr argues, unauthorized access is pretty clear: Mr. Swartz circumvented code-based barriers, and then played "a cat and mouse game" where he tried to access the database and JSTOR repeatedly tried to block him. One criminal defense attorney, [interviewed in an NPR segment](#), questioned whether computer hacking should be crime but acknowledged that was an issue for Congress and that Congress had decided to make it a crime and concluded that prosecutors have an obligation to enforce the law.

Mr. Swartz's death has resulted in a call for change by some, as they [express](#) a need for "a public conversation about what the laws should prohibit and how severe they should be." In the wake of Mr. Swartz's death, some legislators, advocates and media have come out in support of a change to the CFAA. Darrell Issa (R-California), the head of the House Oversight Committee recently announced plans to launch an investigation into the charges Mr. Swartz faced. "I'm not condoning his hacking, but . . . had he been a journalist and taken that same material that he [gained from MIT](#), he would have been praised for it. It would have been like the Pentagon Papers," Mr. Issa [told The Huffington Post](#).

Zoe Lofgren (D-California), a member of the House of Representatives, has [already proposed an amendment to the CFAA](#). In a recent public statement on Reddit, she discusses the "inappropriate efforts undertaken by the U.S. government" and the importance of preventing "a repeat of the abuses of power he experienced." Ms. Lofgren expresses concern over the "vague wording" of the CFAA, which could criminalize everyday behavior by claiming "that violating an online service's user agreement or terms of service is a violation of the CFFA and the wire fraud statute." The law Ms. Lofgren proposes, which will be known as [Aaron's Law](#), would modify the definition of exceeds authorized access. As the law stands now, the phrase is defined as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." Under Aaron's law, the phrase "alter" would become "alter, but does not include access in violation of an agreement or contractual obligation, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or employer, if such violation constitutes the sole basis for determining that access to a protected computer is unauthorized."

Such a change to the CFAA, which [seems intended to limit prosecutorial discretion](#), would likely significantly limit creative prosecutorial interpretations of the CFAA and effectively end criminal and civil liability under the CFAA based on violations of computer usage and terms of service policies. This change would likely result in the demise of the computer usage theory, however, how the proposed law would impact the agency theory adopted in some jurisdictions as discussed above would remain to be seen. Aaron's law could prove frustrating for some employers, who may support a strong CFAA to combat employee data theft, because state causes of action and remedies can be insufficient to deal with unauthorized computer access by former employees who steal company data.

We will keep you apprised of significant development in this evolving debate over the future of the CFAA.

# Trading Secrets



## Computer Activists Take Over Sentencing Commission Website

*By Jessica Mendelson (February 2nd, 2013)*

Anonymous, the aptly named anonymous collective of hackers, hacked into the United States Sentencing Commission's website on January 23 to protest the government's [prosecution of Aaron Swartz](#), who committed suicide last month. The group initially hacked the site on Friday January 22, replacing the contents of the site with its own video. In the video, which has since been taken down, but still exists elsewhere on the internet, Anonymous denounced the government's prosecution of Swartz. According to Anonymous' [statement in the video](#), "a line was crossed" when Swartz, facing 'a twisted and distorted perversion of justice,' decided to kill himself." According to Anonymous, [it was time to do something](#), now that "several more of our brethren now face similar disproportionate persecution." The website was taken offline and restored to its proper formatting, but by Sunday, Anonymous had [hacked the site again](#), replacing it with a game of Asteroids which the visitor must play to reveal the [message](#), "We do not forgive, we do not forget."



According to Anonymous, the hacking was designed to [call attention](#) to "the federal sentencing guidelines which enable prosecutors to cheat citizens of their constitutionally-guaranteed right to a fair trial." In the group's statement, which was posted on the Sentencing Commission's website along with a [ten minute video](#), the group stated, "the time has come to give this system a taste of its own medicine. The time has come for them to feel the helplessness and fear that comes with being forced into a game where the odds are stacked against them." According to the statement, the group chose the U.S. Sentencing Commission's website because of its symbolic nature: "the federal sentencing guidelines. . . enable prosecutors to cheat citizens of their constitutionally-guaranteed right to a fair trial, by a jury of their peers [and] are in clear violation of the 8th amendment protection against cruel and unusual punishments."

In its statement, Anonymous pushes for "reform of outdated and poorly-envisioned legislation." The group objects to legislation like the Computer Fraud and Abuse Act, which is "written to be so broadly applied as to make a felony crime out of violation of terms of service, creating in effect vast swathes of crimes, and allowing for selective punishment." The group also pushes for a reform of mandatory minimum sentencing, and for laws to be upheld "unselectively, and not used as a weapon of government to make examples of those it deems threatening to its power."

Anonymous is [reportedly](#) planning to release a number of files (which the group refers to as "warheads") named after the justices of the United States Supreme Court. According to the [ABA Journal](#), the files are heavily encrypted, and no explanation has been offered as to what the files contain. Anonymous has threatened to release heavily redacted partial contents of the encrypted files to a media outlet, however, the release of these files has yet to occur.

Richard McFeely, the executive assistant director FBI's Criminal, Cyber, Response Services released a [statement](#) in response: "We were aware as soon as it happened and are handling it as a criminal



# Trading Secrets



investigation. We are always concerned when someone illegally accesses another person's or government agency's network."

It remains to be seen whether Anonymous will actually release any files or whether this is simply a ploy in the struggle for legal reform. Regardless, Anonymous' actions are just the latest in a [growing push](#) for legal reform in the wake of Aaron Swartz's death.

A push for legal reform is also occurring in the US House of Representatives, where Darrell Issa (R-California) and Elijah Cummings (D-Maryland) of the House Oversight Committee authored a joint letter to Attorney General Eric Holder regarding Aaron Swartz's criminal prosecution. The letter [questioned](#) the procedural standards applied in the case, including the "factors that led to the decision to prosecute Swartz, along with key decisions after the case began." The letter also asks if Swartz's political advocacy was considered relevant in deciding whether to prosecute Swartz. The Justice Department ("DOJ") has agreed to brief the two congressmen, however, the [Huffington Post](#) notes that the DOJ "has been fighting" efforts to reform the Computer Fraud and Abuse Act, according to a congressional staffer familiar with legislative discussions.

In addition, Aaron's law, the legislation recently proposed by Representative Zoe Lofgren (D-California), has undergone revisions, and is gaining additional support in Congress. [According to Representative Lofgren](#), the draft has been revised to explicitly exclude "breach of terms of service or user agreements as violations of the CFAA or wire fraud statute." Additionally, changing or disguising an IP or MAC address on its own is not sufficient to constitute a CFAA violation. Furthermore, the [revised draft](#) further limits the CFAA's scope by defining "access without authorization" as the "circumvention of technological access barriers." Ms. Lofgren has [begun](#) to solicit co-sponsors in the House of Representatives for the bill. Additionally, Senator Ron Wyden (D-Oregon), who was [involved](#) in the revisions of Aaron's Law, is [poised](#) to sponsor the bill in the Senate. Senator Wyden has begun to talk to members of both parties about how to modify the CFAA. [According to Senator Wyden](#), "This is going to take some time, and as with everything in this area, you try to look for what can actually get accomplished because you have people with very strong views. But to me, if you start with that basic proposition — this law as currently written just kind of defies common sense — then I think that there's an opening."

Aaron Swartz's death is likely to lead to additional calls for reform in the coming months, as well as changes in the law. We will continue to keep you informed of further developments on the Computer Fraud and Abuse Act.

# Trading Secrets



## Missouri Federal Court Finds Violations of Employment Agreement May Constitute Unlawful Access Under the Computer Fraud and Abuse Act

*By Paul Freehling and Daniel Joshua Salinas (February 6th, 2013)*

A recent Missouri [federal court opinion](#) describes an almost unbelievable scenario. Employees signed well-drafted employment agreements — containing such provisions as non-competition, confidentiality, promise of loyalty, and commitment to return employer's property within 24 hours of termination of employment — and then incorporated and operated a competitor company while still employed. Moreover, they transferred the employer's computer source code to their own computers, delayed returning their ex-employer's property after resigning, cleansed their computers before producing them pursuant to a court order, and never did turn over the source code. The court granted summary judgment to the ex-employer



with respect to liability, with only damages issues left to be tried, on the breach of contract counts. The court also ordered a trial as to liability and damages with regard to the ex-employer's CFAA and trade secret misappropriation claims. *Custom Hardware Eng'g & Consulting, Inc. v. Dowell*, Case No. 4:10CV000653 ERW (E.D.Mo., Jan. 23, 2013).

Custom Hardware Engineering (Custom) developed technology permitting its employees to monitor and trouble-shoot computers remotely. Employees signed agreements promising Custom (a) faithful performance and full time attention to its business; (b) non-competition; (c) the return of all of its property, and disclosure to Custom of all relevant passwords and codes, within 24 hours of employment termination; and (d) maintenance of the confidentiality of Custom's trade secrets. Notwithstanding these commitments, several months before resigning from the company four employees transferred Custom's source code to a file they created, and they formed and began operating a competing corporation. In addition, they violated their promises immediately upon termination to return Custom's property and to disclose relevant passwords and codes. After Custom filed suit against them and their competing corporation, they were ordered to produce their personal computers for Custom's inspection. Before complying, they erased pertinent information from the computers.

Custom's complaint alleged copyright infringement, breach of contract, trade secret misappropriation, violation of CFAA, and various other claims. The court granted Custom's motion for summary judgment as to liability with respect to breach of contract and ordered a trial regarding damages. The defendants' motion for summary judgment as to counts alleging copyright infringement, misappropriation of trade secrets, and CFAA violations were denied, and a trial of all issues ordered. However, the defendants did prevail on their motion to dismiss, as preempted by the Missouri Uniform Trade Secrets Act, Custom's claims of breach of fiduciary duty and the duty of loyalty, tortious interference with contract, unfair competition, conversion, and unjust enrichment.

One significant takeaway from this case was survival of the CFAA claim based on the employees' violations of the employer's Employment Agreement. Specifically, the court stated:





# Trading Secrets



*“The terms of Defendant’s Employment Agreements clearly limit their use of CHE’s protected materials to the period of their employment, and for the benefit of CHE; consequently, any access by Defendants after their termination would be unauthorized, as would any access not used for CHE’s benefit.”*

The court applied the “intended use” theory, which is a departure from the Ninth Circuit’s narrow interpretation of the CFAA and the Seventh Circuit’s agency law-based theory. Courts in the Third, Fifth, Eighth, and Eleventh Circuits have applied the intended use theory to find “unlawful access” under the CFAA when employees violate company policies and agreements.

This case reminds us that an employer’s protection under the CFAA against rogue employees that steal valuable company data may simply depend on which jurisdiction they are in and/or the genius of counsel.

# Trading Secrets



## North Carolina Federal Court Uses Computer Fraud and Abuse Act Claim to Exercise Supplemental Jurisdiction Over State Law Claims Against Former Employee and her New Employer

*By Paul Freehling (March 20th, 2013)*

A North Carolina federal court judge exercised his discretion recently to deny a Federal Rule 12(b)(1) motion to dismiss, for lack of subject-matter jurisdiction (complete diversity was absent), multiple state law claims filed by NouvEON against its ex-employee and her new employer. One of the eight counts in the complaint alleged a federal cause of action, violation of the federal



Computer Fraud and Abuse Act by the ex-employee. Because the CFAA allegations were incorporated by reference in the other seven counts, and also because the new employer was accused of common law vicarious liability for the CFAA violations, the court was persuaded that the entire case should be tried in a single federal court proceeding. [NouvEON Technology Partners, Inc. v. McClure, Case No. 3:12-CV-633-FDW-DCK \(W.D.N.C., Mar. 5, 2013\).](#)

McClure was an employee of NouvEON until she resigned and allegedly almost immediately went to work for one of its competitors. She had allegedly signed a covenant not to compete with NouvEON and a promise not to disclose its confidential information. NouvEON sued her and her new employer for “computer trespass” in violation of a North Carolina statute, unfair and deceptive trade practices violative of another North Carolina statute, civil conspiracy, and unjust enrichment. McClure alone was charged with violation of the CFAA and conversion. Her new employer was accused of tortious interference with contract and vicarious liability for her alleged CFAA wrongdoing. Each count of the complaint was incorporated by reference in all of the other counts.

Federal courts have original jurisdiction over CFAA complaints. NouvEON’s CFAA count was the only one for which there was original federal jurisdiction, but the new employer was not named in that count. Moreover, in terms of the number of counts, the state law claims obviously predominated. Nevertheless, in deciding to exercise supplemental jurisdiction over the state law claims, the court reasoned that the existence of a “common nucleus of operative facts,” and the principle of “judicial economy, convenience, and fairness,” were dispositive. Although the countervailing doctrine of “avoiding federal interference with state enforcement schemes” might have weighed in favor of declining to exercise supplemental jurisdiction over the state law claims if that doctrine was implicated, apparently it was not.

The *NouvEON* decision suggests an approach a former employer might use if, notwithstanding the absence of diversity jurisdiction, the plaintiff prefers to litigate state law claims — such as trade secret misappropriation, violation of non-compete, non-solicitation and confidentiality covenants, etc. — in federal court against an ex-employee (together, perhaps, with related causes of action against the new employer). By adding allegations of misconduct as to which a federal court has original jurisdiction, such as a CFAA violation, and then incorporating those allegations by reference in all counts, a plaintiff



# Trading Secrets



may reduce the risk that the federal court will dismiss the state law causes of action. The chances that the federal court will decline supplemental jurisdiction increases, however, if adjudication of purely state law claims will constitute “interference with state enforcement schemes,” and so that potential concern should be addressed in the complaint.

# Trading Secrets



## Recent California Federal Court Rulings Muddy the Interpretation of the Computer Fraud and Abuse Act

By Paul Freehling (March 28th, 2013)

Does the Computer Fraud and Abuse Act (“CFAA”) prohibit hacking—*improperly gaining entrance into a computer system*—or simply prohibit *improper use of a computer system*? U.S. Courts of Appeal are divided. Now, district and appellate court judges in a single federal case pending in the Northern District of California, *U.S. v. Nosal*, have produced several divergent opinions regarding congressional intent with respect to the meaning of the CFAA.

The defendant in *Nosal* allegedly persuaded employees of his former employer to log in to the employer’s computer system and forward confidential information to him. *Nosal* allegedly planned to use the information to compete with his former employer.



The [CFAA](#) provides that an individual who “knowingly and with intent to defraud, *accesses a protected computer without authorization, or exceeds authorized access*” is guilty of a crime. Although the CFAA is a criminal statute, most judicial opinions interpreting it are issued in civil (injunction and damages) litigation. *Nosal* is one of the unique reported CFAA cases in which the defendant was charged with a crime.

The [most recent Ninth Circuit opinion](#) in *Nosal* was written in 2012 by an *en banc* majority. Those judges concluded that the CFAA is simply an anti-hacking statute that criminalizes circumventing “technological barriers.” It does not apply to *Nosal*, the majority held, because he was not the person who entered his former employer’s computer system.

After the Ninth Circuit’s *en banc* decision was issued, affirming the district court’s dismissal of the indictment’s CFAA counts, a superseding indictment was returned. It alleged substantially the same crimes but added more facts with the purpose, apparently, of getting around the *en banc* ruling. *Nosal* again moved to dismiss the CFAA counts, stressing that the statutory words “accesses” and “access” relate to unauthorized logging into the company’s computer, not to the use that is made of the computer after logging in. Since he did not log in, he insisted, he could not be guilty of CFAA crimes.

In a [ruling](#) issued in mid-March 2013, *Nosal*’s motion was denied. The district court judge emphasized that the Ninth Circuit *en banc* majority’s words cannot be taken literally. According to that judge, “[h]acking was only a shorthand term used [by the *en banc* majority] as common parlance . . . to describe the general purpose of the CFAA,” and the phrase “circumvention of technological access barriers” was an aside that does not appear to have been intended as having some precise definitional force.” In short, the district court judge concluded,



# Trading Secrets



**“[i]f the CFAA were not to apply where an authorized employee gave or even sold his or her password to another unauthorized individual, the CFAA could be rendered toothless. Surely Congress could not have intended such a result.”**

[Proposed legislation](#) to expand the scope of the CFAA is currently being circulated among the House Judiciary Committee. Nevertheless, practitioners and parties in the states and territory which encompass the Ninth Circuit — Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, Washington State, and the Territory of Guam — will likely have to wait at least until the next CFAA lawsuit is decided by the Ninth Circuit before they may reliably predict what conduct will be held to violate the CFAA.

# Trading Secrets



## The Computer Fraud and Abuse Act and Disloyal Employees: A Narrow Bridge To Nowhere?

*By Gary Glaser and Jacob Oslick (April 15th, 2013)*

An old folk melody describes the world as “a very narrow bridge,” where one misstep can bring disaster. The song seeks to inspire, calling on people to have “no fear at all” while crossing through life’s perils.

However inspiring this song might be, some metaphorical bridges just aren’t worth crossing. Trying to assert Computer Fraud and Abuse Act (“CFAA”) claims against disloyal employees is a perfect example. Employers rightly want to seek relief against employees who steal confidential information that might not qualify as “trade secrets.” And, at first glance, the CFAA appears to present a promising bridge into federal court for just such a claim. Even better, for a while, many federal courts adopted a broad view of the statute that permitted precisely these claims. In fact, between 2001 and 2010, the First, Fifth, Seventh, and Eleventh Circuits all issued opinions that interpreted the CFAA broadly, which still stand as the precedent in those Circuits.



Over the past few years, however, other federal courts have increasingly construed the CFAA narrowly. In a number of decisions, various federal courts have restricted both the claims that can be brought under the CFAA and the damages available for violations. These days, simply asserting a CFAA claim will almost certainly be met with a time-consuming and burdensome motion to dismiss. And, often, the CFAA proves to be a bridge to nowhere, because the Court dismisses the claim.

The plaintiff in [\*JBCHoldings NY, LLC v. Pakter\*](#), 2013 U.S. Dist. LEXIS 39157 (S.D.N.Y. 3/20/13) recently learned this lesson. In *JBCHoldings NY LLC*, an employer was faced with a familiar situation: it gave a trusted employee access to its highly confidential information, only to have her allegedly misappropriate it for herself, and then allegedly misuse it to pilfer the company’s business opportunities which she then allegedly provided to former business colleagues who had set up a competing entity with her. The employer responded with a CFAA claim, alleging that the disloyal employee had violated the statute because, by stealing data, she accessed the company’s computers “without authorization” or “exceeded [her] authorized access.”

On March 20, 2013, the Southern District of New York dismissed the employer’s claim. The Court reasoned that the CFAA’s “plain meaning” only prohibits accessing information “without authorization” or “exceed[ing] authorized access,” but “does not speak to the misuse of permitted access or the misappropriation of information which an employee is authorized to access.” In so doing, the Court followed recent decisions by the Fourth and Ninth Circuits in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) and *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012), respectively, along with a plethora of Second Circuit district court decisions.

The Court further reasoned that a “review of the statute as a whole confirms the narrow interpretation,” because it defines “loss” quite narrowly. In this regard, the Court noted that an unpublished Second Circuit decision held that the CFAA did not cover losses sustained due to the plaintiff’s





# Trading Secrets



misappropriation of proprietary information. See *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 563 (2d Cir. 2006). Given this limitation, the Court in *JBCHoldings* articulated that “[i]t would be illogical for the statute to prohibit misappropriation of employer information, but not define loss to include the losses resulting from that misappropriation.”

Additionally, the Court held that, while it “does not find the statute ambiguous,” the “rule of lenity” would caution towards a narrow interpretation, “because the CFAA is primarily a criminal statute.”

The Court’s opinion does leave two narrow bridges of hope for employers. First, on the law, the CFAA’s interpretation is far from settled. Despite *WEC Carolina Energy Solutions*, *Nosal*, and district court decisions like *JBCHoldings*, a majority of circuit courts that have addressed this issue have come down on the side of the broader interpretation. And the Supreme Court won’t be resolving this circuit-split anytime soon. The Department of Justice declined to seek certiorari in the *Nosal* case and, back in January, the Supreme Court dismissed the certiorari petition in *WEC Carolina Energy Solutions*, upon the parties’ stipulation. So a “broad” CFAA claim remains viable in many jurisdictions.

Second, on the facts, the *JBCHoldings* court provided direction on how employers can sometimes successfully navigate a narrow CFAA claim. For, although the Court held that the CFAA doesn’t provide a remedy against a disloyal employee who misuses access to a computer, it does apply to an “outside hacker” who lacks any permission whatsoever. The Court further noted that at least some of the Complaint’s allegations created an inference of “outside hack[ing],” including allegations that the disloyal employee may have used spyware or malware to accomplish her goals. That being said, the Court ultimately found that these allegations were “couched in terms of sheer possibility,” and thus failed to pass the *Twombly/Iqbal* “plausibility” standard. This is because it was much more likely that the employee “simply copied the information to her personal laptop,” without resorting to a nefarious program.

Taking that reasoning to heart, employers should remember that the *JBCHoldings* case is not every case. While disloyal employees often just swipe information that they can lawfully access, sometimes they get even greedier. They may load spyware and malware onto their employer’s server to farm for useful information. They may decrypt passwords to access higher-level information than they are permitted. Or they might “hack” this data in other ways. And, when employees engage in such conduct, they do more than just misuse information that they can lawfully access. They exceed their authorized access to a company’s computers, and thus indisputably fall within the CFAA’s ambit.

In fact, this kind of conduct may very well have happened in the *JBCHoldings* case. The employer just didn’t have the facts to back it up its allegations. For, although it began some kind of investigation into the employee’s conduct, this investigation remained “incomplete” when they filed their Complaint, and apparently wasn’t too detailed.

This may have been a fatal mistake. A professional forensic examination can reveal what employees stole, how they stole it, whether they engaged in any other sinister conduct (such as deleting data), and whether they comprised the system’s integrity. Accordingly, this kind of examination can – at least sometimes – provide factual backing for a CFAA claim, even if a Court construes the CFAA narrowly. In short, a forensic examination can help employers decide which potential CFAA claims to avoid, and which to pursue. After all, when you’re crossing a narrow bridge, you want it to be as strongly supported as possible. Even if you have no fear at all.

Employers may also find that they have a better chance of successfully articulating a successful CFAA claim in a “narrow interpretation” circuit, if they draft their confidentiality/trade secrets policies with the



# Trading Secrets



express precepts of the CFAA in mind. Thus, for example, it may pay for an employer to expressly provide that an employee's authorization to access certain specified confidential information of the employer ceases immediately upon certain triggering events. Needless to say, the Courts will have the last word as to whether such policy language can "trump" their interpretation of the terms of the CFAA, but where the employer's policies closely track those very terms, it may be more difficult for the Court to find that authorization, once given, cannot be lost. Just sayin' . . .

# Trading Secrets



## Employee Data Theft and Corporate Hacking Studies Point to Need for Additional Federal Trade Secrets Legislation

*By Robert Milligan and Jessica Mendelson (April 22nd, 2013)*

Today is the [deadline for public comments](#) requested by the Obama Administration on any proposed changes to federal law to combat trade secret theft.

Some legal commentators have proposed several suggested changes to improve America's trade secrets laws, including creating a [federal civil cause of action for trade secrets misappropriation](#) and clarifying that the Economic Espionage Act [applies to defendants](#) who provide trade secrets to a foreign corporation or entity. In addition, [others](#) are considering proposing clarifying that the Computer Fraud and Abuse Act applies to employee data theft, enhancing the penalties for violations of the Economic Espionage Act, and providing U.S. Customs with greater clarity concerning its ability to seize products containing misappropriated trade secrets.

In addition, the American Bar Association Intellectual Property Section [supported](#) a resolution creating a federal civil action for trade secret misappropriation laying out five guiding principles that any future legislation should observe. Others believe that additional legislation may stifle innovation, privacy, and individual rights, or that the existing legal framework is sufficient or further legislation unnecessary.

I have included my [personal submission](#) to the Obama Administration on proposed trade secret legislation.

Two recent studies concerning employee data theft and corporate hacking highlight the growing problem and potential need for further legislation to protect valuable proprietary assets from theft and cyber-attack.

Symantec recently [released](#) a rather depressing survey on employee attitudes toward confidential information, finding that half of employees surveyed who had left jobs within the past year retained confidential information from their former employers. The survey, conducted by the Ponemon Institute, was designed to look at intellectual property theft in the workplace. The survey participants numbered over 3,000, and included individuals from the United States, France, Brazil, Korea, China, and Great Britain. More than half of these employees admit to emailing business documents from workplace to personal emails, and 41% of respondents admitted to doing it on a weekly basis. Furthermore, more than a third of these employees use file sharing applications without their employer's permission, and generally fail to delete the documents included in the files after their use.

While many security initiatives focus on threats by cyber criminals and hackers, often trusted employees can be a significant threat to a company's intellectual property. "Companies cannot just





# Trading Secrets



focus on external attackers and malicious insiders stealing data for financial gain,” [said](#) Lawrence Bruhmuller, Vice-President of Engineering and Product Management at Symantec. As Robert Hamilton, Director of Product Marketing at Symantec, [puts it](#), “employees are the less obvious player, but they can be frenemy #1.” According to the results of the survey, over half of the surveyed employees who had left jobs in the past year retained confidential information and 40% planned to use this confidential information in their new jobs. Perhaps more disturbing, 62% believed there was nothing wrong with transferring corporate data to their personal devices or cloud file-sharing applications, and 42% thought that there was nothing wrong with reusing another company’s source code for another company. Furthermore, a third of employees believe that there is nothing wrong with retaining confidential information, so long as the employee doesn’t profit economically. The majority of these employees rationalized their actions by saying that retaining this confidential information was not harmful to the company.

The survey results [suggest](#) “employees are not aware that they are putting themselves and their employers at risk” by sharing confidential information. Furthermore, the study suggests employees don’t believe using confidential information from a previous employer to be a crime, and instead, consider the owner of the intellectual property to be the person who created the IP.

The results of this study highlight the importance for employers of having coherent policies in place to protect company intellectual property. “The time to protect your IP is before it walks out the door,” Bruhmuller [said](#). Bruhmuller encouraged employers to educate their employees to ensure employee awareness of IP theft, and to establish clear policies regarding confidential information and intellectual property. Employers should also use caution in conducting screening interviews to ensure new employees are not bringing intellectual property from a former employer to their new company. 68% of employees surveyed said that their companies were not taking steps to ensure employees were not using confidential information from competitors, a figure that needs to change if employers wish to prevent costly lawsuits.

Next, a second [study](#) by Symantec revealed a 42% surge during 2012 in targeted hacking attacks compared to the prior year. According to the report, targeted cyber espionage attacks, designed to steal intellectual property, are increasingly hitting the manufacturing sector as well as small businesses, which are the target of 31% of these attacks.

“This year’s ISTR shows that cybercriminals aren’t slowing down, and they continue to devise new ways to steal information from organizations of all sizes,” [said](#) Stephen Trilling, Chief Technology Officer of Symantec. “The sophistication of attacks coupled with today’s IT complexities, such as virtualization, mobility and cloud, require organizations to remain proactive and use ‘defense in depth’ security measures to stay ahead of attacks.”

According to the [study](#), small businesses are now the target of 31% of all attacks, a threefold increase from 2011. Cybercriminals are reportedly enticed by these organizations’ bank account information, customer data and intellectual property.

The study also revealed that manufacturing has moved to the top of the list of industries targeted for attacks in 2012. The study attributes the increase in attacks to cybercriminals targeting the supply chain and contractors and subcontractors who are susceptible to attack and often in possession of valuable intellectual property. According to the study, the most commonly targeted victims of these types of attacks across all industries were knowledge workers (27%) with access to intellectual property as well as those in sales (24%).



# Trading Secrets



Additionally, the Obama Administration's [Strategy on Mitigating the Theft of U.S. Trade Secrets](#) stated:

Emerging trends indicate that the pace of economic espionage and trade secret theft against U.S. corporations is accelerating. There appears to be multiple vectors of attack for persons and governments seeking to steal trade secrets. Foreign competitors of U.S. corporations, some with ties to foreign governments, have increased their efforts to steal trade secret information through the recruitment of current or former employees. Additionally, there are indications that U.S. companies, law firms, academia, and financial institutions are experiencing cyber intrusion activity against electronic repositories containing trade secret information. Trade secret theft threatens American businesses, undermines national security, and places the security of the U.S. economy in jeopardy. These acts also diminish U.S. export prospects around the globe and put American jobs at risk.

Whether additional federal trade secrets legislation is passed to protect U.S. companies from attack and enhance national security, companies can protect themselves from trade secret theft by employing effective trade secret protections now. Employers should ensure that company information is properly classified and protected and that non-disclosure agreements are specific about what can and cannot be disclosed, as well providing clear employee responsibilities for safeguarding confidential information. Employers should also foster a culture of confidentiality so that employees genuinely understand the importance and their self-interest in maintaining the confidentiality of company information. Exit interviews should include a mention of the continued duty to protect confidential information and return company property or devices. Furthermore, employers should consider implementing or updating their data protection policies and computer access policies to ensure intellectual property is not being taken or used inappropriately and employers must enforce their policies. Lastly, companies should employ respected cybersecurity specialists to protect their systems from attack.

# Trading Secrets



## Corporate Recruiter Convicted of Computer Fraud and Trade Secret Theft By San Francisco Jury

*By Robert Milligan and Daniel Joshua Salinas (April 29th, 2013)*

A California federal jury [convicted](#) a San Francisco executive recruiter this week for violations of the Computer Fraud and Abuse Act (“CFAA”) and theft of trade secrets from his former employer. The conviction represents a significant landmark in the closely watched eight-year case that deepened a federal circuit court split concerning the appropriate scope of the CFAA.

The case involves executive recruiter and former employee David Nosal, who allegedly conspired with then-current employees at his former employer, Korn/Ferry, to illegally access and download valuable candidate lists and other trade secret information from Korn/Ferry’s “Searcher” database. Nosal’s accomplices were able to access the computer system through a password provided to them by Nosal after he borrowed the password from a current Korn/Ferry employee. Nosal allegedly used this newly acquired information to start a competing business, Nosal Partners.



Nosal was indicted by a federal grand jury in 2008 for, *inter alia*, violations of the CFAA and trade secret theft. The district court for the Northern District of California initially dismissed several CFAA counts on grounds that the employees he allegedly conspired with had access to the computer systems and, thus, could not “exceed authorized access” under the CFAA. The prosecution argued that the employee’s violations of his employer’s computer use restrictions “exceeded their authorized access,” but the court found the employer’s restrictions irrelevant to such a determination.

In April 2011, the Ninth Circuit Court of Appeals [reversed the district court](#) and held that a former employee “exceeds authorized access” to data on his employer’s computer system under the CFAA where the employee takes actions on the computer that are prohibited by his employer’s written policies and procedures concerning acceptable use (e.g. prohibitions against copying or e-mailing files to compete or help a third party compete with the employer). The decision strengthened the CFAA as a viable remedy to help fight employee data theft.

The following year, however, a Ninth Circuit en banc panel [affirmed the district court’s decision](#), reversed the prior Ninth Circuit opinion, and adopted a narrow interpretation of the CFAA. The panel found that an employee’s violation of his/her employer’s computer usage policies was not a violation of the CFAA. The Court focused on whether the employee originally had access to the information, not whether the employee misused the employer’s confidential information in violation of usage policies. The decision widened a split between the circuit courts regarding the proper interpretation of unauthorized access under the CFAA and its applicability to factual scenarios where employees allegedly steal company data in violation of computer usage policies or in breach of their loyalty obligations.





# Trading Secrets



The government subsequently obtained superseding indictments, and charged Nosal with, *inter alia*, the remaining CFAA and trade secret theft counts. During the two-week trial, Nosal's defense team developed a theme that Korn/Ferry was a corporate Goliath "[using the government to essentially do \[its\] dirty work](#)" and the case was a "[perversion of the criminal process](#)" orchestrated by Korn/Ferry to eliminate him as a competitor. The prosecution responded by reemphasizing that "[it's the defendant that's on trial here ... not Korn/Ferry.](#)"

Nosal was found guilty on these counts on April 24, 2013 after two days of jury deliberations. [None of the jurors would discuss their deliberations.](#)

It is anticipated that the case may again return to the Ninth Circuit Court of Appeal for a third decision. One of the significant issues likely on appeal involves the factual scenario seen in *Nosal* where a password is borrowed by one individual, he/she provides the password to a second individual, and the second individual uses the password to access a computer system—is the first individual liable under the CFAA for "unauthorized access"? In fact, some legal commentators question [whether Nosal actually committed a direct violation of the CFAA](#). Nevertheless, the case will continue to be closely monitored.

Nosal is scheduled for sentencing on September 4, 2013. He faces penalties up to five years' imprisonment and \$250,000 for the computer offenses, and up to 10 years' imprisonment and \$250,000 for the trade secret offenses.

# Trading Secrets



## California Federal Court Dismisses Computer Fraud and State Unfair Competition Claims Alleged Against Ex-Employees Accused Of Stealing Computer Source Code

By Paul Freehling (May 6th, 2013)

A designer and marketer of stereophonic technology for presenting 3-D imaging on a computer screen recently sued some ex-employees in a California federal court for allegedly violating the federal Computer Fraud and Abuse Act (CFAA), among other claims. At some point, the ex-employees allegedly downloaded their former employer's confidential computer code and provided it to their new employer, a competitor. The defendants moved to dismiss on the grounds that there was no allegation as to exactly *how or when* the ex-employees obtained the code. In response to the motion, the plaintiff said it would need discovery in order to ascertain that information.



The court granted the motion and dismissed the complaint for failure to plead “facts giving rise to a valid claim under the CFAA.” The plaintiff was allowed 30 days “to amend, keeping in mind Rule 11 [the federal civil procedure sanctions rule], if Plaintiff is able to plead facts giving rise to a valid CFAA claim.” [\*Metabyte, Inc. v. Nvidia Corp.\*](#), Case No. 12-0044 SC (N.D. Cal., Apr. 22, 2013).

The CFAA prohibits “access[ing] a computer without authorization or exceed[ing] authorized access.” Some federal courts, such as the Ninth Circuit Court of Appeals, interpret that phrase narrowly and typically only find a violation if the “access” occurs by someone who was not authorized to use that computer or in excess of that authorization. See, e.g., *U.S. v. Nosal*, 676 F.3d 854 (2012) (*en banc*) and *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (2009).

Some other federal courts, including the Seventh Circuit Court of Appeals, disagree. They hold that, under the CFAA, *use of a computer to misappropriate* is unlawful even though the user was authorized to access the computer for lawful purposes. See, e.g., *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2008).

In addition to charging the individual defendants with violation of the CFAA, Metabyte accused Nvidia of violating the California Unfair Competition Law (UCL). Nvidia moved to dismiss the claim on the ground that it was pre-empted by the U.S. Copyright Act because Metabyte simply accused Nvidia of selling copies of products for which Metabyte had a copyright. The court agreed and dismissed that claim with prejudice.

Metabyte pled some causes of action besides those based on the CFAA and the UCL. For example, Metabyte claimed copyright infringement, breach of contract, and misappropriation of trade



# Trading Secrets



secrets. With respect to the CFAA claim, however, there is little likelihood that within a period as short as 30 days Metabyte will be able to learn sufficient relevant facts to adequately support an allegation of hacking or other actionable conduct. In the future, plaintiffs averring CFAA violations for misappropriation of confidential information by use of a computer, but uncertain exactly how or when the defendant obtained the information and/or access to the computer, would be well advised to carefully consider whether the federal circuit in which they plan to sue permit such claims.

# Trading Secrets



## No Damages? Illinois Federal Court Tosses Computer Fraud and Abuse Act Claim Alleging Hacking of Law Firm Network

*By Paul Freehling (May 13th, 2013)*

An Illinois federal court recently found in the favor of the defendant on a plaintiff's Computer Fraud and Abuse Act claim because the plaintiff allegedly failed to satisfy the statute's \$5,000 damages threshold.

The plaintiff, a computer consulting servicing company which spent time restoring its client's computer network (a Chicago law firm) after it was allegedly hacked by the plaintiff's former employee, sued the former employee for violation of CFAA, among other claims.

**CFAA's damages requirement.** The CFAA requires that a plaintiff prove the damage or loss resulted in losses to one or more persons during any one year period aggregating at least \$5,000 in value. 18 U.S.C. § 1030(c)(4)(A)(i). Summary judgment was entered against the plaintiff in the case for failure to show sufficient damages. [\*Technology Sourcing, Inc. v. Griffin\*, Case No. 10 C 4959 \(N.D. Ill., 4/30/13\)](#).

**Lawsuit filed against an alleged hacker.** TSI filed the lawsuit seeking to recover the value of the time it claimed it spent in restoring service to its client's computer network which crashed after being hacked. TSI's client was not a party to the lawsuit and apparently incurred no significant expense as a result of the hacking.

**Responsibility for the computer network crashing.** On June 10, 2010, TSI fired Griffin, its primary technician. Seven weeks later, one of TSI's clients reported that its server and network were inoperative. In the course of investigating the disruption and restoring the client's computer service at no cost to the client, TSI learned that the shutdown likely was caused by an unauthorized user twice attempting to log into the client's server. The unauthorized user's printer name belonged to Griffin. Suspecting that he was the hacker, the plaintiff sued him in federal court in Chicago.

**Summary judgment denied to the plaintiff and granted to the defendant.** After discovery was completed, both parties moved for summary judgment. The court held that partial summary judgment for the defendant was appropriate with respect to the plaintiff's CFAA count because TSI presented no "evidence that data was destroyed, erased, manipulated, [or] sent to a third party." Further, the plaintiff's president's deposition testimony, and his belated affidavit which was inconsistent in part with his testimony, did not satisfy the court that the \$5,000 damages threshold was met. The remaining claims — state law pendent jurisdiction causes of action — were dismissed without prejudice, as a matter of the court's discretion, to be pursued in state court if TSI chose to do so.

**Takeaways from this decision.** Unlike TSI's lawsuit, in the typical CFAA case, the plaintiff's computer, not a third party computer, is alleged unlawfully accessed. Also unlike TSI's lawsuit, the usual contention is either that data from the plaintiff's computer was used without permission by the person(s)





# Trading Secrets



who wrongfully accessed the computer or that the data was provided to someone else who used it without permission. The *Technology Sourcing, Inc.* opinion further indicates how difficult it is to state a justiciable CFAA claim when the only alleged damages are unbilled time incurred by a service technician spent in restoring a computer network which crashed due to alleged hacking.

# Trading Secrets



## Recent Alleged Cyberattack By Ex-Employee Demonstrates Importance of Employer Diligence On Protecting Network Passwords

*By Robert Milligan and Grace Chuchla (June 3rd, 2013)*

A recently unsealed criminal [complaint](#) out of the Eastern District of New York raises allegations that paint a frightening picture for employers of the havoc that disgruntled ex-employees can wreak on company computer networks.

The prosecution [alleges](#) that a former employee of an unnamed company that manufactures high-voltage power supplies in Suffolk County, New York improperly downloaded company files, accessed the company network, and altered key company source code after his resignation on December 30, 2011.

The employee allegedly resigned because he was unhappy about being passed over for a promotion and set his final day to be January 13, 2012. However, only one week after announcing his resignation, on January 6, 2012, the employee's supervisor claims to have observed him copying files from his computer onto a flash drive. Acting swiftly, the company blocked his access to their servers and VPN on January 7, 2013, but unfortunately, this was not enough to thwart the employee's alleged tampering with the company's networks.



During his time at the company, the employee worked with another unnamed employee maintaining the company's software. In the course of working together, this employee allegedly shared his password with the defendant. Furthermore, this employee had the practice of rotating between the same two or three passwords whenever the company's system prompted him to change it, and thus, the prosecution claims that the defendant, with some easy guesswork, was able to gain access to the company's systems via their VPN even after he had resigned and after the company had blocked his access to its system.

Working under his former coworker's credentials and after he left the company's employee, the defendant allegedly:

- Obtained the email addresses of candidates applying to fill his now vacant position and sent them messages from iamconcern2012@gmail.com telling them not to work for the Company;
- Modified dates within the computer code for the Company's Period Roll Tables, which prevented the Company from processing transactions during a critical month-end period;
- Deleted purchase order tables from the Company's systems; and





# Trading Secrets



- Deleted key lines of code from a program that calculates work order costs, which led to incorrect calculations.

When all was said and done, the company estimates that it spent approximately \$94,000 investigating and addressing the employee's alleged actions.

The U.S. Attorneys' Office [charged](#) the defendant under the Computer Fraud and Abuse Act.

"The defendant engaged in a 21st century campaign of cyber-vandalism and high-tech revenge," Loretta E. Lynch of the U.S. Attorney's Office for the Eastern District of New York [said](#) in a statement. "We will hold accountable any individual who victimizes others by exploiting computer network vulnerabilities."

FBI Assistant Director in Charge Venizelos [stated](#), "Bent on revenge, the defendant exploited his access and his technical know-how to sabotage his former employer. As alleged, he caused significant disruption and monetary damage. The FBI is committed to vigorous enforcement of laws governing computer intrusions."

The defendant could face up to 10 years in prison, a \$250,000 fine and restitution. He posted a \$50,000 bond and a Federal Defender was appointed to represent him.

The case is *United States of America v. Meneses*, case number 13M343, in the United States District Court for the Eastern District of New York.

This case follows the highly publicized *U.S. v. Nosal* case in which an executive recruiter [was convicted](#) under the Computer Fraud and Abuse Act where there were allegations of password sharing to obtain access to the company's computer network.

Regardless of the outcome of *Meneses*, the allegations made by the prosecution highlight a core rule of data protection — employees must keep their passwords confidential. In this day and age, we have hundreds of passwords swirling around our heads. It's no wonder, therefore, that they begin to lose their importance, and all too often, employees will nonchalantly share their passwords with a colleague or rotate between the same few passwords whenever the system requires a password change. Employers should be on the lookout for this kind of activity and should frequently impress upon employees how important it is to have both **unique and confidential passwords** and that they routinely change their passwords. IT specialists [recommend](#) that special care should be given to password security. Some believe that the [use of biometric authentication](#) will eventually surpass conventional passwords. Even implementing other trade secret protection measures — such as granting employees access to trade secrets only on a need-to-know basis — are useless if one employee obtains another employee's password and is able to have free reign on the company's computer network.

Additionally, companies must immediately disable network access of departing employees at termination. Most internal attacks happen through access obtained on the job that is not removed when the employee leaves, FBI assistant special agent Austin Berglas [reportedly told](#) businesses leaders at a recent cybersecurity conference. More commonly a "company fires someone in their IT department and forgets to block or cancel their login credentials," Mr. Berglas [reportedly said](#). "It's just so easy for them to use that password to steal data or do destructive things to the network...and it looks like normal traffic to IT staff."



# Trading Secrets



In this case, the company shut down the employee's access the day he left but he was allegedly able to figure out another employee's password because he had previously shared it with the defendant and that colleague rotated between similar passwords.

In the end, hindsight is 20/20, but the simple steps of maintaining the confidentiality of employee passwords, having unique passwords that are changed often, and shutting off network access of departing employees at termination can go a long way toward protecting your trade secrets and your company networks as a whole. Companies should also stay abreast of the latest in technologic enhancements, such as biometric authentication. We will continue to keep you apprised of developments in this case. For more information on the threats to trade secrets posed by cybersecurity attacks and mitigation strategies, please see [my recent presentation](#) with U.S. Attorney Wesley Hsu and cybersecurity specialist Steve Lee.

# Trading Secrets



## Minnesota Federal Court Dismisses Computer Fraud and Abuse Act Claim Based on Departing Employee's Downloading of Customer List

*By Erik von Zeipel (June 17th, 2013)*

On June 3, 2013, the U.S. District Court for the District of Minnesota granted in part and denied in part a motion for summary judgment filed by defendant former employees in a dispute arising out of the sale of a business to the plaintiff former employer, and the seller's subsequent starting of a competing business which the defendants joined. Of particular interest here, the Court granted summary judgment against the Computer Fraud and Abuse Act ("CFAA") claim related to the taking of the former employer's customer list and pricing index, holding that the CFAA requires more than just a misappropriation of information, it requires that access to the information was forbidden.



In June 2005, Lee Randt sold Randt Oil Company and related assets (including customer lists) to the principal of plaintiff Lubrication Technologies, Inc. ("Lube-Tech"). Shortly thereafter, Lube-Tech hired defendant Darren Randt, Lee Randt's son, as Operations Manager and his wife, defendant Jessica Randt, to perform day-to-day operations.

In the spring of 2011, Lee Randt formed a new company called Lee's Oil Service, LLC ("Lee's Oil") with his wife as the sole owner. Lee's Oil was a direct competitor to Lube-Tech. In May 2011, defendant Darren Randt resigned from Lube-Tech and went to work for Lee's Oil. Defendant Jessica Randt followed in July 2011. Before leaving Lube-Tech, Ms. Randt downloaded Lube-Tech's customer list and pricing index. Around the same time as Ms. Randt's departure, defendant Ronald Kern also left Lube-Tech and joined Lee's Oil. After joining Lee's Oil, Mr. Kern continued to serve many of the customers he had served at Lube-Tech. Some of those customers claimed that Mr. Kern made statements to the effect that Lube-Tech was no longer in business and would not be able to serve them.

On August 30, 2011, Lube-Tech filed an amended complaint alleging violations of the CFAA, the Lanham Act, the Uniform Deceptive Trade Practices Act, the Uniform Trade Secrets Act, common law fraud, trade secret misappropriation, breach of contract, tortious interference with business relationships and contract, civil theft, breach of fiduciary duty and usurpation of corporate business opportunities. Defendants answered and alleged counterclaims based on state law for unpaid wages, fraud and intentional interference with prospective economic advantage. On September 8, 2011, the Court issued a preliminary injunction enjoining defendants from, among other things, disclosing Lube-Tech's proprietary information, doing business with certain suppliers and making false statements about Lube-Tech.

The Court first addressed plaintiff's claim that defendant Jessica Randt violated the CFAA by downloading Lube-Tech's customer list and pricing index before leaving Lube-Tech, allegedly to benefit Lee's Oil. Under the CFAA, a person who "intentionally accesses a computer without authorization or



# Trading Secrets



exceeds authorized access, and thereby obtains ... information from any protected computer” is subject to imprisonment and a fine. 18 U.S.C. § 1030(a)(2)(C), (c). Citing *Walsh Bishop Assocs., Inc. v. O’Brien*, No. 11-2673, 2012 WL 669069, at \*2 (D. Minn. Feb. 28, 2012), the Court stated that “The Eight Circuit has not determined whether the CFAA imposes civil liability on employees who access information with permission but with an improper purpose.” Further citing *Walsh Bishop*, the Court stated that “a violation of the CFAA requires more than misappropriation of information” and the relevant inquiry was “whether defendants accessed information that they were forbidden to access.” Here, one of Ms. Randt’s primary responsibilities at Lube-Tech included implementing software to catalog Lube-Tech’s customers. Lube-Tech also had not alleged it had security measures or a computer-use policy. Because there was no evidence any defendant had obtained information they were forbidden to access, the Court granted summary judgment on the CFAA claim.

Having dismissed the CFAA claim, the Court granted summary judgment on plaintiff’s Lanham Act claims based on Lee Oil’s alleged copying of Lube-Tech’s logo and manifest. Having dismissed the only claims the Court had original jurisdiction over, the Court declined to exercise supplemental jurisdiction over the remaining state law claims and dismissed the same without prejudice.

# Trading Secrets



## Massachusetts Federal Court Narrowly Construes Computer Fraud and Abuse Act and Holds That Company Cannot Sue Former Employees For Downloading Proprietary Information Absent Showing of Fraud

*By Erik Weibust and Ryan Malloy (June 25th, 2013)*

You may recall that we previously [reported](#) on *Advanced Micro Devices, Inc. v. Feldstein, et al.*, C.A. No. 13-40007, in which Judge Timothy S. Hillman of the U.S. District Court of Massachusetts granted a preliminary injunction against three former employees of Advanced Micro Devices (AMD) who allegedly stole trade secrets from the plaintiff, without requiring a showing that the defendants actually used that information for the benefit of a competitor.



In the same case, Judge Hillman has now [ruled](#) that AMD company cannot sue former employees under the Computer Fraud and Abuse Act (CFAA) for downloading proprietary information onto personal devices before they left to work for a competitor without establishing that the employees had fraudulently or unlawfully accessed the information.

As noted in the previous blog entry, AMD is a designer and manufacturer of microprocessors and other computer parts. Defendants are former AMD employees who left AMD and were hired by AMD's competitor, Nvidia Corp. According to AMD, three of the defendants copied proprietary data from AMD-owned storage devices onto their own thumb drives and external hard drives while still employed by AMD, and retained the information after they left. Last January, AMD sued the defendants in U.S. District Court and asserted a claim for violation of the CFAA against the three defendants who allegedly copied proprietary data.

Although Judge Hillman declined to dismiss AMD's CFAA claim with prejudice, citing an "incomplete" evidentiary record, he nevertheless adopted a narrow definition of the term "authorized access" under the CFAA by requiring a showing that defendants acted with fraud or deception. Specifically, Judge Hillman found that AMD's allegations were insufficient to sustain a CFAA claim under a narrow interpretation of the statute, but permitted AMD to re-plead specific details indicating that some or all of the defendants used fraudulent or deceptive means to obtain confidential AMD information, and/or that they intentionally defeated or circumvented technologically implemented restrictions to obtain confidential AMD information.

In contrast, the broad definition of "authorized access" that has been adopted in other jurisdictions defines access in terms of use. Under this approach, any time an employee breaches a contractual obligation or a fiduciary duty to its employer, then the employee's authorization to access information on the employer's system terminates and all subsequent access is considered unauthorized. Noting that courts have taken conflicting approaches to the definition, Hillman warned:



# Trading Secrets



[I]f this court were to adopt a broad interpretation of the term of art ‘access that exceeds the scope of authorization’ then arguably any violation of a contractual obligation regarding computer use [such as idle Internet browsing] becomes a federal tort ... As between a broad definition that pulls trivial contractual violations into the realm of federal ... penalties, and a narrow one that forces the victims of misappropriation and/or breach of contract to seek justice under state, rather than federal law, the prudent choice is clearly the narrower definition.

Defendants’ motion to dismiss was also denied as to all other claims, except for AMD’s claim for unfair competition under Mass. Gen. Laws ch. 93A, section 11, on the ground that defendants correctly asserted the “inter-enterprise” exception to the statute



# Trading Secrets



## Significant Amendments Proposed to the Computer Fraud and Abuse Act to Limit Its Use to Traditional Hacking Scenarios

*By Robert Milligan and Grace Chuchla (June 26th, 2013)*

Earlier this year, [we blogged on](#) federal legislative efforts to amend the Computer Fraud and Abuse Act (“CFAA”) following the death of computer activist Aaron Swartz. These efforts were spearheaded by Representative Zoe Lofgren (D-CA), who released her [discussion draft](#) of proposed amendments to the CFAA on January 15, 2013 on Reddit. Lofgren’s January draft sought to modify the definition of “exceeds authorized access” so that those who only violate, for example, a computer use policy or internet terms of service cannot be held liable under the CFAA.

On Thursday, June 20, Representative Lofgren and Senator Ron Wyden (D-OR) formally introduced companion bills in both the [House](#) and [Senate](#) seeking to amend the CFAA. According to [Senator Wyden’s website](#), these amendments seek to eliminate “vagueness” and “redundant provisions” from the CFAA and “establish that a mere breach of terms of service, employment agreements, or contracts are not automatic violations of the CFAA.” Additionally, with the nickname “Aaron’s Law,” they also seek to limit what some see as the CFAA’s tendency to allow for overzealous prosecution that they claim characterized Aaron Swartz’s case.



As before, both [bills](#) seek to clarify the meaning of “exceeds authorized access” by striking it and replacing it with the phrase “access without authorization,” which is defined to mean

- a) “to obtain information on a protected computer”;
- b) “that the accesser lacks authorization to obtain”; and
- c) “by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information.”

Both bills also propose amendments to the definition of punishable offenses under the CFAA by inserting a requirement that offenses committed for commercial advantage or private financial gain must also involve information that has a market value over \$5,000.

Lofgren and Wyden [said](#) in their opinion piece for Wired that, “Aaron’s Law is not just about Aaron Swartz, but rather about refocusing the law away from common computer and Internet activity and toward damaging hacks.”



# Trading Secrets



Opinions are split on how successful these proposed amendments will be. On the one hand, [previous efforts to amend the CFAA](#) in April 2013 failed after there was significant opposition from both the left and the right. Those proposed amendments to the CFAA, however, are not similar to what is currently in front of Congress. The Justice Department has previously been against amendments to the CFAA that would significantly narrow the Act's scope. It recently obtained the [conviction](#) of David Nosal under the CFAA in San Francisco, California (the conviction has been appealed to the Ninth Circuit). Additionally, Richard Downing, Deputy Section Chief for Computer Crime and Intellectual Property, [told the House in 2011](#) that removing key parts of the CFAA "could make it difficult or impossible to deter and punish serious threats from malicious insiders."

BSA Software Alliance has come out [against](#) the proposed legislation, arguing that it would force companies to build additional security mechanisms into their networks and systems to adequately protect them from unauthorized parties. "Everyone agrees that lying about your age on Facebook shouldn't be a felony, but Aaron's Law is a flawed solution to that problem," Tim Molino, BSA's director of government relations, [reportedly said](#) in a [statement](#). "Tying liability to theft that involves 'knowingly circumventing technological or physical measures' is out of step with the technology innovations driving today's economy. It would compel many companies to erect new technical protection measures throughout their networks and support systems, reversing a trend that has contributed the growth of cloud computing, software as a service, and on-demand support."

Additionally, with the [highly publicized omnipresent cybersecurity threat](#) and [recent high profile employee data theft cases](#), there may not be significant momentum to drastically change the CFAA, particularly with the Obama Administration [focused](#) on addressing the cybersecurity threat. Echoing those sentiments, Molino [reportedly said](#) the bill is "especially troubling at a time when hacking and intellectual property theft are rampant — weakening cybercrime laws would be like handing out keys to the castle."

On the other hand, however, advocacy groups have come out in vocal support of Lofgren's and Wyden's bills. The [Center for Democracy and Technology](#) and [Demand Progress](#) have both issued recent statements applauding Aaron's Law for "prevent[ing] the government from using the Computer Fraud and Abuse Act (CFAA) to prosecute mere terms-of-service violations as computer crimes, and prevent prosecutors from bringing multiple redundant charges based on a single crime." Further, the Electronic Frontier Foundation has also been a [vocal supporter](#) of the proposed amendments, [stating that](#), "(t)he CFAA was originally intended to cover the hacking of defense department and bank computers, but it's been expanded so that it now covers virtually every computer on the Internet while meting out disproportionate penalties for virtual crimes. We've written extensively about the need for CFAA reform and Aaron's Law is a great first step." Additionally, with the recent NSA and Snowden kerfuffle, there may be public support for limitations on the CFAA, including limiting its use for pure hacking scenarios.

How this will play out is anyone's guess. What started with a circuit split after the [Ninth Circuit's decision in U.S. v. Nosal](#) has grown into a hot-button topic for everyone from civil rights activists to technology lobbying organizations to employers looking to protect their data. Stay tuned for updates as the saga unfolds.

# Trading Secrets



## Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part I

*By Erik von Zeipel (August 29th, 2013)*

On April 25, 2013, a federal jury [convicted](#) Executive Recruiter David Nosal on three counts under the [Computer Fraud and Abuse Act](#) (“CFAA”), two counts under the [Economic Espionage Act](#) (“EEA”), and one count of conspiracy to violate the CFAA and EEA, for Nosal’s conduct leaving his former employer and establishing a competing business in 2004 and 2005.

The conviction followed an FBI investigation and multiple indictments alleging that Nosal conspired with former co-workers to gain unauthorized access to his former employer’s computers system and to illegally obtain its trade secrets – source lists of candidates compiled for search assignments – to use in his competing business.



On August 7, 2013, U.S. District Judge Edward Chen heard argument on Nosal’s motions for acquittal and a new trial and took both motions under submission. On August 15, 2013, the Court [issued its ruling](#), denying both motions in a 39-page order.

This is Part I of a three part post. In this post we will look at the Court’s order on Nosal’s conviction of the CFAA counts. In Part II, we will review the EEA counts. Finally, in Part III, we will try to foresee what the future may hold for Nosal and look at some lessons employers can learn from this case.

### **A. Nosal’s Conviction on the CFAA Counts:**

Nosal was convicted of three counts under the CFAA for accessing his former employer’s computers and obtaining information on three separate occasions. In relevant part, the CFAA provides criminal penalties for:

[whoever] knowingly and with intent to defraud, accesses a protected computers without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computers and the value of such use is not more than \$5,000 in any 1-year period;

18 U.S.C. § 1030(a)(4).

In his motions, Nosal argued broadly that he was entitled to acquittal or a new trial on the CFAA counts because: (1) no person gained unauthorized access to his former employer’s computers within the meaning of the CFAA; (2) the deliberate ignorance jury instruction was confusing; (3) there was insufficient evidence that Nosal had the requisite mental state to commit the CFAA violations; and (4) there was insufficient evidence of a conspiracy.



# Trading Secrets



## 1. Unauthorized Access to his former employer's Computers

In support of the “no unauthorized access” argument, Nosal argued that: (1) under the [Ninth Circuit's en banc decision](#) in this case (*United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012)), there can be no CFAA violation because any access to his former employer's computers was gained with the permission of the password holder and there was no circumvention of technological barriers; (2) Nosal's former co-workers were authorized to access the computers; and (3) Nosal was authorized to receive certain information in the course of his work as an independent contractor for his former employer.

The Court rejected Nosal's first argument, holding that “[n]owhere does the court's opinion in *Nosal* hold that the government is additionally required to allege that a defendant circumvented technological access barriers in bringing charges under § 1030(a)(4)” and also noted that the indictment actually does allege circumvention of a technological barrier because “password protection is one of the most obvious technological access barriers that a business could adopt.”

The Court also dismissed Nosal's second argument that his former co-workers were authorized to access his former employer's computer, holding that the evidence established they did not have his former employer's authorization and “that it is the actions of the employer who maintains the computers system that determine whether or not a person is acting with authorization.” In so doing, the Court distinguished Nosal's argument that the verdict was criminalizing the allegedly common practice of employees sharing passwords with each other to access their employer's computers systems by explaining that here, an employee of his former employer impermissibly gave her password, not to a co-worker, but to former employees who were not authorized to access the computers.

The Court also rejected Nosal's argument that his former co-workers were authorized to access his former employer's computers on the relevant dates, finding that the evidence sufficiently established that they were not authorized. Finally, the Court rejected Nosal's argument that he was authorized to receive certain information from his former employer's computers in his work as an independent contractor, holding he was only authorized to receive limited information relevant to specific work he was doing for his former employer, but that the information he received was for his competing business.

## 2. Deliberate Ignorance Jury Instruction

Nosal also argued that an instruction that the jury could find that he had acted “knowingly” to violate the CFAA if he was aware of a high probability that his former executive assistant or former co-workers had gained unauthorized access to the computers or misappropriated trade secrets, and he deliberately avoided learning the truth, was confusing because his former executive assistant was at all relevant times employed by his former employer and was authorized to access the computers while the other former co-workers were not employed by his former employer and were not authorized.

The Court held that Nosal had waived this argument by not raising it earlier. Moreover, the Court held that the instruction was sufficiently clear that the jury could not convict Nosal on the CFAA counts if they concluded his former executive assistant has accessed the computers, because such access would not have been “unauthorized.”

## 3. Evidence Nosal had Knowledge of Unauthorized Downloads

Nosal further argued that there was insufficient evidence he had knowledge of downloads from his former employer's computers were unauthorized because the downloads were not conducted by his



# Trading Secrets



former executive assistant. Reciting substantial evidence presented at trial by the government, including evidence that Nosal gave his former co-workers specific directions about information he wanted from his former employer's computers, that he knew a former co-worker had a large amount of data taken from the computers, that he knew they were not authorized to obtain the information, and that Nosal's executive assistant did not know how to do so, the Court concluded the government had proved beyond a reasonable doubt that Nosal knew of, was deliberately indifferent to, and/or had conspired to commit the CFAA violations.

#### **4. Evidence of Conspiracy**

Nosal also argued that there was not sufficient evidence of conspiracy. The Court dismissed this argument, concluding that the same evidence that Nosal had knowledge of the downloads from his former employer's computers was sufficient to support the verdict on the conspiracy count.

***In Part II of this post, we will look at Nosal's conviction on the EEA counts.***

# Trading Secrets



## Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part II

*By Erik von Zeipel (August 30th, 2013)*

In [Part I](#) of this post, we reviewed the Court's ruling on Nosal's conviction on the CFAA counts. Here in Part II, we turn to the Court's ruling on the [EEA](#) counts, and the exclusion of evidence regarding Nosal's non-compete provision.

### **B. Nosal's Conviction on the EEA Counts:**

Nosal was convicted of two counts under the EEA for downloading, copying and duplicating his former employer's trade secrets without authorization, and for receiving and possessing his former employer's stolen trade secrets. In relevant part, the EEA provides:



Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly –

...

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3);

...

shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a).

Nosal raised four arguments for acquittal or a new trial on the EEA counts: (1) instruction that jury could find Nosal guilty of conspiracy to commit the EEA violations even if there was no trade secret was erroneous; (2) there was insufficient evidence that the source lists were trade secrets; (3) there was





# Trading Secrets



insufficient evidence that Nosal and his co-conspirators knew or believed that the source lists were trade secrets; and (4) there was insufficient evidence that Nosal and his co-conspirators knew or believed that taking the source lists would cause his former employer economic harm. The Court rejected each of these arguments.

## 1. Requirement of Existence of Actual Trade Secret

Nosal argued for acquittal or a new trial on all counts claiming the Court erroneously instructed the jury that it could find him guilty of conspiracy to misappropriate, receive, possess, and transmit trade secrets even if the source lists were not trade secrets as long as he “firmly believed” they were.

The Court rejected this argument based on authority holding that legal impossibility is not a defense to conspiracy charges, including *United States v. Hsu*, 155 F.3d 189, 193 (3d Cir. 1998). The defendants in *Hsu* were charged with attempt and conspiracy to steal trade secrets, and sought discovery to prove that the documents they had attempted to obtain were not trade secrets. The *Hsu* court ruled that the documents were not relevant because legal impossibility is not a defense to either attempt or conspiracy. *Id.* at 203. The Court further cited the Supreme Court’s recognition that conspiracies are distinct and independent evils punishable by themselves. *Salinas v. United States*, 522 U.S. 52, 65 (1997).

The Court also found that the legislative history of EEA specifically supported a finding that a “firm belief” satisfied the “knowingly” element. The Court further concluded that any error in the instruction was harmless because the jury found Nosal guilty of the substantive EEA counts, and to do so it had to find that at least one of the source lists was a trade secret. The Court also dismissed several other arguments, including that the conspiracy instruction was a constructive amendment of the indictment because it sought conviction based on the theory that Nosal “firmly believed” the source lists were trade secrets, even if they were not.

## 2. Evidence the Source Lists Were Trade Secrets

Nosal also argued for acquittal or a new trial on the EEA counts because there was insufficient evidence the source lists were, in fact, trade secrets, and specifically that the information was not drawn from publicly available sources and that the source lists had not been publicly disclosed.

The Court dismissed this argument citing evidence introduced at trial that would support a finding that the source lists were compilations of both public and non-public information, and that the jury could have inferred based on Nosal’s efforts to retrieve the source lists that the information therein was not entirely public.

The Court also held that the jury could reasonably have found that the trade secret status of the source lists was not destroyed by disclosure to third parties based on evidence that such disclosure was relatively rare and that the alleged trade secrets had not been disclosed to third parties, or had been disclosed only subject to a confidentiality agreement.

Finally, based on a review of the balance of evidence, the Court concluded there was sufficient evidence to conclude his former employer had taken “reasonable” steps to protect the source lists as trade secrets.

## 3. Evidence Conspirators Knew Source Lists Were Trade Secrets



# Trading Secrets



Nosal also demanded acquittal or a new trial because there was not sufficient evidence that he and his co-conspirators knew the source lists were trade secrets. The Court disagreed, holding there was sufficient evidence showing both that the co-conspirators were aware that the specific source lists were, in fact, trade secrets, and that the co-conspirators attempted to keep their activities secret, from which the jury could have inferred they knew the information was trade secret.

#### **4. Evidence Conspirators Knew Taking Source Lists Would Cause Harm**

Nosal also argued for acquittal or a new trial because there was insufficient evidence that the co-conspirators intended or knew that their actions would injure his former employer, as is required by the EEA. In reviewing the evidence, the Court concluded there was sufficient evidence from which the jury could conclude that the co-conspirators knew their actions would injure his former employer, including that they were starting a business to compete with his former employer.

#### **C. Exclusion of Evidence Regarding Non-Compete**

Finally, Nosal demanded a new trial on all counts claiming he was prejudiced by not being allowed to argue that a non-compete provision in his independent contractor agreement with his former employer was illegal.

The Court stated that, in ruling on motions *in limine*, it precluded *either* party from presenting evidence or argument as to whether the provision was actually legal and enforceable. In rejecting Nosal's demands, the Court held that there was no convincing argument that this ruling was in error, or that Nosal was so unfairly prejudiced by evidence and argument presented at trial relating to the non-compete as to require a new trial.

***In the final part of this post, we will look at what may be next for Nosal, and also look at some lessons employers can learn from this case.***

# Trading Secrets



## Nosal Update: Court Denies Motion for Acquittal and New Trial in Marathon CFAA and Trade Secret Misappropriation Criminal Case – Part III

*By Erik von Zeipel (September 3rd, 2013)*

In Parts [I](#) and [II](#) of this post, we looked at the Court's ruling on Nosal's motion for acquittal and new trial following his conviction of three [CFAA](#) counts, two [EEA](#) counts and one count of conspiracy. In this final part, we look at what may lie ahead for Nosal and lessons employers may learn from this case.

### What's Next for Nosal?

Sentencing in this case is now scheduled for October 9, 2013. Nosal faces a maximum statutory penalty of five years' imprisonment and a fine of \$250,000, plus potential restitution, on the conspiracy and CFAA counts, and 10 years' imprisonment and a fine of \$250,000, plus potential restitution, on the EEA counts.



Presumably, this matter will once again end up before the Ninth Circuit which will determine whether the conviction and the Court's denial of Nosal's motions for acquittal and a new trial will stand or whether they run afoul of the Ninth Circuit's earlier *en banc* decision in this case. Earlier, Judge Kozinski, writing for the majority, affirmed the dismissal of CFAA counts against Nosal finding that the statute was intended to punish hacking, not misappropriation of trade secrets in violation of an employer's acceptable use policies. In the opinion, Judge Kozinski stated that to hold otherwise would make a federal crime out of non-business related conduct in violation of acceptable use policies such as "g-chatting with friends, playing games, shopping or watching sports highlights." A strong dissent by Judge Barry Silverman argued that this case has nothing to do with such innocent violations of employer policy, apparently suggesting that such conduct, although "unauthorized access," would not fall under the CFAA because the required element of fraud is missing. Conversely, Judge Silverman stated that this case was about fraudulent and unauthorized access to a computers with the intent to steal valuable information.

Perhaps any future ruling will address password sharing and provide useful guidance on how to design acceptable use policies prohibiting conduct running afoul of the CFAA, without offending Judge Kozinski's sensibilities. Stay tuned.

### What can employers learn from this case?

Obviously, Nosal's former employer did a lot of things right which allowed the government to successfully prosecute and convict Nosal. For starters, his former employer protected its trade secrets by in a number of ways, including that: (1) it did not permit trade secrets to be sent outside the company; (2) it required usernames and passwords to access computers; (3) it housed its database containing the trade secrets at a secure data center with restricted access; (4) it protected the database with a firewall and anti-virus software; (5) it monitored users' downloading activity; (6) the database



# Trading Secrets



warned users with messages that information was to be used for “company business only”; and (7) lists exported from the database stated the information was “Proprietary & Confidential.” Based on these efforts, the Court concluded that Nosal’s former employer took reasonable steps to protect its trade secrets.

However, although ultimately not determinative in this case, the Court also noted evidence of things that Nosal’s former employer did not do, including that: (1) it did not prevent users from e-mailing source lists outside the company; (2) it did not prevent users from printing source lists; (3) it did not encrypt source lists or protect them with separate passwords; and (4) it did not have a procedure for preventing employees from printing and taking source lists home. It is possible some of these additional safeguards may have made misappropriation more difficult, or even prevented it altogether.

There are also a number of additional safeguards and procedures not referenced in the order that companies should consider as part of “best practices” in preventing trade secret theft. For example, the order is silent as to Nosal’s former employer’s onboarding procedures, and whether it used non-disclosure and trade secret protection agreements to protect sensitive information. It is also unclear what, if anything, his former employer did to educate and to continue to remind its workers regarding their obligations to protect company information. There is also no information as to whether his former employer conducted exit interviews, and whether it used exit interview certifications requiring departing workers to confirm they did not have any company trade secrets or confidential or proprietary information. All of these may be helpful tools in protecting company information. While none of these efforts by themselves prevent misappropriation, workers who are informed and understand that a company values and protects such assets are presumably less likely to misappropriate.

# Trading Secrets



## Computer Fraud And Abuse Act Violated By Bundling Facebook And Other Social Networking Accounts Without Authorization

*By Paul Freehling (October 7th, 2013)*

A California federal court recently issued a substantial monetary award in favor of Facebook and permanent injunction against a website that enabled its users to aggregate their data in social networking sites and messaging services.

Summary of the case. Power Ventures, Inc. (PVI) operates a website called power.com which integrates multiple social networking accounts. In late 2008, PVI began permitting participants to access their Facebook accounts through power.com. Then, PVI launched a promotion in which participants were offered an opportunity to receive a cash payment by selecting Facebook “friends” to whom power.com advertising should be sent. The advertising did not mention PVI and implied that it came from Facebook.



When it learned of the promotion, Facebook blocked power.com’s access to Facebook accounts. In addition, Facebook sued PVI and its principal owner-officer, Vachini, alleging various causes of action including violation of the Computer Fraud and Abuse Act (“CFAA”). All parties moved for summary judgment. In February 2012, Facebook’s motion was granted. [Facebook, Inc. v. Power Ventures, Inc.](#), Case No. 08-05780 (C.D. Calif., Feb. 16, 2012) (Ware, J.). A few days ago, the defendants’ motion for reconsideration was denied. [Id.](#) (Sept. 25, 2013) (Koh, J.).

The court’s February 2012 ruling that PVI violated the CFAA. The CFAA prohibits obtaining “information” by accessing, without authority, a protected computer. 18 U.S.C. §1030(a)(2)(C). The statute also prohibits accessing a protected computer without authorization and obtaining “anything of value” provided that it is worth \$5,000 or more. §1030(a)(4). Judge Ware [found](#) that PVI violated §1030(a)(2)(C) by accessing Facebook’s website without authorization and obtaining “information.” Further, the court found that Facebook had standing to sue because its documented costs incurred in thwarting PVI’s continued unauthorized access exceeded \$5,000. Facebook’s motion for summary judgment against PVI was granted. Unresolved were what relief to award and whether Vachani also was liable.

Denial of reconsideration. Due to a number of intervening events, a decision on the unresolved issues and on the defendants’ motion for reconsideration was not announced until 17 months after the original ruling. Those events included the filing and later dismissal of PVI’s and Vachani’s bankruptcy petitions. In addition, while the automatic bankruptcy stay was in effect, Judge Ware resigned from the bench, and the case was reassigned to Judge Koh.

The defendants’ first argument in support of reconsideration was that no violation of CFAA was shown because Judge Ware did not find that the “information” PVI obtained from Facebook had



# Trading Secrets



“value.” Section 1030(a)(4) criminalizes unauthorized access to a protected computer and obtaining “anything of value” of at least \$5,000. Curiously, however, the word “value” is not mentioned in §1030(a)(2) which simply prohibits obtaining “information” from unauthorized access to a protected computer, even, apparently, if the information has no *value*. Judge Koh held that Judge Ware’s finding of a violation of §1030(a)(2) was warranted.

PVI also said that no violation of the CFAA was shown because the defendants were not alleged to have destroyed any information or data. Many CFAA complaints do allege that a defendant destroyed computerized information or data, but neither §1030(a)(2) nor §1030(a)(4) requires such an allegation.

The defendants challenged Facebook’s standing to sue because, allegedly, no harm was demonstrated. Section 1030(a)(5)(C) criminalizes accessing a protected computer without authorization which “causes damage and loss.” Judge Koh [held](#) that Facebook satisfied the statutory standing requirement by showing that Facebook incurred “damage and loss” by “responding to an offense” and “conducting a damage assessment” (§1030(e)(11)).

Finally, with regard to Vachani’s liability, Judge Koh cited Ninth Circuit authority for a finding of personal liability when a corporate officer or director authorizes, directs, or participates in corporate wrongdoing. Drawing all reasonable inferences in Vachani’s favor, she said that the undisputed evidence proved that he authorized and directed the statutory violation.

For the foregoing reasons, Judge Koh held that Facebook was entitled to compensatory damages from both defendants. Since all of the requisites for obtaining a permanent injunction were satisfied, the defendants also were enjoined from committing further violations of the CFAA.

Takeaways. Many reported CFAA decisions concern either (a) an employee’s or ex-employee’s alleged unauthorized access to computerized information obtained for the purpose of engaging in unfair competition, or (b) hacking into a computer. The allegations in *Facebook* are different. Judge Koh summarized Facebook’s CFAA claim as: The defendants induced “Facebook users to provide their login information,” used “that information to ‘scrape’ Facebook’s proprietary material,” and proceeded to “display Facebook’s material on power.com. Facebook asserts that it never gave Defendants permission to use its material in that way.” PVI’s position was that it did not circumvent any technical barriers in order to access the Facebook site, and Facebook’s own servers sent the emails at issue, and so PVI did not violate the CFAA.

Arguably, at its core, *Facebook* may be said to hold that the CFAA prohibits accessing a computer network without express authorization and obtaining (a) information, regardless of its value, or (b) anything else that has substantial value. If so, the decision may support the proposition, for example, that actions as common as accessing without permission someone’s social media site in order to gather information or valuable data concerning the user of that site violates the CFAA.



# Trading Secrets



## Whatever Happened to Detention? Principal Sues Students Under Computer Fraud and Abuse Act For Allegedly Creating Fake Social Media Account

*By Jessica Mendelson (October 25th, 2013)*

As social media becomes more engrained in our lives, we hear more and more about its use among students. Although some of these uses are perfectly legitimate, others, such as the use of social media for bullying or defamatory purposes, are not. In a recent case in Oregon, [Matot v. CH et al](#), the court addressed the question of whether the “subject of a fake social media account” could successfully claim a violation of the Computer Fraud and Abuse Act (“CFAA”) against the creators of the fake profile. The court answered the question with a resounding “No.”



Recently, students at a Oregon high school allegedly created a fake social media account for the school's principal and allegedly began posting obscene materials on this page. Mr. Matot filed suit against both the students and their parents, alleging defamation and negligent supervision, as well as a violation of the CFAA. According to the principal, in allegedly creating these postings, the defendant students had allegedly used school computers in a manner which “exceeded authorized access” under the CFAA.

The federal district judge in Oregon, however, found otherwise, and held that there was no violation of the CFAA. In determining this, the court first addressed [LVRC Holdings L.L.C. v. Brekka](#), a Ninth Circuit case, where the court found that an employee's misuse or misappropriation of an employer's confidential or proprietary information is not “without authorization” as long as the employer has given permission to the employee to access this information. Here, unlike in *Brekka*, the defendants were not employees of the social media sites, and instead, their relationship with the website was entirely based on an alleged forgery. The court next addressed the [United States v. Nosal](#) case, where the Ninth Circuit previously held that lying on social media websites was common, and declined to recognize this as a CFAA violation.

Ultimately, the court in [Matot](#) concluded that the term authorization has been narrowly interpreted under Ninth Circuit law, and any ambiguity concerning criminal statutes should “be resolved in favor of lenity.” Here, if the court were to consider lying on social media websites a violation of the CFAA, millions of people could be charged with violations of this statute, including law enforcement officials. As such, the court found dismissal of this claim was proper. Furthermore, the court denied leave to add a RICO claim, [finding](#), “Congress did not intend to target the misguided attempts at retribution by juvenile middle school students against an assistant principal in enacting RICO.”

Interestingly, as Venkat Balasubramani [points out](#) on the Technology and Marketing blog, the court failed to address the question of whether the principal actually had standing to pursue the claim. According to Balasubramani, civil claims under the CFAA can only be pursued where a computer is accessed without authorization and the principal failed to show the students lacked such



# Trading Secrets



authorization. Additionally, he points out that the court did not address the impact of the students' First Amendment Rights, if any, or whether their parents could actually be held liable.

Based on this case and some other rulings in the Ninth Circuit, creating a fake social media profile, on its own, cannot be the basis for a CFAA claim, at least for now apparently.



# Trading Secrets



## Non-Competes & Restrictive Covenants

# Trading Secrets



## To Work or Not to Work – Maryland’s Senate Considers Changes To Non-Compete Law for Those on Unemployment

*By Scott Schaefer (January 17th, 2013)*

On January 9th, the Maryland Senate introduced a bill which if passed would invalidate employee “noncompetition covenants” for former workers who applied for and obtained unemployment benefits. [Senate Bill 51](#) is sponsored by Senator Ronald N. Young, Democrat, who just began his third year in the Maryland Senate. If enacted, the bill will take effect on October 1, 2013, and would not affect any noncompetition covenant entered into before then.



Theoretically, the bill’s purpose is to eliminate obstacles for workers on unemployment to return to work, thus reining in benefit payments and, by extension, unemployment taxes on employers. So far, so good. But I have to ask:

### 1. Will it work?

In other words, what will the bill as written really do? Will it apply to purely non-compete agreements, where an employee is barred from working for a competitor in a directly competitive capacity for a limited time? Or will they apply more broadly to other types of restrictive covenants, i.e., agreements not to solicit current employees or customers, or non-disclosure agreements? As explained below, it’s an important distinction.

As presently worded, the bill would apply to “noncompetition covenants.” But Maryland state and federal courts have used the term “restrictive covenant” and “noncompetition covenant” interchangeably, with little or no distinction between non-competes, non-solicitations, and non-disclosures. See, e.g., *MCS Servs., Inc. v. Jones*, No. WMN-10-1042, 2010 WL 3895380, at \* 3-4 (D. Md. Oct. 1, 2010); *Mansell v. Toys ‘R’ Us, Inc.*, 673 F.Supp.2d 407, 416-17 (D. Md. 2009); *Becker v. Bailey*, 268 Md. 93 (1973).

Sure, one might respond by saying of course SBI won’t apply to agreements beyond pure non-competes. After all, statutes in derogation of common law are strictly construed (*Cosby v. MDHR*, 425 Md. 629, 645 (2012)), and SB 51 doesn’t say anything other than noncompetition covenants. Further, Maryland’s Trade Secrets Act’s non-preemption provision, which keeps intact all breach of contract claims based on information theft (Md. Com. Law § 11-1207), is a counter-statutory basis to keep SB 51 away from employers’ breach of NDA claims. In addition, because the “inevitable disclosure” theory does not exist in Maryland, crafty employers can’t pull an end run around the non-compete bar by suing SB 51-eligible employees unless they have proof of actual trade-secret theft. *LeJeune v. Coin Acceptors, Inc.*, 381 Md. 288 (2004).

Nevertheless, even with the non-compete-only reading, employers and their attorneys can be clever. They can call something a non-solicit or non-disclosure, but give it a non-compete’s teeth. For



# Trading Secrets



example, John Smith's (fictional) non-solicit says he cannot solicit orders or sales from any of TUV's (his former employer, also fictional) customers for two years. John is a widgets salesman, and his territory is nationwide. He knows no other customers, and knows no other trade. No competing company will hire him without a portable and sizeable book of business. He knows, he tried. On its face, therefore, his non-solicit with TUV doesn't bar him from competing, but in reality, it does. SB 51 won't help him.

Further, the non-solicits and non-disclosures often have the same deterrent effect as non-competes have legal effect. Betty Boop, a former software engineer for Acme, who unlike John doesn't have a non-solicit, but who does have a non-compete and a three-page NDA with Acme which appears to cover every piece of paper she ever touched there, may nevertheless be inhibited by her NDA from taking a job with a competitor for fear of breaking that agreement. This is so even though she is not legally prohibited from working for that competitor. So, even though SB 51 would erase Betty's non-compete when she got on unemployment, her NDA still hung over her head enough to render SB 51 meaningless.

Or consider this: Sly Stallone and his new employer could time Sly's hire date at the day after he obtains unemployment benefits. That way, Sly's non-compete with his former employer will be dead, and Sly and his new employer are off the hook. Now, maybe that's not such a bad thing – an employee whose former employer laid him off on grounds other than for cause can't turn around and enforce his non-compete. Indeed, there is some Maryland authority (albeit tenuous) which suggests that an employer which terminates the employment without cause also terminates the employee's non-compete obligations. *Jorgensen v. United Comms. Group LP*, No. 8:10-CV-00429-AW, 2011 WL 3821533, at \* 10 (D. Md. Aug. 25, 2011).

But two caveats to that. First, as indicated, *Jorgensen* by no means is settled law, but instead relied on the bland contract principle that one who materially breaches can't also sue for breach. And *Jorgensen* did not actually declare the non-compete void, it merely denied summary judgment on that point. Second, many employees are terminated for something they did wrong, but out of respect for the past relationship, e.g., are allowed to call it a lay-off with the promise that the employer won't fight unemployment. Such employees with a non-compete will have benefited under SB 51 from whatever they did wrong to get them fired. Is that fair?

Now some might say, "so what? All this happens anyway, with or without a non-non-compete law like SB 51." I agree. Which brings me back to my original question – will SB 51 really do anything?

## **2. Another question – does Maryland really want SB 51?**

Put differently, will anyone win? Employers may fight harder against unemployment claims, now that the stakes are higher. That is, employers are already on the hook for increased unemployment insurance taxes for each successful claimant, so the added loss of non-compete protection may cause them to oppose claims more often and with more intensity. This will lead to more backlogs in the unemployment office, and more time, effort, and expense for the office, employer, and employee.

Please also see [Ken Vanko's excellent post](#) on the proposed legislation.

In the end, though SB 51 at first blush may seem like a good idea, in practice it may have little if any effect. Worse, it may backfire. We will keep our eye on how the bill moves through the Maryland legislature.

# Trading Secrets



## California Appellate Decision Clarifies Standard for Injunctive Relief Carve-Outs Within California Arbitration Agreements

*By Robert Milligan and Grace Chuchla (January 22, 2013)*

Arbitration agreements with carve-outs for provisional remedies are again the topic du jour, particularly in California courts which apply a stringent unconscionability analysis to employee arbitration agreements.

As we previously [discussed](#) on this blog, in October 2012, a federal district court for the Eastern District of California upheld an arbitration agreement even though it excluded suits seeking injunctive relief for unfair competition and/or disclosure of trade secrets (*Steele, et. al v. American Mortgage Solutions d/b/a Pinnacle*, 2012 WL 5349511 (E.D. Cal., Oct. 26, 2012)). In doing so, the district court [made clear](#) that such carve-outs for trade secret protection do not necessarily inspire the same level of suspicion that other types of exclusions do. As the district court saw it, Pinnacle had “valid reasons, entirely independent from any intent to place the employees at a relative disadvantage or to generate one sided results, for excluding claims of unfair competition or trade secret violations from the mandatory arbitration agreement provisions of the Agreement.”



Such common sense reasoning regarding the relationship between arbitration agreements and provisional remedies has now also found a voice in the California Court of Appeals. Specifically, in [its December 20, 2012 decision](#) in *Maribel Baltazar v. Forever 21, Inc.*, the Court of Appeal for Second District, Division One, upheld an arbitration agreement despite plaintiff's claims that the agreement's incorporation of California Code of Civil Procedure Section 1281.8 rendered it substantively unconscionable.

Following Baltazar's complaint filed in California state court asserting nine causes of action under both the FEHA and the Ralph Civil Rights Act of 1976, Forever 21 filed a Motion to Compel Arbitration in September 2011. After hearing arguments from both sides, the trial court sided with the plaintiff, finding that the agreement was unconscionable because it: 1) required arbitration of only claims likely to be brought by the employer; 2) gave Forever 21 the right to take “all necessary steps” to protect its confidential or trade secret information; and 3) mandated arbitration even if the agreement was found unenforceable.

Forever 21 appealed, and the Court of Appeal began its analysis of the arbitration agreement by first clarifying that the California Arbitration Act (“CAA”), rather than the Federal Arbitration Act (“FAA”), governed. The agreement was silent on this matter, and although plaintiff claimed that the FAA should prevail unless the parties expressly “opted out,” the lack of any evidence of interstate commerce led the Court to hold that the CAA governed.





# Trading Secrets



Looking next at procedural and substantive unconscionability, the Court easily found the agreement to be procedurally unconscionable, for Baltazar was forced to sign it as a condition to employment. Substantive unconscionability, however, inspired a much lengthier discussion, as the Court addressed individually each of the four areas of the arbitration agreement that the plaintiff claimed to be substantively unconscionable.

**1) Unilateral arbitration** – Citing to a list in the agreement of disputes that must be arbitrated, Baltazar argued that the agreement was set up to force only claims brought by employees into arbitration. However, despite the fact that this list did consist of claims that employees would most likely bring against their employer, the Court recognized that adjacent language in the agreement destroyed plaintiff's argument. Specifically, the fact that the list was prefaced by the phrase "include but are not limited to" and the fact that the paragraph immediately following stated that "each of the parties voluntarily and irrevocably waives any and all rights to have any Dispute heard or resolved in any forum other than through arbitration" led the Court to recognize that the agreement was bilateral, rather than unilateral.

**2) Availability of provisional relief** – This analysis was the core of the Court's ruling. Plaintiff's argument rested on the claim that the agreement's specific incorporation of California Code of Civil Procedure Section 1281.8 rendered it unconscionable.

In relevant part, section 1281.8 states that:

"A party to an arbitration agreement may file in the court in the county in which an arbitration proceeding is pending, or if an arbitration proceeding has not commenced, in any proper court, an application for a provisional remedy in connection with an arbitrable controversy, but only upon the ground that the award to which the applicant may be entitled may be rendered ineffectual without provisional relief."

While many non-California attorneys may be puzzled as to why plaintiff's argument was not patently frivolous, we are in California after all.

The relationship between section 1281.8 and arbitration agreements had previously been examined by the court of appeals in *Trivedi v. Curexo Technology Corp.*, 189 Cal. App. 4th 387. In this case, the court found a carve-out for provisional remedies within an arbitration agreement to be unconscionable even though it also recognized that the language in the agreement was coextensive with section 1281.8. The Court in Baltazar thankfully took issue with this contradictory logic for three reasons.

First, the cases that the Court of Appeal relied on in *Trivedi* (*Mercuro v. Superior Court*, 96 Cal. App. 4th 174, and *Fitz v. NCR Corp.*, 118 Cal. App. 4th 172) "do not suggest that the incorporation of section 1281.8 is unconscionable." Rather, *Mercuro* and *Fitz* dealt with carve-outs in arbitration agreements that were cherry picked by the employer and were clearly unilateral. Second, the Court could not "say that Forever 21 is more likely to seek injunctive relief than an employee." As the Court astutely pointed out, seven of Baltazar's nine claims were brought under statutes that allow her to seek injunctive relief. Finally, the Court made the common sense observation that, because the agreement is subject to the CAA, not the FAA, "section 1281.8 would apply even if it were not expressly mentioned in the agreement."

"[B]ecause the Agreement is subject to the CAA, not the FAA, [CCP] section 1281.8 would apply even if it were not expressly mentioned in the Agreement. Put another way, an arbitration agreement



# Trading Secrets



governed by the CAA permits a party to seek provisional remedies, such as injunctive relief, in court regardless of whether section 1281.8 is mentioned in the agreement.”

Expressly incorporating what would otherwise be automatically read into the agreement cannot create substantive unconscionability. In other words, expressly referencing procedural mechanisms in your arbitration agreement permitted under California state law is not unconscionable!!!!

3) **Forever 21’s Protected Information** – Plaintiff also took issue with the provision of the agreement which stated that, during arbitration, “all necessary steps” would be taken to protect Forever 21’s trade secret and confidential information as unconscionable. The Court held otherwise, finding that this provision was sufficiently narrow and consistent with both the Uniform Trade Secrets Act and general confidentiality and non-disclosure agreements.

4) **Arbitration Notwithstanding the Agreement’s Unenforceability** – Within the arbitration agreement, there is a section which states that arbitration will be conducted pursuant to the rules of the American Arbitration Association (“AAA”) or the rules of the CAA if the AAA rules are found to be unenforceable. Plaintiff claimed that this section has the effect of continuing to force arbitration even if the agreement is declared unenforceable. However, such an interpretation is, according to the Court, “without merit.” As the Court recognized, this section of the agreement “refers only to the invalidation of AAA rules, not the validity of the Agreement” (*italics in original*). There is nothing unconscionable about providing an alternate forum in the unlikely event that the AAA rules are declared unfair.

In sum, the Court’s ruling in *Baltazar v. Forever 21* is a refreshing moment of cogent common sense analysis much like what we saw from the district court in *Steele v. Pinnacle*. Not only did the Court pay no heed to Plaintiff’s selective reading of her arbitration agreement, but it also undertook a careful analysis of existing case law and declined to follow the contradictory logic of *Trivedi*. For employers looking to shore up their arbitration agreements governed by the CAA, this decision suggests that, as long as an agreement’s carve-outs for the provisional remedies stem directly from the language of section 1281.8, the agreement will be enforceable. Remember, however, that this decision is not *carte blanche* to start excluding a variety of claims from arbitration agreements at least under agreements governed by the CAA. *Mercuro* and *Fitz* are apparently still good law pending determination of whether the U.S. Supreme Court’s decision in *Concepcion* renders the unconscionability analysis moot, and the Court’s decision here rests in large part on the fact that section 1281.8 would be incorporated into Forever 21 arbitration agreement even without specific mention in the agreement. That said, despite the Court’s narrowly tailored ruling, there is no denying that *Baltazar* brings some clarity for employers looking to both enforce their arbitration agreements and protect their trade secrets while doing business in the great state of California.

# Trading Secrets



## Massachusetts Legislators Introduce “Noncompete Agreement Duration Act”

*By Erik Weibust and Ryan Malloy (January 29th, 2013)*

Massachusetts has entered a new chapter in a long-standing effort to enact comprehensive non-compete reform in the Commonwealth. Recall from these [previous posts](#) that Senator Will Brownsberger and Representative Lori Ehrlich each introduced competing non-compete legislation in 2008 — Brownsberger’s would have gone the way of California and a few other states and banned all non-compete agreements, whereas Ehrlich’s would have been far less restrictive. In the spring of 2009, the legislators collaborated on a compromise bill, Massachusetts House Bill 2293, entitled “An Act Relative to Noncompetition Agreements.” House Bill 2293 aimed to codify existing common law while affording greater procedural protections to those subject to contractual restrictions on employment mobility. After several revisions, House Bill 2293 ultimately failed to pass.



This session, however, Representatives Brownsberger and Ehrlich have taken a simplified approach with the introduction of a new bill that focuses exclusively on the duration of non-compete agreements in the employer-employee context. The proposed bill, entitled the “Noncompete Agreement Duration Act,” is based on the following findings:

- “[T]he Commonwealth of Massachusetts has a significant interest in its economic competitiveness and the protection of its employers, and a strong public policy favoring the mobility of its workforce” and
- “[T]he Commonwealth of Massachusetts has determined that an employee noncompetition agreement restricting an employee’s mobility for longer than six months is a restraint on trade and harms the economy.”

The proposed bill leaves intact much of the existing common law, but creates a presumption that a non-compete agreement of up to six months is reasonable, whereas a non-compete agreement that lasts longer than six months is unreasonable, with three exceptions: (i) “the employee has breached his or her fiduciary duty to the employer;” (ii) “the employee has unlawfully taken, physically or electronically, property belonging to the employer;” or (iii) “the employee has, at any time, received annualized taxable compensation from the employer of \$250,000 or more.” If a court determines that the duration of the non-compete agreement is unreasonable and one of the exceptions does not apply, however, the non-compete agreement will be unenforceable in its entirety. This represents a big departure from existing Massachusetts law, which permits the court to reform an unenforceable agreement to make it enforceable.

Like House Bill 2293, the Noncompete Agreement Duration Act does not impact non-disclosure agreements, non-solicitation agreements, non-competes in connection with the sale of a business, non-competes outside of the employment context, forfeiture agreements, or existing trade secrets law.

We will continue to monitor the progress of this legislation and will provide updates when appropriate.

# Trading Secrets



## Federal Trade Commission Removes Bleach Companies' Non-Compete Agreement

*By Jessica Mendelson (January 30th, 2013)*

The Federal Trade Commission ("FTC") [recently put an end](#) to a non-compete agreement between two bleach companies that allegedly drastically reduced competition in the American South. Oltrin Solutions, LLC and JCI Jones Chemicals Inc., were competitors in the market for bulk bleach, which is used primarily as a disinfectant in municipal water treatment. Oltrin is a joint venture between Trinity Manufacturing and Olin Corporation, the largest bleach producer in North America. JCI is one of the world's leading producers and distributors of various water treatment chemicals, including bleach.

According to the original [complaint](#), in March 2010, Oltrin agreed to pay JCI a sum of \$5.5 million over the course of four years. In exchange, JCI agreed to provide Oltrin with a list of their bulk bleach customers, and agreed not to sell bulk bleach in either North or South Carolina for a period of six years.

Bulk bleach is typically sold in quantities of 4500-4800 gallons, an amount large enough that it limits the ease of transport. Because of these transportation difficulties, the FTC defined the relevant geographic markets as the area within 300 miles of JCI's former bleach production plant. Essentially, this area includes North and South Carolina and southern Virginia. According to the FTC, the agreement between Oltrin and JCI eliminated competition between the two companies "in the relevant geographic market; substantially increased the market concentration for bulk bleach sales in the relevant geographic market; and increased Oltrin's ability to raise bulk bleach prices."

Based on the terms of a proposed consent order, which was unanimously approved by the FTC, Oltrin will be required to release JCI from the non-compete agreement, and to transfer some of its bulk bleach contracts back to JCI. Additionally, Oltrin must provide JCI with a short-term backup supply agreement in order to assist JCI with its reentry back into the market. Additionally, Oltrin and JCI are both required to notify the FTC prior to entering into any agreements in the bulk bleach market. Oltrin is also required to notify any customer who has placed a bid after 2010 that JCI is in the bulk bleach business in this market again. The consent order is subject to public comment until February 21, 2013, at which point the FTC will choose whether the order becomes final.

In light of the Department of Justice's [recent activity](#) in the high-tech sector concerning no-hire agreements and the FTC's activities from [In the Matter of Renown Health](#), which we previously [blogged](#) about, companies should be cognizant of the effect of their market share/the use of non-compete agreements in particular markets and the possibility of government regulatory activity regardless of whether the jurisdiction permits non-compete agreements.



# Trading Secrets



## California Federal Court Ships Fiduciary Duty and Unfair Competition Suit to Delaware Based Upon Forum Selection Clause

*By Robert Milligan and Grace Chuchla (January 31st, 2013)*

Using a forum selection clause to transfer a case out of California federal court may have become easier thanks to a recent order from Judge Koh of the United States District Court for the Northern District of California. In her [order](#), Judge Koh granted defendants' motion to transfer plaintiff's complaint to Delaware federal court, finding that the forum selection clauses contained in two agreements were both broadly applicable to tort and statutory claims and enforceable despite allegations that enforcing them would violate California public policy, e.g. the inclusion of an alleged unenforceable jury trial waiver. [AJZN, Inc. v. Donald Yu, et al.](#), Case No. 5:12-cv-03348-LHK, (N.D. Cal.)



The agreements and forum selection clauses in question came to be when plaintiff sold all of its assets to one of the defendants in exchange for a warrant giving plaintiff the option to purchase a stake in one of the defendants and that defendant's assumption of plaintiff's debt. This transaction was accomplished via an Asset Purchase Agreement and a Warrant Agreement, both of which contained jury trial waivers and forum selection clauses stating that suits arising under the agreements must be filed in Delaware.

Following the transaction, the relationship between the parties took a turn for the worse, and on July 3, 2012, the plaintiff filed suit alleging eight causes of action under both federal and California law related to misrepresentations in the Warrant Agreement and in the defendants' actions, including claims for breach of fiduciary duty and unfair competition.

Defendants responded with a motion to dismiss or transfer based on the forum selection clauses in both the Asset Purchase Agreement and the Warrant Agreement. In its opposition, plaintiff argued that the claims it brought were not covered by the forum selection clauses and that the clauses were unenforceable due to their inclusion of a jury trial waiver. Judge Koh disagreed with plaintiff and struck down each of its arguments in turn. The Court found that federal law, not California law, controlled the question of the enforceability of the forum selection clauses and that the plaintiff had the burden of establishing the lawful basis to set aside the clauses.

First and foremost, Judge Koh refuted plaintiff's assertion of inapplicability by approving of the broad wording of the forum selection clauses. The text of these clauses reads:

"The parties agree that all actions or proceedings relating to this Agreement (**whether to enforce a right or obligation or obtain a remedy or otherwise**) will be brought solely in the state or federal courts located in or for Wilmington, Delaware." (emphasis added)





# Trading Secrets



As Judge Koh saw it, these clauses “do not require that claims seek to enforce the agreements, or seek remedies under the agreements.” Rather, they “require only that claims relate to, or are based on matter in connection with, the agreements.” Using this broad interpretation of the forum selection clause, Judge Koh easily held that plaintiff’s claims fall within the scope of the clause.

Plaintiff’s second argument — that the forum selection clauses should be struck down because of their inclusion of a jury trial waiver — met with a similar fate. Although Judge Koh recognized that jury trial waivers may be unenforceable in California, she did not view the forum selection clause as a contravention of California public policy. In its briefings, plaintiff did “not presen[t] any reason why a Delaware federal court could not protect [its] interests as well as a California court could.” Based on this lack of a concrete threat, Judge Koh was not ready to speculate about how a Delaware court would handle this case. Perhaps it would apply California law. Perhaps it would apply “some other law that would be equally protective of the interests of California citizens.” The answer was unclear, and therefore plaintiff did not meet its burden of proving that enforcing the forum selection clauses would contravene California public policy.

Coming on the heels of cases such as [Hartstein v. Rembrandt](#) and [Hegwer v. American Hearing and Associates](#) — both of which also came from the Northern District and enforced forum selection clauses despite claims of violation of California public policy, i.e. Business and Professions Code section 16600 – *AJZN v. Yu* is yet another example of how California federal courts are generally willing to enforce forum selection clauses, absent a strong showing that enforcement would be unreasonable or unjust. Notable here is Judge Koh’s insistence that plaintiff concretely demonstrate that transferring this case to a Delaware court would contravene California public policy. As Judge Koh stated at the end of her analysis:

“A mere unspecified ‘risk’ that a court could, in theory, enforce the waiver...cannot carry AJZN’s heavy burden to establish that ‘enforcement of the clause *would* contravene a strong public policy’ of California.” (citing to *Argueta v. Banco Mexicano, S.A.*, 87 F.3d 320, 324 (9th Cir. 1996), emphasis in original).

Although it remains to be seen how concrete of a “risk” California federal judges will demand from plaintiffs in the future, Judge Koh has provided further authority for courts to demand that plaintiffs all but predict the future if they want to have a forum selection clause declared unenforceable because it contravenes California public policy. Because we cannot predict the future (try as we might!), only time will tell how this dispute over the enforceability and applicability of forum selection clauses will play out in California. Expect the continued use of aggressive use of forum selection and choice of law provisions to attempt to secure a more favorable forum for future disputes.

Delaware is typically viewed as business friendly as sophisticated parties attempt to avail themselves of Delaware courts through mandatory forum selection, choice of law, and consent to jurisdiction provisions. Delaware also has a favorable choice of law/venue statute, [6 Del. C. § 2708](#), which provides that parties to [certain contracts over \\$100,000](#) may use Delaware choice of law provisions in their contracts and that it “shall conclusively be presumed to be a significant, material and reasonable relationship with this State and [the agreement] shall be enforced whether or not there are other relationships with this State.”



# Trading Secrets



## California Federal Court Dismisses California Employee's Challenge Of His Non-Compete Agreement Based Upon Enforceable Forum Selection Provision

*By Robert Milligan and Grace Chuchla (February 12th, 2013)*

California federal courts have again said it loud and clear — when analyzing whether or not the enforcement of a forum selection clause within a non-competition agreement is contrary to California public policy, the court will not consider the substantive effects of enforcing the clause. In a recent case out of the Northern District, [\*Meras Engineering v. CH2O, Inc., Case No. C-11-0389 EMC\*](#), Judge Chen articulated this concept by ruling that the enforcement of the forum selection clause was in no way determinative of which state's law would ultimately be applied. As he reasoned, forum selection and choice of law analyses are not one in the same, or in other words, "the selection of a forum does not always dictate the choice of law."



Clear as Judge Chen's ultimate ruling might have been, the background leading up to this order is a muddled one, involving multiple parties, states, suits, motions, and stays. Events were set in motion on January 26, 2011, when Rich Bernier and Jay Sughrue left their employment with CH2O and went to work for Meras Engineering. Both CH2O and Meras are industrial water purification companies, with their principle places of business in Washington and California, respectively. Bernier and Sughrue signed non-competition agreements with CH2O that contained choice of law and forum selection provisions stating that all suits arising under the agreement would be heard in Thurston County, Washington. Both Bernier and Sughrue worked and lived in California and visited CH2O's Washington office only twice.

On the same day that Bernier and Sughrue left CH2O, they filed suit along with Meras in the Northern District of California seeking declaratory judgment against CH2O to void their non-competes. Six days later, on February 2, 2011, Meras filed suit against Bernier and Sughrue in Washington state court seeking enforcement of the same non-competition agreements. Bernier and Sughrue then successfully removed the Washington case to federal court and moved to dismiss, stay, or transfer the Washington case to the Northern District of California under the first-to-file rule. The Washington federal court denied this motion because of the forum selection clause in the agreements. Following Bernier's and Sughrue's unsuccessful attempts to transfer the Washington case, the Washington court granted two separate stipulated stays, the first of which was lifted on May 23, 2012. The second stay, which was granted because Bernier filed for bankruptcy, was lifted on September 6, 2012, but only with respect to CH2O's claims for injunctive relief.

With the proceedings in Washington stayed until the resolution of Bernier's bankruptcy case, CH2O brought a motion to stay the California case pending the outcome of the Washington case. CH2O based its argument on the fact that Washington courts had already ruled that the choice of law clause



# Trading Secrets



in Bernier's and Sughrue's non-competes was enforceable and therefore Washington law should decide this case. Plaintiffs objected, stating that the California case was more advanced than the Washington case, which meant that the "gravitational pull" of the litigation was toward California, not Washington.

Using the test laid out in *Landis v. North American Company*, 299 U.S. 248, (9th Cir. 1962), Judge Chen pointed out that the simple fact that Meras was not a party to the Washington case was sufficient to show that plaintiffs would suffer "a fair possibility of harm" if the stay in California were granted, as a resolution of the Washington case would directly impact Meras's rights without allowing it to participate in the litigation. This, in conjunction with the fact that CH2O did not successfully show how it would be harmed if the case were to proceed, led Judge Chen to deny CH2O's request for a stay in California.

Judge Chen then moved on to the forum selection clause in Bernier's and Sughrue's non-competition agreements. Nowhere in its motion to stay did CH2O raise this issue; however, it was an element of Plaintiffs' motion for summary judgment, which Judge Chen also ruled on in this order. After resolving the question of whether or not CH2O had waived the issue of venue through its conduct, Judge Chen rejected Plaintiffs' claim that the enforcement of the forum selection would violate California public policy. The basis of Plaintiffs' argument was that the enforcement of the forum selection clause would lead to the application of Washington law, which, because Washington allows for certain non-competition agreements, would create a result that is contrary to California public policy. Judge Chen took issue with this three-part chain of events and Plaintiffs' conflation of enforcing a forum selection clause and deciding what law applies. Forum selection and choice of law are two very distinct questions. There is nothing in the forum selection clause that "dictate[s] *a priori*" that Washington law would apply, and simply having a case heard in a different forum is not contrary to California public policy. Therefore, by severing the tie between where the case is heard and what law will apply, Judge Chen reasoned that the forum selection clause in Bernier's and Sughrue's non-competes was enforceable and valid and that their case should be dismissed.

This order reaffirms the recent trend out of California federal courts when it comes to forum selection clauses in non-competition agreements. Just as Northern District judges did in [Hartstein v. Rembrandt](#) (2012 WL 3075084, N.D. Cal., July 30, 2012) and [AJZN v. Yu](#) (2013 WL 97916, N.D. Cal., January 07, 2013), Judge Chen refused to look beyond the procedural effects of the forum selection clause and into its substantive ramifications. As this string of cases has made clear, the "contrary to California public policy" element of the *Bremen* test extends only as far as ensuring that all parties have their procedural rights protected at the same level that they would California (*M/S Bremen v. Zapata Off-Shore Co.*, 407 US 1). Anything that delves into the substance of the transferee court's handling of a California case — such as that court's choice of what substantive law should apply — is beyond the scope of what California federal courts will consider when ruling on the enforceability of a forum selection clause.

That said, this order is by no means carte blanche for defendants looking to enforce forum selection clauses and other courts may disagree with the analysis. As Judge Chen is careful to point out, there are "some situations where a forum selection clause may have the effect of selecting the substantive law to be applied." In these scenarios, forum selection clauses are not enforceable, but this of course leaves the door open for interpretation as to how exactly a court will define these "situations." Judge Chen does provide some clarification when he explains that forum selection is appropriate as long as it does not "preordain" the choice of law, but again, at what point can one say that the result of a suit are preordained? The answers to these questions are uncertain, but one can be sure that this recent string of cases out of the Northern District of California has bolstered the power of forum selection clauses while also defined a standard to be used when deciding whether or not to enforce such provisions when non-competition agreements are at issue in the suit.

# Trading Secrets



## New York Federal Court Denies Injunction to Enforce Restrictive Covenants Against Terminated Employee

*By Paul Freehling (February 13th, 2013)*

Garrod, a salesman for more than 25 years in the field of elastomeric precision products (EPP), was terminated in mid-2012 after spending an aggregate of a dozen of those years working for manufacturers of EPP parts Fenner and a company acquired by Fenner.

He had signed both employers' agreements containing non-compete and customer non-solicitation clauses—which appeared reasonable on their face—and Pennsylvania choice-of-law provisions. After Fenner discharged him, he was hired by Mearthane, another EPP company. When he began calling on Fenner's customers, Fenner sued Mearthane and him in the U.S. District Court for the Western District of New York, seeking to enforce the restrictive covenants contained within the employment agreements.



Earlier this month, Fenner's motion for a preliminary injunction was denied largely because the court found the non-compete and non-solicitation clauses to be unreasonable. According to the court, Pennsylvania law "disfavors enforcement of restrictive covenants against employees who are fired for poor performance" since the employer views those employees as "worthless." [\*Fenner Precision, Inc. v. Mearthane Products Corp.\*, Case No. 12-CV-6610 CJS \(W.D.N.Y., Feb. 4, 2013\)](#).

Garrod asserted that the agreements lack consideration, and that Fenner had not made a sufficient showing of irreparable harm, but the court rejected those assertions. He was more successful with his argument that the agreements are not enforceable because they are unreasonable. He pointed out that he is 58 years old, reducing the likelihood that he can obtain employment outside the EPP industry, and that Fenner gave no reason for his termination. He emphasized that he had worked in the EPP industry for more years before joining Fenner's predecessor than he spent with that company and Fenner, and that he had significant contacts with, and knowledge about, EPP manufacturers before he became their employee.

The court concluded that Fenner's concerns about Garrod's ability to harm its sales "seem overstated in light of the fact that he yet to close any sales since commencing work for Mearthane." Moreover, those concerns "are belied" by Fenner having "removed him from the company's most profitable accounts" before firing him. In sum, "Considering all the relevant factors in the record, and weighing the parties' competing interests," the court found that "Garrod is likely to prevail in demonstrating that enforcement of the non-solicitation clause against him would not be reasonable."

This case reminds us that employers can face an uphill battle in enforcing a non-compete clause against a terminated employee. However, there are courts that enforce such contracts as written regardless of the reason the employee left his or her prior employment.

# Trading Secrets



## Federal Court Requires Foreign Resident To Litigate Non-Compete Dispute in Missouri Based Upon Forum Selection Clause

*By Robert Milligan and Grace Chuchla (February 26th, 2013)*

It's 8,242.7 miles or a 17 hour flight between the Philippines and Missouri. Nobody would dispute that this is a significant distance, but as far the Eastern District of Missouri is concerned, forcing a defendant who lives in the Philippines to participate in litigation occurring in Missouri does not constitute an unfair or unreasonable burden. [\*Emerson Electric Co. v. Yeo\*](#), Case No. 4:12CV1578 JAR (E.D.M.O. 12/28/2012).



On August 30, 2012, Emerson Electric sued Peter Ramos Yeo, a former employee of its subsidiary Astec International, Ltd., in St. Louis County Circuit Court for violating the non-compete clause that was included with a Stock Option Agreement that Yeo signed in 2011. The case was removed to federal court, at which point Yeo brought a Motion to Dismiss for Failure to State a Claim and Lack of Personal Jurisdiction. Yeo's sought to invalidate his non-compete on three fronts – 1) that the Stock Option Agreement containing the non-compete was an illusory promise, 2) that the non-compete was unenforceable due to lack of adequate consideration, and 3) that the forum selection clause within the non-compete was unenforceable.

In support of his first and second claim, Yeo argued that, under his Stock Option Agreement, Emerson retained the right to terminate him at any time. Therefore, because his stock options did not vest for one year, Emerson had the ability to relieve itself of its promises, rendering the stock option grant illusory and the agreement unenforceable. Additionally, Yeo argued that, even if the agreement were not illusory, Emerson's agreement to buy back his stock upon termination was not sufficient consideration to support the non-compete clause that the agreement contained.

Judge Ross rejected both of these arguments, noting that, in certain circumstances, Yeo did in fact have the right to exercise his options before they vest. The court also distinguished Yeo's situation from the facts of *Sturgis Equipment Co., Inc. v. Falcon Industrial Sales Co.*, 930 S.W.2d 14 (Mo.Ct.App. 1996), where the Missouri Court of Appeals held that an agreement to buy back stock was insufficient consideration to support a non-compete clause. Unlike *Sturgis*, where the agreement dealt solely with stock options, Yeo's agreement contained language regarding the protection of Emerson's confidential information. Thus, Yeo's "stock options were granted to [him] in consideration of his position with Emerson and in recognition of his role as a key employee," which "constitutes sufficient consideration to support the non-compete clause."

Finally, Yeo sought to invalidate the forum selection clause of his non-compete by arguing that he currently resides in the Philippines, has minimal contact with Missouri, and would face a huge burden if he were forced to litigate in a court over 8,000 miles away. Despite these geographic realities, Judge Ross did not find Yeo's argument convincing. A 17 hour plane ride apparently does not meet the



# Trading Secrets



standard of “so gravely inconvenient that he will for all practical purposes be deprived his day in court.” See *Servewell Plumbing LLC v. Federal Ins. Co.*, 439 F.3d 786 (8th Cir. 2006). That said, geography was not the only factor in the court’s decision. Judge Ross also pointed out that, as “an educated person,” Yeo is “presumed to have agreed to the forum selection clause knowingly and intelligently.” Thus, there is nothing unjust about “hold[ing] him to his bargain” and making Yeo defend himself in a Missouri court.

This order is notable for just how strictly it enforces Yeo’s forum selection clause. There is no denying that the geographic realities of this case suggest that Missouri federal courts are ready and willing to enforce even the most logistically challenging forum selection clauses. Add this decision to cases such as *MB Restaurants, Inc. v. CKE Restaurants, Inc.*, (enforcing a forum selection clause despite plaintiff’s objections about the expense, 183 F.3d 750 (8th Cir. 1999)) and *Afram Carriers, Inc. v. Moeyskens* (enforcing a Peruvian forum selection clause against a destitute family, 145 F.3d 298 (5th Cir. 1998)) — both of which were cited by Judge Ross in his order — and one has to question if there are *any* situations that a Missouri federal court would deem “gravely inconvenient” when it comes to enforcing forum selection clauses. But speculation aside, there is no question that this order bodes well for Missouri employers looking to avoid both the difficulty of litigating in a variety of forums and the possibility of having to bring suit in courts that are unfriendly toward non-compete agreements. Please also see [our previous post](#) on a California federal court’s decision finding personal jurisdiction over an Irish company in a business dispute, involving a non-disclosure agreement.



# Trading Secrets



## California Style Non-Compete Legislation Introduced In Minnesota

*By Justin Beyer (March 14th, 2013)*

New proposed legislation introduced in the Minnesota House of Representatives would invalidate effectively all employee non-compete agreements if passed.

On February 11, 2013, Democratic-Farmer-Labor party members Joe Atkins and Alice Hausman introduced H.F. No. 506. The bill was read and referred to the Committee on Labor, Workplace and Regulated Industries, a committee chaired by Rep. Sheldon Johnson (DFL-St. Paul). The proposed legislation—which essentially tracks California Business and Professions Code sections 16600 through 16602.5—would invalidate all non-compete agreements between an employer and its employees. No current statute specifically addresses treatment of non-compete agreements in Minnesota.

Neither Rep. Atkins nor Hausman appear to have sponsored similar legislation in the more recent legislative regular sessions.



Nonetheless, while Minnesota's governorship and legislature are currently controlled by the DFL (by an 11-vote margin in the Senate and a 12-vote margin in the House), it appears unlikely that this legislation will become Minnesota law, at least in 2013. This is likely given the strong push that Gov. Mark Dayton has made toward jobs creation and business attraction during his first two years in office. Furthermore, no hearings have been scheduled regarding this bill yet.

The full text of the proposed bill reads:

### Section 1 [325D.72] Noncompete Agreements Void.

A contract that prohibits a party to that contract from exercising a lawful profession, trade, or business is void with the following exceptions:

- (1) a seller of a business' goodwill can agree to refrain from carrying on a similar business in a specified county, city, or party of one of them if the buyer carries on a like business in that area;
- (2) partners dissolving a partnership can agree that one or more of them will not carry on a similar business in a specified county, city, or part of one of them where the partnership transacted business; and
- (3) a member, when dissolving or terminating their interest in a limited liability company, can agree that the member will not carry on a similar business in a specified county, city, or part of one of them where the business has been transacted if another member or someone taking title to the business carries on a like business in that area.





# Trading Secrets



**Effective Date.** This section is effective the day following final enactment.

Minnesota businesses and out-of-state businesses who employ Minnesota employees must be mindful of the potentially chilling consequences if this legislation becomes law.

Like California Business and Professions Code section 16600, enactment of a similar statute in Minnesota would have potentially devastating consequences on Minnesota employers who have utilized non-compete agreements as a means to protect their business interests. For example, in California, the California Supreme Court has interpreted section 16600 to invalidate any contract that restrains anyone from engaging in a lawful profession, trade, or business of any kind, which it deemed to include any non-compete or customer non-solicitation restrictions. *Edwards v. Arthur Anderson LLP*, 44 Cal 4th 937 (2008).

Unlike California, Minnesota has not historically treated noncompetition agreements with the sort of disdain that California has. Indeed, Minnesota courts have routinely upheld narrowly tailored restrictive covenants, including non-compete, customer non-solicitation, and anti-raiding provisions. The proposed legislation would be bad for Minnesota businesses and would also place Minnesota outside the mainstream of current United States non-compete law. While this legislation is not likely to be adopted in 2013 (hopefully), Minnesota businesses or businesses that employ Minnesota employees should continue to closely monitor this situation.

# Trading Secrets



## Massachusetts Governor Weighs In On Non-Compete Reform Debate

*By Ryan Malloy (March 14th, 2013)*

At the annual meeting of the Massachusetts Technology Leadership Council on March 12, Massachusetts Governor Deval Patrick [reportedly](#) described arguments in favor of eliminating the state's longstanding approval of non-compete clauses as "compelling," while stopping short of endorsing those efforts.

During a question-and-answer session at the conference, Branko Gerovac, chief strategy officer at search engine optimization startup Jungle Torch, [reportedly](#) expressed concern that non-compete agreements cause businesses to leave for other states, particularly California, which prohibits them. "The Boston area is falling behind," he reportedly said, and the reason is that non-compete clauses decrease the available workforce for high-tech jobs.



Governor Patrick [reportedly](#) said that the state's strong technology sector has been critical in allowing Massachusetts to regain the total number of jobs lost during the recession, and he agrees that broad non-compete agreements restrain jobs. He also reportedly noted that "there are a handful of tech sector people on the other side" of the debate. He also reportedly [said](#), "I am not practicing law anymore but I have some serious doubts as a lawyer whether a [sic] non-compete is even enforceable in Massachusetts."

In January, Sen. Will Brownsberger and Rep. Lori Ehrlich [proposed legislation](#) to limit non-compete agreements. Under the bill, H1715, any agreement that lasts longer than six months would be "presumed unreasonable" and unenforceable in Massachusetts. H1715 is still awaiting a date for a hearing before the Labor and Workforce Development Committee. We will keep you posted on any further material developments in the debate.

# Trading Secrets



## Illinois Legislator Proposes Unique Employment Noncompete Agreement Act

*By Paul Freehling (March 19th, 2013)*

Rep. Thomas Morrison, a Republican member of the Democratic-controlled Illinois General Assembly, has introduced HB 2782 (98th G.A.) – the “[Employment Noncompete Agreement Act](#).” The bill would create a new Illinois statute, not simply an amendment to an existing one, that differs markedly from every current state non-compete statute. Rep. Morrison introduced the identical bill in the previous session of the General Assembly (HB 5570, 97th G.A.), but it never passed out of committee.



### **Controversial provisions**

Apart from the question of whether the Illinois General Assembly would agree that legislation of any sort on the subject is needed, the specific provisions of HB 2782 that are likely to generate the most controversy are those:

- asserting that employers have a legitimate commercial interest in being protected against competition and solicitation by former employees,
- providing a formula that ties the maximum duration of permissible post-employment covenants to the annualized compensation of the ex-employee on the date of termination, and
- mandating, if litigation between the former employer and the ex-employee proceeds all the way to verdict, a shift to the losing party (plaintiff or defendant) of the burden of paying the prevailing party's damages, attorneys' fees, and expenses.

### **Analysis and Insight**

The bill begins by proclaiming that “all employers have vested, protectable interests in their customers, clients, and identified prospects which are legitimately protectable through the use of noncompete agreements.” In Illinois, the principle that reasonable restrictions applicable to employees' post-employment are enforceable is well-established by case law. So, it is not apparent why Rep. Morrison believes that Illinois needs to have non-compete and non-solicitation covenants expressly authorized by statute in Illinois (to be sure, a few states other than Illinois have laws providing that such covenants are unenforceable altogether or are disfavored).

In one section, Rep. Morrison's bill states that the maximum “duration of a post-employment restriction period must have a reasonable relationship to an employee's position and salary at the time of termination.” However, there is no mention of an employee's “position” in the section setting allowable time limits for enforceable restrictions. Rather, presumably based on an assumption that the larger an employee's annualized compensation, the longer the period during which the former employer needs



# Trading Secrets



protection, the proposed statute ties the permissible length solely to the ex-employee's final earnings. Thus, a restriction may not exceed:

1. six (6) months for an employee earning less than \$50,000,
2. nine (9) months for those making \$50,000-\$99,999,
3. twelve (12) months if compensation is \$100,000-\$149,999, and
4. eighteen (18) months for an employee being paid \$150,000 or more.

These limitations apparently would not be applicable to independent contractors, since they are not employees, but would apply to employees even in the instance of the purchase of a company or its assets, or the dissolution of a partnership. No state statute contains any comparable provisions.

HB 2782 would require courts to award to the prevailing party – whether that party is the former employer or the ex-employee – in litigation seeking to enforce a non-competition agreement “damages, costs and expenses, and reasonable attorney’s fees.” This, too, would be unique; the only state statute that’s even close mandates an award of fees and costs to an ex-employee who prevails, but the law is silent with respect to a prevailing former employer.

Rep. Morrison’s bill may be unlikely to garner the necessary votes, especially in its present form, to be enacted and signed into law. Should the bill become law, however, the fee shifting provision would give both parties a strong incentive to settle rather than proceed to judgment. Moreover, in any given case, a court may or may not find the statutory formula for determining the permissible length of a post-termination restriction to be reasonable.

# Trading Secrets



## Protecting Company Information When Employees Bail: California Alternatives to Employee Non-Compete Agreements

*By Robert Milligan, Jessica Mendelson, and Joshua Salinas (March 22nd, 2013)*

How does a California employer prevent its business from walking out the door along with a departing employee? In most jurisdictions, the employer could have the employees sign a non-compete agreement. Not in California.

One of the notorious employment laws that separates California from other states is its [long-standing prohibition of employee non-compete agreements](#). California's strong public policy against non-competes not only affects local employers, but it often complicates efforts of multi-state employers to utilize uniform restrictive covenants—such as non-competes and non-solicitation provisions—with its employees. Here is a brief recap:



"I'm concerned you might bail."

### **Non-Competition Agreements**

**Most States:** Most states enforce agreements where employees agree not to compete with their former employer for a reasonable period after employment, within a reasonable geographical area.

**California:** In California, even narrowly drawn restraints are contractually invalid, unless they fall within the specific statutory exceptions, such as agreements in connection with the sale of a business.

### **Customer non-solicitation provisions**

**California:** California significantly limits the use of customer non-solicitation provisions and will likely prevent enforcement of a contract clause purporting to ban a former employee from soliciting former customers to transfer their business away from the former employer to the employee's new business.

### **Employee non-solicitation provisions**

**California:** The California ban on non-compete agreements can extend to "no hire" agreements between two businesses. While some California courts still enforce non-solicitation of employees provisions, "no hire" agreements are not enforceable.

### **No "blue-penciling"**

**Many States:** Many states permit the modification or "blue-penciling" of overly broad restrictive covenants to make them enforceable.



# Trading Secrets



**California:** California courts typically do not allow “blue-penciling” in the employment context. Instead, they refuse to enforce agreements, even if the parties have agreed to “save” the clause to the extent enforceable.

## **Is there a trade secrets exception?**

Some California courts have stated that certain non-competition clauses are enforceable if they are necessary to protect trade secrets, while others have cast doubt on whether a trade secret exception exists. To date, there has not been a detailed analysis of the nature of the trade secrets exception, if any, and what an employer must show to support its application. Caution is thus the watchword in relying on a trade secrets exception. If it turns out there is no genuine trade secret, nonsolicitation clauses are likely to be unenforceable. Plus, the inclusion of such a provision may open up the employer to liability under California’s unfair business practice statute.

Without the backstop of non-compete agreements, **what is the California employer to do** to ensure that its trade secret information is adequately protected?

## **Workplace Solutions**

California employers must be vigilant to ensure that their employees don’t share their valuable information with competitors.

Best practices include:

- Robust confidentiality and invention assignment agreements.
- Effective entrance and exit interview protocols.
- Employee education programs that create a culture of confidentiality whereby employees understand the value of protecting company data.
- Effective trade secret protection measures that take into account new technologies and threats, including cyber threats and social media/cloud computer issues.

Please see our recorded webinar on [Trade Secret Protection Best Practices: Hiring Competitors’ Employees and Protecting the Company When Competitors Hire Yours](#) for more details on how to put your company in the best position.



# Trading Secrets



## New Jersey Legislators Propose Banning Non-Compete Agreements With Employees Who Can Claim Unemployment

*By Robert Milligan and Jessica Mendelson (April 9th, 2013)*

New Jersey state legislators recently proposed [A3970](#), a bill designed to prevent New Jersey businesses from enforcing “non-compete agreements with staffers who can claim unemployment compensation.”

The bill, which is [sponsored by](#) Assembly members Joseph Egan and Peter Barnes, was recently referred to the state’s Assembly Labor Committee. If the bill passes, it would invalidate contracts or agreements “not to compete, not to disclose or not to solicit” in cases where individuals qualify for state unemployment benefits. The changes would not apply to preexisting contracts.

Theoretically, the bill would eliminate obstacles for workers on unemployment to return to work, thus reducing benefit payments and, by extension, unemployment taxes on employers. However, the legislation will likely face opposition from employers who rely upon non-compete agreements to protect legitimate business interests such as trade secrets and confidential information.



Traditionally, New Jersey courts enforce restrictive covenants if they are reasonable in scope and duration. In determining whether a non-compete covenant is reasonable, New Jersey courts use a three-prong test, where an employer must show the restriction is necessary to protect the parties’ legitimate interest, that the restriction does not cause undue hardship for the former employee, and is not against the public interest. Under existing law, impacted employees are already able to apprise New Jersey courts of their unemployment status in opposing the enforcement of non-compete agreements.

If [A3970](#) passes, it will further limit the enforceability of non-compete agreements in New Jersey. The state currently has a 9.3 percent unemployment rate, which has led to increased proposals for legislation pertaining to jobless benefits. Given this high rate of unemployment in New Jersey, the passage of the bill will make it harder for employers to enforce non-compete agreements against former employees.

New Jersey is hardly the first state to consider such a change to its non-compete law. In fact, the Maryland state Senate [considered](#) passing a similar bill earlier this year. We will continue to keep you apprised of significant proposed changes in trade secrets and non-compete law as they emerge.

# Trading Secrets



## New Jersey Appellate Court Affirms No Damages Award Against Individual Defendants In Non-Compete Case

*By Paul Freehling (April 26th, 2013)*

A New Jersey jury decided that two individual defendants violated their non-competition contractual commitments but that they owed no damages. The trial court then denied the former employer's motion to enjoin the individuals from continuing to compete. A few days ago, the State's Appellate Court held that there was a plausible explanation for these several results and affirmed. [Miles Technology, Inc. v. Apex I.T. Group, LLC, Case No. A-3453-11T4 \(NJ App. Court, 4/5/13\).](#)



Former employer's first lawsuit. Yetter, an employee of Miles Technology, signed a contract prohibiting him from providing competitive services to Miles' customers for two years after his employment terminated. Yet, almost immediately after resigning from Miles and acknowledging his obligation not to compete, he went to work for Miles-competitor Apex I.T. Group and began soliciting his former employer's customers. Miles sued Yetter and Apex. The suit was dismissed without prejudice, however, when Apex's counsel wrote Miles' lawyer that Apex had fired Yetter.

Former employer's second lawsuit. Shortly following the dismissal, Apex rehired Yetter and then hired Tavares, another Miles Technology employee who also had signed a non-compete. On behalf of Apex, Yetter and Tavares solicited two of Miles' customers, and Apex obtained an order or two from one while the other moved all of its business to Apex. Miles filed a second lawsuit. Yetter and Tavares were charged with breach of contract, and Apex was accused of intentional interference with (a) non-compete contracts, and (b) prospective economic advantage. Miles sought hundreds of thousands of dollars in compensatory damages, as well as an injunction against the individuals and punitive damages from Apex.

The puzzling result. After a jury trial, Miles prevailed with respect to liability but was awarded nothing from the individual defendants, and just \$70,000 in compensatory damages and \$30,000 in punitive damages from Apex. The defendants appealed the denial of their motion for judgment notwithstanding the verdict, and Miles appealed the denial of its motion for an injunction. The Appellate Court affirmed.

Justifying the jury verdict regarding the ex-employees. According to the court of appeals, "The jury may well have perceived that the gravamen of the harm to Miles here did not stem from the contractual breaches of its employees' restrictive covenants but instead was principally caused by Apex's arguably more venal act of deception in falsely assuring that Tavares would no longer work there." Miles claimed the misconduct of the defendants caused a loss of business aggregating about \$700,000 over six years. The Appellate Court surmised that even though the jury found Yetter and Tavares breached their contractual obligations, the jury may have concluded that the evidence tying the breaches to a specific dollar amount of damages was insufficient.



# Trading Secrets



Explaining the verdict against the new employer. The \$70,000 compensatory damages award against Apex equaled approximately 90% of the lowest one year's alleged loss of revenue from just one of the customers. This was enough, according to the appeals court, to render the award reasonably related to the evidence. With respect to the punitive damages assessed against Apex, "the [trial] judge charged the jury in accordance with [the applicable] legal principles. . . . We see no reason to disturb this result."

Reasons for not enjoining the ex-employees. The question of whether to issue an injunction "is typically a matter of the trial court's discretion," the Appellate Court said, and it found no abuse of discretion. Further, since the two-year non-compete period had expired by the time of the appellate ruling, "there is no longer a justification to impose restrictions on" the individual defendants.

Lessons learned. Conventional wisdom teaches that a plaintiff like Miles Technology often will fare better with respect to a damages award in a jury trial rather than in a bench trial. The jury did sympathize with Miles, ruling in its favor with respect to liability as against all defendants, but for some reason only minimal damages were awarded.

The jury may have returned a compromise verdict, slapping the defendants with findings of liability but not hammering them with a punishing damages award. We'll never know, however, because jurors do not have to explain their rationale; affirmance was not surprising because jury verdicts rarely are reversed on appeal.

If the *Miles Technology* case had been the subject of a bench trial, the judge would have had to disclose precisely how his or her decision was reached. One can only speculate as to whether there would have been an affirmance if (a) that hypothetical bench trial had produced the same verdict as the one actually reached by the jury, (b) the trial judge, in explaining the basis for the verdict, had rationalized it in a manner similar to the way the Appellate Court surmised the jury reached its decision, and (c) the verdict was appealed.

# Trading Secrets



## Non-Compete Legislation Proposed in Connecticut

*By Jessica Mendelson (May 25th, 2013)*

Connecticut has recently proposed non-compete legislation which could dramatically impact restrictions on employee mobility.

The bill, known as “Employer Use of Noncompete Agreements,” is [House Bill 6658](#). The bill recently passed in the Judiciary Committee, and is currently pending before Connecticut’s House of Representatives.

As it is written, the bill is intended to apply to all Connecticut employers. The bill will regulate all non-compete agreements in effect after October 1, 2013, and will be the first of its kind in Connecticut. As of now, requirements for non-compete agreements are based on case law.



The [bill](#) permits the use of non-compete agreements if: “(1) the agreement or covenant is reasonable as to its duration, geographical area, and the type of employment or line of business, and (2) prior to entering into the agreement or covenant, the employer provides the employee a reasonable period of time, of not less than ten business days, to seek legal advice relating to the terms of the agreement or covenant.” The notice provision is similar to the notice requirements in Oregon and New Hampshire.

Unlike the current requirements for non-compete agreements, which can be found in the state’s case law, this new legislation would provide employees with a statutory basis for filing suit against employers who act in violation of the law. The new law would allow for the recovery of both damages and attorney’s fees as follows: “any person who is aggrieved by a violation of this section may bring a civil action in the Superior Court to recover damages, together with court costs and reasonable attorney’s fees. To the extent any such agreement or covenant is found to be unreasonable in any respect, a court may limit the agreement or covenant to render it reasonable in light of the circumstances in which it was entered into and specifically enforce the agreement or covenant as limited.” The proposed legislation permits equitable modification by the court of an overbroad agreement.

Employers should take note of this proposed legislation, as it could have significant implications if it passes. Such a statute may encourage litigation, as employees who are at all successful in challenging their agreement may stand to recover a significant sum.

The [Connecticut Business and Industry Association](#) has pointed out that the legislation may be overly broad. The definition of employee is broad enough that it could potentially include independent contractors. Furthermore, even if an agreement otherwise complies with the laws, an employee could have a cause of action if an employer fails to provide a ten day waiting period.

As [the Connecticut Employment Law blog explains](#), the bill could prove problematic for the courts, as it is not consistent with the case law: courts “use a variety of factors to evaluate the reasonableness of a restrictive covenant including: (1) the length of time the restriction operates, (2) the geographical area



# Trading Secrets



covered, (3) the fairness of the protection afforded the employer, (4) the extent of the restraint on the employee's opportunity to pursue his occupation, and (5) the extent of interference with the public interest. " Here, there is no telling how the courts would interpret the reasonableness standard in the legislation, and whether it would be consistent with current case law. Additionally, as Ken Vanko points out on his [non-compete blog](#), the proposed legislation likely does not apply to confidentiality agreements and it is unclear whether it applies non-solicitation agreements.

Whether the Connecticut bill will pass remains to be seen, as we expect that the Connecticut business community will weigh in. We will continue to keep you apprised of future developments concerning the bill.

# Trading Secrets



## Illinois Appellate Court Partially Reverses Broad Non-Compete Injunction Against Physicians

*By Molly Joyce (May 29th, 2013)*

The First District of the Illinois Appellate Court, in the case of [\*Northwest Podiatry Center, Ltd., et al. v. Ochwat, et al.\*](#), recently found that a trial court improperly enjoined physician-defendants in a few key respects. The decision serves as a reminder of how courts will closely scrutinize restrictive covenants in Illinois.



The case was filed after two longtime physicians affiliated with plaintiff Northwest Podiatry Center, Ltd. (“NPC”) left the practice to form a competing practice. One of the physician-defendants, Dr. Ochwat, worked at NPC for over 20 years and was also a vice-president and a member of NPC’s board of directors. The other physician-defendant, Dr. Halihan, worked at NPC since 2006 and signed a restrictive covenant agreement that contained a non-compete clause (barring competitive practice for 36-months within a five mile radius of NPC); a “privileges” restriction (requiring that he surrender his clinical privileges at any hospital where he currently holds privileges, with no durational limitation); and a non-solicitation restriction (prohibiting him from soliciting business away from NPC for a 36-month period).

Based upon evidence presented at a preliminary injunction hearing, the trial court found that the defendants began soliciting NPC employees and clients before they resigned, misused company assets to set up a competing company and interfered with NPC’s contracts. The trial court entered an injunction that, in part, ordered Dr. Halihan to resign his clinical privileges at certain facilities and prohibited both defendants from treating NPC patients.

The First District of the Illinois Appellate Court partially reversed the injunction. First, it found that the trial court’s order requiring Dr. Halihan to forfeit his privileges was improper. It found that a “privileges” restrictive covenant that provides that a physician, when leaving the employ of a practice, will surrender his clinical privileges at any hospital or treatment center at which the employee holds privileges, is overbroad.

Plaintiff NPC argued that the restrictive covenant was ambiguous because it unintentionally omitted the 36-month temporal restriction that the other provisions contained. Plaintiff further argued that because the provision was ambiguous, the court should consider extrinsic evidence of the parties’ intent. The trial court agreed, concluding that the parties intended the 36-month restriction to apply, but the court ultimately did not follow the 36-month limitation, and instead did not put any durational limitation on the restriction.

The appellate court reversed on this point, finding that just because the other restrictive covenants in the same agreement contain limitations for a 36-month period, that does not mean that the covenant without a temporal restriction is ambiguous. In fact, it is evidence that the parties never intended to include a temporal restriction. The court went on to find that without a durational limitation, requiring Dr. Halihan to permanently resign all clinical privileges was overbroad and not necessary to protect NPC’s legitimate business interests.





# Trading Secrets



Second, the appellate court reversed the injunction to the extent it prohibited the defendant-physicians from treating any current or former patients of NPC's practice. The court noted that a "patient has a right to seek treatment from his or her doctor at the doctor's new place of employment unless that doctor is restrained by contract." Defendant Dr. Ochwat did not have a restrictive covenant with plaintiff, so the appellate court found that restricting him in this fashion was unsupported.

Yet, the appellate court found that even the injunction against Dr. Halihan, who did have a 36-month non-solicitation provision in his contract, was improper. The appellate court recognized that, in Illinois, a court has the power to modify a restrictive covenant to make it narrower. Yet, a court cannot create a provision that was not part of the contract. The court held that the lower court "did not modify an overly broad restriction; rather the court created its own patient restriction where none was contemplated by the parties."

The NPC decision provides us with a few important reminders when it comes to restrictive covenants in Illinois:

- It is not advisable to have a non-compete provision in a contract that does not have a temporal limitation. Don't assume that a court will modify or "blue-pencil" such a provision by looking to other restrictions in the same agreement.
- Don't assume that a court will fashion narrower restrictions than the ones you agreed to in your contract. While many courts have the authority to narrow restrictive covenants in certain instances, they cannot create new covenants never agreed upon by the parties.
- Courts are reluctant to prohibit physicians from treating patients unless there is a valid agreement expressly prohibiting their treatment of their former employer's patients.
- Injunctions can be entered against employees even if their restrictive covenant agreements might not be relevant or enforceable. In this case, the defendants' breaches of fiduciary duty and tortious interference led the trial court to enjoin their ability to contract with an independent practitioner's association, and the appellate court affirmed that part of the ruling.

# Trading Secrets



## New Oklahoma Law Clarifies Enforceability of Non-Solicitation of Employee Covenants

By Daniel Joshua Salinas (May 30th, 2013)

Oklahoma recently passed a new law ([Senate Bill 1031](#)) that clarifies the enforceability of non-solicitation of employee covenants within the state. The new law attempts to resolve uncertainties that may have arisen about such restrictive covenants after the Oklahoma Supreme Court's 2011 decision in [Howard v. Nitro-Life Technologies, LLC](#).

In *Howard*, the Oklahoma Supreme Court found the restrictive covenants in an employee's agreement with his former employer void and unenforceable as against Oklahoma's public policy. Oklahoma is one of the three states that generally prohibit non-competition agreements. (California and North Dakota are the others).



Specifically, the court in *Howard* found the non-solicitation of employees covenant void and unenforceable because it also prohibited the hiring of individuals that might seek employment on their own initiative and absent any solicitation or inducement by past employees. Accordingly, the court held that the **entire** non-solicitation provision was void, which suggested that such anti-raiding provisions may not be enforceable under Oklahoma law.

While the U.S. Supreme Court ultimately [vacated the decision in Howard](#) because of the Oklahoma court's failure to comply with the subject agreement's arbitration provision, uncertainty remained regarding the enforceability of anti-raiding provisions under Oklahoma law.

The new law clarifies that non-solicitation of employee provisions are not unlawful restraints of trade:

"A contract or contractual provision which prohibits an employee or independent contractor of a person or business from soliciting, directly or indirectly, actively or inactively, the employees or independent contractors of that person or business to become employees or independent contractors of another person or business shall not be construed as a restraint from exercising a lawful profession, trade or business of any kind."

It is significant that the text of the statute appears to permit only the non-solicitation of employees or independent contractors and not prohibitions on the hiring or employment of such individuals. This would be consistent with the Oklahoma Supreme Court's analysis in *Howard* where it scrutinized a non-solicitation of employees provision that also prohibited the hiring of employees who may have never actually been solicited. Oklahoma's new law appears to parallel California's hostile non-compete laws, which allow the non-solicitation of employee covenants but generally prohibit no-hire or anti-employment provisions. (See *Loral Corp. v. Moyes*, 174 Cal. App. 3d 268 (1985)).

The new law goes into effect on November 1, 2013.

# Trading Secrets



## Massachusetts Federal District Court Rules That Initiating Contact Not Necessary For Finding of Solicitation In Breach of Customer Non-Solicitation Agreement

*By Erik Weibust and Ryan Malloy (June 4th, 2013)*

An employer can enforce a non-solicitation provision against a former salesman even where the clients initiated contact with the salesman, according to Judge Douglas P. Woodlock of the U.S. District Court for the District of Massachusetts

In [\*Corporate Technologies, Inc. v. Harnett, et al.\*](#), a Massachusetts information technology company, sued its former salesman, Brian Hartnett, for allegedly violating his non-solicitation agreement. In October 2012, after working for CTI for over nine years, Harnett accepted a job offer from OnX Enterprise Solutions (OnX), a competitor of CTI.



On Harnett's first day at his new job, OnX sent an announcement to over 100 potential clients notifying them of Harnett's new position. The list included Harnett's eight most active CTI clients in 2012. Four of the clients responded to OnX's announcement, and Harnett allegedly met with them to discuss and encourage their business on behalf of OnX. One of these discussions ultimately ripened into a client relationship. CTI sued Harnett and OnX in the Massachusetts Superior Court in December 2012, and OnX and Hartnett removed the case to federal court and asserted counterclaims for intentional interference with business relations and unfair business practices. CTI moved for preliminary injunctive relief to enforce the non-solicitation provision.

Notably, Harnett did not dispute that he had been competing with CTI for the business of his former clients, but argued that such dealings did not violate his non-solicitation agreement because it was the clients, and not him, who made first contact. In a 33-page decision, Judge Woodlock explained that it is the nature of the communications, not who initiated them, that determines whether solicitation has occurred, and held that "the Agreement itself provides that Harnett may not 'solicit ... or entice away' CTI's clients, and ***"neither the plain meaning of the word solicit, nor the plain meaning of the word entice, requires some kind of first contact."***

Judge Woodlock was careful to note, however, that a non-solicitation agreement does not prevent a company from receiving business initiated by the client with no direct or indirect participation by the individual employee bound by the non-solicitation agreement. This narrow carve-out does not permit a salesman to actively persuade the client and actually solicit his business. "In this case," however, Judge Woodlock ruled that "Harnett and OnX have done more than simply receive business."

Judge Woodlock granted CTI's request for a preliminary injunction, and enjoined Harnett from soliciting business from those companies within his territory for which he was responsible while employed at CTI. The injunction does not, however, bar OnX as an entity from doing business with those companies, so long as it does not involve Harnett in those efforts.

# Trading Secrets



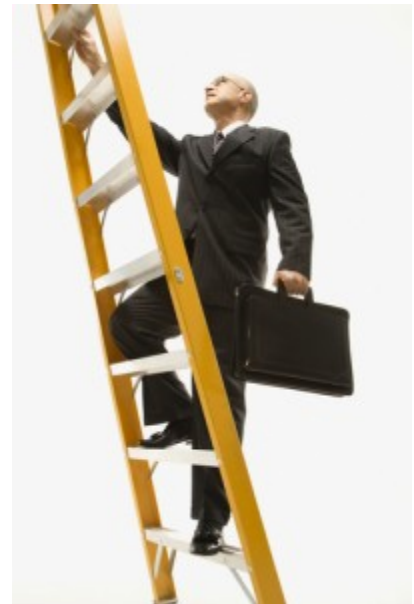
## Massachusetts Case Demonstrates Benefit of “Material Change in Employment” Clause in Non-Compete Agreement

*By Erik Weibust and Ryan Malloy (June 10th, 2013)*

The Massachusetts Superior Court recently rejected a claim by a former employee that his post-employment restrictive covenants were void because his employment had materially changed, relying on a clause in the employee’s agreement providing that the covenants would survive any such changes.

Plaintiff A.R.S. Services, Inc. commenced litigation against its former employee, Daniel Morse, and his current employer, 24 Restore NE, LLC, alleging harm arising out of Morse’s breach of a non-competition and non-solicitation agreement with A.R.S. On April 5, 2013, Judge Edward Leibensperger of the Massachusetts Superior Court issued a preliminary injunction in favor of A.R.S. and rejected several defenses offered by Morse, including that his employment had “materially changed” such to void the agreement.

Morse was hired by A.R.S. in 2004 to work in the field of “disaster restoration,” which involves the clean-up and restoration of properties affected by natural disaster and chemical damage. Prior to joining A.R.S., Morse signed an agreement that included non-solicitation and non-competition provisions that prohibited Morse from working in the disaster restoration business within 50 miles of any A.R.S. office for one year following his termination. During his employment, Morse changed positions twice, but he was at all times one of the five highest-compensated A.R.S. employees.



In late 2012, Morse left A.R.S. to work for 24 Restore, a company also in the business of disaster restoration. 24 Restore was informed of the non-competition and non-solicitation agreement between Morse and A.R.S. When A.R.S. demanded that Morse cease breaching the agreement, Morse began working for Restore 24 only in Maine. Nonetheless, A.R.S. filed the present lawsuit and moved for preliminary injunctive relief.

In opposition to A.R.S.’ motion, Morse argued that the non-competition and non-solicitation agreement was void because his employment relationship with A.R.S. had materially changed on two occasions after he signed the agreement. He argued that the agreement would only be enforceable if A.R.S. offered a new agreement in exchange for his changed employment relationship. Judge Leibensperger rejected Morse’s argument because the agreement expressly provided that “The terms and condition of this Agreement and its enforceability shall continue to apply and be valid notwithstanding any change in [Morse’s] duties, responsibilities, position or title with [A.R.S.]. . . .” Judge Leibensperger also [determined](#) that, although Morse’s job title changed twice during his employment, he remained one of the five highest-compensated employees at A.R.S., and that any change in his responsibilities was not material because each role “required Morse to be involved in A.R.S.’s disaster restoration projects and to promote A.R.S.’s brand by attending industry seminars and maintaining his industry relationships.” Based on these facts, the court concluded that A.R.S. had a substantial likelihood of



# Trading Secrets



successfully establishing that the agreement is enforceable and that Morse's change in employment status "did not act to vitiate the bargained for Agreement."

Massachusetts case law with respect to the voidability of non-competition agreements because of material change in employment is inconsistent. Interestingly, Judge Leibensperger discussed but did not distinguish an October 2012 Superior Court case that voided a non-competition agreement because of a material change in the defendant's employment, even where the agreement stated that a material change in employment would not void the agreement. See *Akibia, Inc. v. Hood*, C.A. No. 2012-02974 (Mass. Super. Oct. 9, 2012). Nevertheless, the recent *A.R.S.* decision suggests that employers should include "material change" clauses in their employment agreements.

# Trading Secrets



## Pleading Former Employer's Breach Of Employment Contract: Affirmative Defense Or Counterclaim To Suit For Violating Non-Compete And Non-Solicitation Covenants?

*By Paul Freehling (June 11th, 2013)*

### **Affirmative defenses and compulsory counterclaims.**

In many instances, the consideration for an ex-employee's non-compete and non-solicitation covenants was new or continued employment. If the former employer then breaches the employment contract — for example, by failing to pay all of the compensation and benefits to which the ex-employee was entitled — but nevertheless sues the ex-employee in an effort to enforce the covenants, the ex-employee probably will plead “unclean hands” (that is, one who seeks equity must do equity) as an affirmative defense. But here's the rub: An ex-employee's affirmative defense of unpaid compensation and benefits may derail the former employer's covenant violation lawsuit, but the ex-employee may be held to have waived the right to collect the sums due her unless she also files a counterclaim.



**Affirmative defense of former employer's material breach of contract.** Recently, Jumbo Sack Corporation sued an ex-employee in a Missouri state court for breach of a non-competition covenant. The ex-employee responded that Jumbo Sack's failure to pay him all of the compensation to which he was entitled warranted the entry of summary judgment for him in the non-compete litigation. The trial court agreed. The appellate court reversed and remanded for a determination of whether Jumbo Sack *materially* breached its contract, holding that (a) only a material breach would preclude enforcement of the covenant, and (b) materiality is a question of fact which cannot be decided on a motion for summary judgment. *Jumbo Sack Corp. v. Buyck*, No. ED98134 (Mo. Ct. of Ap., 5/21/13).

**Affirmative defense vs. compulsory counterclaim.** In an unrelated recent Massachusetts court case, Sentient Jet, LLC sued two ex-employees for violating noncompetition and non-solicitation covenants. The ex-employees did not counterclaim but asserted as an affirmative defense that the covenants were unenforceable because Sentient failed to give them all the compensation and benefits to which they were entitled. After being instructed that “[Sentient] promised to provide a job for the [ex-employees] at a certain level of pay. If [Sentient] failed to pay the [ex-employees] according to the terms of the contract, then it cannot recover against [them] for breach of contract,” the jury returned a verdict for Sentient.

While the state court case was pending, the ex-employees sued Sentient in a Massachusetts federal court, alleging violation of federal and state statutes governing payment of wages, and breach of the employment contract. When the state court entered judgment for Sentient based on the jury verdict,





# Trading Secrets



the company moved for summary judgment in the federal case, arguing that (a) the state court judgment collaterally estopped the ex-employees' statutory claims of unpaid wages, and (b) the Massachusetts compulsory counterclaim rule required dismissal of the counts alleging breach of contract. The federal court agreed and entered summary judgment for Sentient on all counts. [\*Brennan v. Sentient Jet, LLC\*, Civil No. 12-cv-11519-LTS \(D. Mass., 5/21/13\)](#).

**Takeaway.** Ex-employees, sued for violating covenants not to compete or solicit, may plead as an affirmative defense that the former employer materially breached their contract of employment. If the forum has a compulsory counterclaim rule (federal courts and some states do, Illinois and some other states do not), the ex-employees may not have the option of filing a separate breach of contract cause of action. Even if there is no applicable compulsory counterclaim rule, however, pleading "unclean hands" as an affirmative defense to the former employer's complaint for violation of covenants may lead to a holding that the doctrine of collateral estoppel controls the breach of contract lawsuit.

# Trading Secrets



## Wyoming Supreme Court Upholds Non-Compete Prohibiting Sale of Booze At Bowling Alley

*By Paul Freehling (June 18th, 2013)*

**Owner of bowling alley promises not to sell alcoholic beverages in competition with neighboring restaurant and bar.** The owner and operator of a restaurant and bar where liquor was sold and consumed conveyed an adjacent unimproved portion of the lot to purchasers who intended to and did construct and operate a bowling alley there. In connection with the real property purchase and sale, the parties executed a party wall agreement which included the purchasers' covenant not to sell alcoholic beverages on the premises of the bowling alley. There was no time limit on the covenant. Subsequently, the purchasers began selling liquor there.

**Wyoming Supreme Court rules that the covenant is enforceable.** The seller demanded that those sales cease. In response, the purchasers filed a declaratory judgment action in a Wyoming state court, seeking entry of an order that the covenant was unenforceable and void as a matter of law because it purportedly continued indefinitely. Both parties filed motions for summary judgment. The trial court granted the purchasers' motion. On appeal, the Supreme Court of Wyoming reversed and remanded with directions to enter summary judgment for the seller. [Oliver v. Quynn, No. S-12-0161 \(6/5/13\).](#)

**Reasons for the Supreme Court's decision.** Citing the Restatement (Third) of Property: Servitudes § 3.6, Comment b (2000), several non-Wyoming cases, and a 1982 New York University Law Review article, the Supreme Court held that the following factors were particularly significant in deciding that the covenant was valid:

- (a) The covenant was made in connection with a purchase and sale of property, not as part of an employment contract.
- (b) The covenant related to a single parcel of land.
- (c) The purchasers were well aware of the covenant when they signed the party wall agreement.
- (d) The restriction had only a minimal effect on competition.
- (e) Measured by the remaining useful life of the existing buildings, the likely duration of the restraint was not unreasonable.

**Takeaway.** A covenant not to compete is a restraint on trade which, therefore, must be reasonable or it will not be enforced. The decision concerning enforceability of any such restraint requires balancing the conflicting legal principles of freedom of contract versus freedom to work or conduct a business. This decision illustrates the circumstances which may lead a court to opt in favor of freedom of contract by enforcing a non-competition covenant without a time limit.



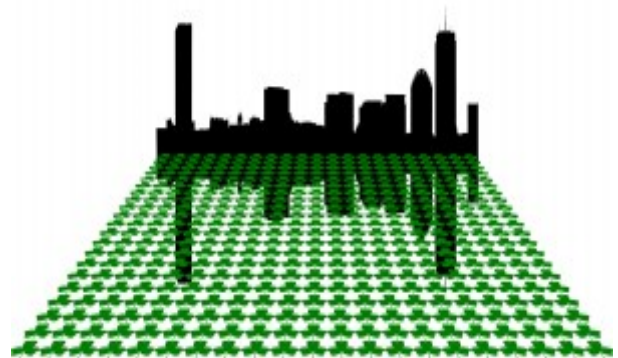
# Trading Secrets



## Doc Rivers: Will He Stay or Will He Go to La La Land?

*By Erik Weibust (June 21st, 2013)*

While most NBA fans have been focused on the recently-concluded championship series between the Miami Heat and the San Antonio Spurs, those of us in Boston have been keeping a close eye a different NBA story (to the extent we're not focused entirely on the Bruins' Stanley Cup run): What will become the fate of beloved coach Doc Rivers, who helped bring a 17th championship to Boston after 22 long years? A press conference with Rivers and president of basketball relations Danny Ainge scheduled for this afternoon [was abruptly cancelled and postponed until Monday](#).



Rivers has indicated his desire to leave the team, and the Celtics seem willing to oblige. There is one major issue getting in the way, however, and that is the fact that Rivers' contract with the Celtics (which has three years and \$21 million remaining) contains a non-compete clause that prohibits him from coaching for another team without the Celtics' consent. This is different, and far more restrictive, than most NBA coaches' contracts, which permit teams to negotiate compensation for coaches to switch teams before their contracts expire. The non-compete clause in Rivers' contract also gives the Celtics far more leverage, and the ability to demand substantial compensation from any team who wishes to employ Rivers. Hence the on-again-off-again talks between the Celtics and the Clippers, in which the Celtics have allegedly demanded star players and the Clippers don't seem inclined to part with any decent players or draft picks (although recent reports indicate that the talks are, perhaps, on again).

Of course, no team wants a disgruntled coach on its sideline, so there is little doubt that a deal will get done. Celtics fans can only hope that, unlike former Red Sox general manager Theo Epstein (who the team allowed to leave for the Chicago Cubs in exchange for an injured relief pitcher and the promise of a "player to be named later"), the Celtics hold out for real compensation so that they can begin the process of rebuilding.

We could go into how this relates to your business, but [Ken Vanko](#) and [Eric Ostroff](#) have already done that in two very informative blog posts of their own. We'll just stick to sports for this one.

# Trading Secrets



## Connecticut Legislature Passes Non-Compete Legislation

*By Daniel Hart (July 1st, 2013)*

We previously [reported](#) on H.B. 6658, which was introduced earlier this year in the Connecticut House of Representatives. The Connecticut Legislature passed the legislation on the last day of the legislative session. The final text of the Act, which was enacted as Public Act No. 13-309 and will go into effect on October 1, 2013 assuming the Act is signed by the governor, can be found [here](#).

The Act provides that, in certain circumstances specified in the Act, a “noncompete agreement” (which is not defined in the Act) entered into, renewed, or extended on or after October 1, 2013 between an employer and employee is void, unless, “before entering into the agreement, the employer provides the employee with a written copy of the agreement and a reasonable period of time, of not less than seven calendar days, to consider the merits of entering into the agreement.” Employees can waive the right provided under the Act if the waiver is reduced to a separate writing, sets forth the right being waived and is signed by the employee prior to entering into the agreement.



Because the Act represents the first time that Connecticut has enacted a non-compete statute of general applicability to all employees in the state (existing statutes apply only to security guards and broadcasters), the Act represents a significant development in Connecticut noncompete law. Nevertheless, the Act contains a significant limitation: unlike earlier drafts of the legislation, the Act **only** applies when:

- (1) “an employer is acquired by, or merged with, another employer,” **and**
- (2) “as a result of such merger or acquisition an employee of the employer is presented with a noncompete agreement as a condition of continued employment with the employer.”

The final version of the Act also contains three other noteworthy departures from the draft bill.

First, a prior draft of the bill would have provided employees with a statutory basis for filing suit against employers who act in violation of the law (including recovery of damages and attorney’s fees). The Act lacks this provision.

Second, a prior draft of the bill would have required employers to provide employees with “at least 10 days, and more if reasonable, to consider the merits of entering into the agreement.” The final bill dropped the number from 10 to 7 days and omitted the vague “more if reasonable” language.

Third, a prior draft of the bill provided that the bill applies to “an agreement or covenant which protects an employer’s reasonable competitive business interests and expressly prohibits an employee from



# Trading Secrets



engaging in employment or a line or business after termination of employment.” In contrast, the final version of the Act refers only to “a noncompete agreement” without further definition. It is unclear whether the legislature intended the language in the final version to be shorthand for true noncompete agreements (i.e., agreements that “expressly prohibits an employee from engaging in employment or a line or business after termination of employment”) or whether they intended the term “noncompete agreement” to include other post-termination restrictive covenants, such as covenants not to solicit customers and employees. However, given that the final version of the Act limited the scope of the original bill in most respects, it seems unlikely that the legislature intended to expand the scope of the Act to include restrictive covenants other than true noncompete covenants.

We will continue to monitor developments on this new law. In the meantime, any employers with operations in Connecticut should include compliance with this statute in any due diligence checklist for mergers or other acquisitions. For more information on this legislation or other non-compete or trade secret legislation, please see our recent [webinar](#) and [podcast](#) regarding the topic.

# Trading Secrets



## Illinois Appellate Court Rules That Employment For Less Than Two Years Is Inadequate Consideration For Enforcement Of Non-Compete And Non-Solicitation Covenants

*By Paul Freehling (July 2nd, 2013)*

### Overview

Non-compete and non-solicitation covenants in an employment agreement are not enforceable unless the restrictions are supported by adequate consideration. Illinois courts have held that there “must be at least two years or more of continued employment to constitute adequate consideration in support of a restrictive covenant.” No reported decisions from other states are in accord.



### The covenants and the lawsuit

Premier acquired Fifield’s prior employer and insisted that he sign an employment agreement. He did so on October 30, 2010 and went to work for Premier two days later. Its standard agreement contained nationwide two-year non-compete and non-solicitation covenants with respect to anyone with whom Premier had a business relationship during the 12 months immediately prior to termination. Before signing, however, Fifield negotiated an amendment to the effect that the covenants would not apply if he was terminated without cause in his first year of employment. Four months after he began working for Premier, he resigned and joined a competitor. He and his new employer filed a complaint in the Circuit Court of Cook County, Illinois, seeking a declaratory judgment that the covenants were unenforceable for lack of consideration. In a counterclaim, Premier asked for an injunction enforcing the covenants.

### Trial court grants requested declaratory relief

Premier maintained that, since the agreement was signed before Fifield came to work, the consideration was employment itself. Further, Premier argued that Illinois court decisions invalidating restrictive covenants in the absence of employment for a substantial period of time were intended to protect employees against deprivation of their livelihood if they are hired and then precipitously fired, but this couldn’t happen to Fifield because he was protected if he was discharged without cause within one year. Rejecting Premier’s contentions, the trial court granted the declaratory judgment sought by Fifield and his new employer.

### The Appellate Court’s analysis

The court of appeals affirmed. It held that in Illinois, “[P]ost-employment restrictive covenants are carefully scrutinized . . . because they operate as partial” restraints on trade. Absent other consideration, there must be continuous employment for at least two years. The court deemed irrelevant the facts that (a) Fifield’s employment started after he signed the employment agreement, (b)





# Trading Secrets



he resigned rather than being discharged, and (c) he was protected for one year which is only one-half of the requisite two-year mandatory protection.

## **What *Fifield* teaches**

The traditional rule in a breach of contract case is that the law does not inquire into the adequacy of consideration, only its existence. In the context of postemployment restrictive covenants, however, Illinois appellate courts hold that less than two years of employment is insufficient consideration; the Illinois Supreme Court has not yet opined. Under *Fifield*, assuming no consideration — other than employment — for such restrictions, employers who want to enforce the covenants may have to retain employees for at least two years. *Indeed, an employee apparently could nullify the restrictions unilaterally simply by resigning earlier than the second anniversary of the agreement.* To avoid these results, employers should consider whether the unique facts of this case requires the tender of something else of value besides just the offer of new or continued employment as consideration for the covenants. Please also see Ken Vanko's amusing ["dissenting" opinion](#) on the *Fifield* decision.

# Trading Secrets



## Connecticut Governor Vetoes Noncompete Statute Passed By Legislature

*By Daniel Hart (July 16th, 2013)*

We previously [reported](#) on H.B. 6658, which was introduced earlier this year in the Connecticut House of Representatives. On the last day of the legislative session, the Connecticut legislature enacted a substantially watered-down version of the bill as Public Act No. 13-309, the full text of which can be found [here](#). In yet another twist, however, last Friday Governor Dannel P. Malloy [vetoed](#) the legislation, returning the bill to the legislature with a letter noting his concerns about a lack of clarity in the final version of the bill enacted by the legislature.



The final bill, which would have gone into effect on October 1, 2013 if signed by Governor Malloy, provides that, in certain circumstances, a “noncompete agreement” (which is not defined in the bill) entered into, renewed, or extended on or after October 1, 2013 between an employer and employee is void, unless, “before entering into the agreement, the employer provides the employee with a written copy of the agreement and a reasonable period of time, of not less than seven calendar days, to consider the merits of entering into the agreement.” Employees can waive the right provided under the bill if the waiver is reduced to a separate writing, sets forth the right being waived and is signed by the employee prior to entering into the agreement.

Because the bill represents the first time that Connecticut has enacted a non-compete statute of general applicability to all employees in the state (existing statutes apply only to security guards and broadcasters), the bill would have represented a significant development in Connecticut noncompete law if signed into law. Nevertheless, the final bill contains a significant limitation: unlike earlier drafts of the legislation, the bill only applies when:

- (1) “an employer is acquired by, or merged with, another employer,” and
- (2) “as a result of such merger or acquisition an employee of the employer is presented with a noncompete agreement as a condition of continued employment with the employer.”

The final version of the bill also contains three other noteworthy departures from the draft bill.

First, a prior draft of the bill would have provided employees with a statutory basis for filing suit against employers who act in violation of the law (including recovery of damages and attorney’s fees). The final bill lacks this provision.

Second, a prior draft of the bill would have required employers to provide employees with “at least 10 days, and more if reasonable, to consider the merits of entering into the agreement.” The final bill dropped the number from 10 to 7 days and omitted the vague “more if reasonable” language.



# Trading Secrets



Third, a prior draft of the bill provided that the bill applies to “an agreement or covenant which protects an employer’s reasonable competitive business interests and expressly prohibits an employee from engaging in employment or a line or business after termination of employment.” In contrast, the final version of the bill refers only to “a noncompete agreement” without further definition. It is unclear whether the legislature intended the language in the final version to be shorthand for true noncompete agreements (i.e., agreements that “expressly prohibits an employee from engaging in employment or a line or business after termination of employment”) or whether they intended the term “noncompete agreement” to include other post-termination restrictive covenants, such as covenants not to solicit customers and employees.

In his letter returning the bill to the legislature, Governor Malloy observed that, in light of uncertainty in the final bill, “it would be better for both employers and employees to receive greater clarity from the General Assembly on this issue next session.” We will continue to monitor developments on legislation in Connecticut if and when comparable legislation is introduced in the legislature at the next legislative session.

\*Please note that there was confusion within several media outlets and blogs, including Trading Secrets, as to whether the Governor had in fact signed this legislation. We apologize for any confusion caused by those reports.

# Trading Secrets



## Material Change Defense To Non-Compete Enforcement Gaining Acceptance In Massachusetts

By Erik Weibust (July 17th, 2013)

In a series of recent decisions by the Massachusetts Superior Court, a longstanding, but oftentimes unsuccessful, defense to the enforceability of non-compete agreements and other post-employment restrictive covenants has quietly been gaining acceptance.



Perhaps this is a result of the economy picking up and employees having increased options and mobility, or perhaps it is indicative of a growing hostility to non-competes in Massachusetts. In any event, the Superior Court has been applying the so-called “material change” doctrine — the principle that a restrictive covenant is unenforceable if there are material changes to an employee’s employment relationship after the agreement is signed — with increased frequency over the past year to void otherwise enforceable restrictive covenants. Neither the Massachusetts Appeals Court nor the SJC has interpreted the “material change” doctrine to date. As a result, these recent decisions by the Superior Court have left practitioners, and their clients, with a series of unanswered questions on the enforceability of both current and future post-employment restrictive covenants.

The material change doctrine originally appeared in The SJC’s 1968 seminal decision in *F.A. Bartlett Tree Expert Co. v. Barrington*, 353 Mass. 585 (1968), but its rationale has not been applied with any notable consistency until this past year. In *Bartlett Tree*, the SJC held that changes to the employee’s compensation and sales territory “strongly suggest that the parties had abandoned their old arrangement and entered into a new relationship,” and, therefore, the non-compete agreement “was inoperative when the defendant terminated his employment with the plaintiff.” *Id.*, at 587-88.

Subsequent decisions have applied and refined the material change doctrine, including *Lycos, Inc. v. Jackson*, 18 Mass. L. Rptr. 256 (Mass. Super. 2004), in which the Superior Court held that “[e]ach time an employee’s employment relationship with the employer changes materially such that they have entered into a new employment relationship a new restrictive covenant must be signed.” *Id.* Several other Superior Court decisions have reached the same result. See, e.g., *Cypress Group, Inc. v. Stride & Assocs., Inc.*, 17 Mass. L. Rptr. 436, 2004 WL 616302 (Mass. Super. Ct. Feb. 11, 2004); *Intertek Testing Servs. N.A., Inc. v. Curtis Strauss, LLC*, 2000 WL 1473126 at \*6 (Mass. Super. Ct. Aug. 8, 2000); see also *ABC Cable Sys., Inc. v. Clisham*, 62 F. Supp. 2d 167, 173 (D. Mass. 1999) (applying Massachusetts law); *Iron Mountain Information Mgmt., Inc. v. Taddeo*, 455 F. Supp. 2d 124, 132 (E.D.N.Y. 2006) (applying Massachusetts law). As a result of these decisions, defendants began raising the material change defense with increasing frequency, but the doctrine never really seemed to gain a foothold until last year.

In 2012, the Superior Court ruled in *Grace Hunt IT Solutions, LLC v. SIS Software LLC*, 2012 WL 1088825 at \*4 (Mass. Super. Feb. 14, 2012) (previously reported on here), that a change in management that resulted in an employee’s base salary being reduced voided a restrictive covenant. Later that year, in *Sentient Jet LLC v. Mackenzie* (Unreported, March 2012), the Superior Court rejected the material change defense, however, ruling that “It is not a situation where a covenant not to



# Trading Secrets



compete is sought to be enforced after dropping someone's . . . base salary by 20 percent and making it unlikely they'd ever be able to make it up, as was the case in [*Grace Hunt*]." This seemingly narrowed the holding of *Grace Hunt* to situations in which an employee's salary was reduced.

Earlier this year, however, the Superior Court ruled in the opposite direction in *Intepros, Inc. v. Athy*, 2013 WL 2181650 (Mass. Super. May 5, 2013). In that case, rather than decreasing the defendant's salary, he was promoted and his salary was increased several times after he signed his non-compete agreement some 15 years earlier. *Id.*, at \*5. That was enough of a change to void his non-compete agreement, the Court ruled, because just as in *Bartlett Tree* and its progeny, "Mr. Athy's employment relationship with Intepros materially changed over his many promotions. As a result, the non-competition agreement executed in 1997 between Mr. Athy and Intepros must be declared void and unenforceable." *Id.* Also this year, in *Rent-A-PC, Inc. v. March, et al.*, (May 18, 2013), U.S. District Court in Massachusetts ruled that *Bartlett Tree* "is a significant problem for the plaintiff. [Defendant] underwent several material changes to his employment, but he did not sign any additional restrictive covenant agreements."

As a result of the *Bartlett Tree* line of cases, many employers began included material change clauses in their post-employment restrictive covenants, which provide that the agreement will remain enforceable regardless of any material changes in the employee's employment relationship. Although no appellate level court has addressed this issue, or offered an opinion on whether such clauses are enforceable, the Superior Court ruled earlier this year in *A.R.S. Services, Inc. v. Morse*, 2013 WL 2152181 (Mass. Super. Apr. 5, 2013) (previously reported on [here](#)), that the existence of such a clause in a non-compete agreement was sufficient to defeat a material change defense: "[T]he parties understood that the Agreement was intended to be enforceable notwithstanding a potential change in employment responsibilities. . . . No persuasive reason is advanced by Morse for ignoring the terms of the Agreement." *Id.*, at \*9.

Whether including a material change clause in a post-employment restrictive covenant is sufficient to defeat a material change defense remains an open issue. While it certainly cannot hurt to include such a clause, it will not necessarily carry the day. As such, until the Appeals Court and/or the SJC rule definitively on the issue, we would recommend that if an employee's employment relationship materially changes (although that phrase remains undefined in the caselaw), he or she should be required to sign a new non-compete agreement as a condition of continued employment. Indeed, given the lack of guidance and increased focus on this defense in Massachusetts, it may be prudent for certain companies to require employees to reaffirm their post-employment obligations on an annual basis, both to remind them of their obligations and to avoid any argument that their employment relationship was materially changed. Of course, there are many other considerations that must go into in any post-employment restrictive covenant, particularly for companies with employees in multiple states, and we recommend that experienced counsel review any post-employment restrictive covenants prior to requiring employees to sign them.

# Trading Secrets



## You've Already Signed Your Offer Letter– Can You Still Be Subject to a Non-Compete Agreement Signed at the Inception of Employment Without New Consideration? Pennsylvania Supreme Court Says Yes

*By Jessica Mendelson (July 18th, 2013)*

Is new consideration required for a valid covenant not to compete presented to an employee at the inception of their employment after they sign their offer letter?

Under the majority approach, recognized in many states continued employment is sufficient consideration for a valid non-compete agreement. However, a minority of jurisdictions, will not enforce a non-compete agreement offered for signature after the employee has already begun work unless it is supported by new consideration. In those jurisdictions, continued employment is typically not considered sufficient consideration and they instead require that any non-compete be supported by new consideration such as a promotion, stock options or some other tangible benefit. The minority rule can prove problematic in situations where there are multiple employment documents which may be construed as a non-compete agreement and, therefore, the commencement of employment date and the date of execution of employment agreements are often essential. The Pennsylvania Supreme Court recently addressed the issue of whether a covenant not to compete is enforceable when offered after the employee has already accepted an offer letter and employment has commenced in the case of [\*Pulse Technologies, Inc. v. Notaro\*](#).



In 2005, Pulse Technologies, Inc., offered a position to Peter Notaro in an offer letter describing his responsibilities, salary, benefits, start date, and confidentiality requirements. The letter stated that he would be asked to sign an employment agreement on his first day of work, which he subsequently signed, along with a covenant not to compete. Four years later, Notaro resigned and joined a competitor, MK Precision, LLC, and Pulse sued to enforce the non-compete agreement. The superior court granted a preliminary injunction enforcing the non-compete agreement, and the appellate court subsequently vacated the decision, finding that there was inadequate consideration.

On appeal, however, the Supreme Court of Pennsylvania reversed the appellate court and reinstated the non-compete agreement, [\*finding that\*](#) “the offer letter was simply part of the hiring process and did not constitute the actual employment contract.” Instead, the court found that the letter simply summarized the relationship between the parties, which would eventually be memorialized in the employment contract. According to the court, because the letter **indicated that an actual employment agreement would be required**, the non-compete agreement was a condition of the employment relationship, and thus, was enforceable because it was supported by consideration.





# Trading Secrets



Employers in Pennsylvania and potentially other states enforcing the minority rule regarding consideration for a non-compete agreement should be aware of this decision, as it indicates that courts will closely analyze the language and circumstances of an offer letter in order to determine whether it is an actual employment agreement. Employers should be careful about clearly indicating to employees that they are expected to sign an employment agreement or restrictive covenant, and make sure to explain this prior to finalizing an employment contract so that there is no confusion between the parties. Doing so may reduce the potential for litigation in the future. For more details on this important decision, please see John Marsh's instructive [analysis](#) of the decision.

# Trading Secrets



## Comply or Lose: New York Affirms Enforcement of Non-Compete in Rescission Action for Employee Equity Grants

By Marcus Mintz (July 19th, 2013)

A New York Supreme Court recently affirmed the viability of the “employee choice doctrine” in a rescission action involving employee equity grants. [See \*Lenel Systems Int'l., Inc. v. Smith\*](#), 106 A.D. 3d 1536, 966 N.Y.S.2d 618 (N.Y. App. Div. 2013). The “employee choice doctrine” arises when an employee has a choice between complying with post-employment obligations, such as a non-compete or non-solicitation agreement, or risk forfeiting certain benefits, such as equity grants.



Generally, post-employment restrictions will be reviewed by a court for reasonableness and are disfavored as a restraint on an employee's ability to earn a living. When an employee is given the choice of compliance or forfeiture of benefits, however, “there is no unreasonable restraint upon an employee's liberty to earn a living” as a matter of law. Put simply, if an employee can choose whether or not to comply with a restrictive covenant, then there is no “unreasonable restraint” on the employee's ability to earn a living.

The New York Supreme Court was recently asked to consider the application of the employee choice doctrine to an action for rescission of stock options granted to an ex-employee, Smith, based on his alleged breach of a non-compete provision in the stock option agreement. While employed at plaintiff Lenel Systems International, Inc., Smith was granted stock options. The stock option agreement required that, as a condition of the grant, Smith would not compete with Lenel while employed and for two years following his termination from employment. Smith voluntarily terminated his employment and assumed employment with an alleged competitor.

Lenel filed a lawsuit against Smith, alleging that he was violating the non-compete in his stock option agreement and seeking rescission of the stock options. Smith moved for summary judgment on Lenel's claim for rescission, arguing that the restrictive covenants in the stock option agreement were unreasonable and, therefore, unenforceable as a matter of law. While the court acknowledged the general policy of disfavoring restrictive covenants against employees, it held that such policy did not apply to the facts in *Lenel Systems* because the employee **had a choice** between compliance and forfeiture. In addition, the court held that when the “employee choice doctrine” applies, a restrictive covenant will be enforceable **“without regard to reasonableness”** provided that the employee voluntarily terminated his or her employment.

In addition to other tools an employer may use to protect its business interests, enforcing restrictive covenants contained in equity grants through actions for enforcement of express forfeiture provisions may provide an effective mechanism for retaining employees. However, employers must be mindful that any inducements to comply with restrictive covenants must be sufficiently lucrative to ensure employee compliance.

# Trading Secrets



## Even Preparing To Compete In Texas May Be Prohibited During A Non-Competition Covenant Period

*By Paul Freehling (July 22nd, 2013)*

### Overview

Nationsbuilders, an insurance underwriter, and two of its ex-employees executed a contract which contained a covenant barring the individuals, for one year, from competing with the underwriter or working for an “entity that *conducts or plans to conduct* a business that is in competition” with the underwriter. The ex-employees used that year to prepare for the competition that would commence after 12 months. The underwriter claimed that what they were doing violated the non-compete agreement, and a few days ago a Texas appellate court announced that it agrees. [Nationsbuilders Ins. Services, Inc. v. Houston Int’l Ins. Group, Ltd., No. 05-12-01103-CV \(Tex. App., 7/3/13\).](#)



### The “competition”

While they were employed by Nationsbuilders, the individuals covenanted not to compete. When they resigned and went to work for a competitor, Nationsbuilders complained. Thereafter, the parties entered into a settlement agreement which contained a 12-month non-competition period. During that year the ex-employees did not sell, quote or bind any insurance products in the relevant markets, but they did (a) send out marketing materials to potential clients, (b) prepare state agency regulatory filings, (c) develop underwriting guidelines, (d) draft policy and claim forms, and (e) conduct market research. Nationsbuilders considered those activities to constitute a violation of the settlement agreement.

### Arbitration

The agreement provided for arbitration of any dispute, and so the underwriter filed a statement of claim alleging impairment of the “bargained for dormant period of non-competition.” In response, the ex-employees denied that they were competing and asserted that, in any event, (a) Nationsbuilders’ contention that it had been damaged was hypothetical, and (b) the covenant was unenforceable for other reasons.

### The award

The arbitrator sided with Nationsbuilders. He ruled that the parties’ agreement entitled Nationsbuilders to a one year “dormant restricted period of non-competition, including the full extent of the no planning prohibitions.” His award included a 12-month equitable extension of the non-compete covenant, and during that period the ex-employees were directed not to engage in “head start’ planning for



# Trading Secrets



competition.” The settlement agreement provided for application of Delaware law. Both that state and Texas permit equitable extension of a non-compete covenant.

## **The arbitrator’s powers**

The ex-employees persuaded a Texas trial court to vacate the arbitration award, but the Texas Appellate Court recently reversed. The Appellate Court stressed that the decision of an arbitrator must be upheld if its terms are rationally inferable from the parties’ contract. The court found that the arbitrator’s award here drew “its essence” from the wording and purpose of the non-compete covenant. The ex-employees maintained that the award was excessively vague because it did not state precisely what they are and what they are not permitted to do during the extension period. The court disagreed and held that the award clearly prohibits conduct enabling them “to engage in ‘Competition’ after the restricted period sooner than they would be able without the conduct.” The ex-employees queried whether all “passive contemplation” — such as internal and external communication, budgeting, and spending of money — is prohibited during the covenant period. The appellate tribunal’s answer was that “passive contemplation” might “constitute a technical breach of the settlement agreement but ‘would not rise’ to the level of a material breach” unless it results in a “head start.”

## **Remand**

The Appellate Court observed that in the lower court the ex-employees had made two arguments not decided by the trial court. They had maintained that the award (a) “serves as an unconscionable restraint on competition” because of the vast geographic expanse of the covenant, and (b) violated public policy by improperly interfering with their business despite the absence of any loss of customers or revenue to Nationsbuilders. Neither argument was dealt with in the lower court’s decision, and so the cause was remanded for consideration of those arguments.

## **Takeaways**

The Appellate Court’s decision in *Nationsbuilders* could be viewed as a product of its own peculiar facts and circumstances which might seldom, if ever, recur. Thus, the opinion might have little precedential significance. On the other hand, it may be a harbinger of things to come. The ruling may lead to development of a generalized legal principle that potentially penalizes virtually all preparation for competition during the non-compete period.

A prohibition in a non-compete covenant of employment by an entity that *conducts or plans to conduct* business in competition with the former employer in the relevant market might at least discourage ex-employees from using the non-compete period to prepare for competition. However, employers should recognize that, if litigation ensues, a court might conclude that the restriction is unduly vague or otherwise unenforceable.

# Trading Secrets



## Physician Noncompetition Agreements May Be Challenged More Often After Recent Texas Appellate Decision

*By Randy Bruchmiller (July 23rd, 2013)*

A recent appellate decision out of the Beaumont Court of Appeals may throw a new wrinkle into Texas's ever-evolving law on physician noncompetition agreements.

In Texas, physician noncompetition agreements must contain buyout provisions to be enforceable. That is, the physician must be allowed to buy his or her way out of the geographical and temporal restrictions the noncompetition agreement imposes. This requirement is unique to physicians and mandated by statute. As a practical matter, large buyout amounts have traditionally kept physicians from violating their agreements.



Historically, many practitioners and legal scholars have read the statute to require that the buyout clause do one of two things: (1) recite a specific payment amount; or (2) provide that an arbitrator will determine the buyout number. The working theory among many practitioners has been that, if the parties choose the former option, the courts will enforce the agreed-upon amount. The Court of Appeals in Beaumont recently interpreted the statute differently.

In [\*Sadler Clinic Association, P.A. v. Hart\*](#), 2013 WL 2631482 (Tex. App. Beaumont 2013), the court held that, even if the agreement provides a specific buyout amount and does not provide for arbitration, courts may nonetheless order the parties to arbitrate the amount if the physician claims the amount is not "reasonable" at the time he or she departs. In so holding, the Court "presume[d] that the parties contracted with knowledge of the statute's arbitration provision concerning the price," and used that as a basis to allow arbitration.

This new decision may result in some physicians violating their noncompetition agreements and litigating rather than abiding by the agreement due to a large buyout provision. Further complicating the situation is the likelihood that agreements currently used by some hospitals and physician associations omit one or more statutorily-required provisions simply because they have been handed down over the years without being updated. Accordingly, many physician contracts in Texas are likely on shaky ground. Entities contracting with physicians should therefore be especially careful that their noncompetition agreements meet all the statutory requirements and comply with recent case law.



# Trading Secrets



## Massachusetts Non-Compete Legislative Update

*By Erik Weibust (July 24th, 2013)*

On July 23, 2013, the Boston Bar Association hosted its [5<sup>th</sup> Annual Symposium on Employee Non-Compete Agreements, Trade Secrets, and Job Creation](#).

Speakers at the well-attended event included Senator William N. Brownsberger and Representative Lori A. Ehrlich, co-sponsors of a compromise non-compete bill that is working its way through the state legislature, along with Jennifer Lawrence, General Counsel of the Massachusetts Executive Office of Housing and Economic Development (who participated as a representative of Governor Deval Patrick's Administration), and several private practitioners (including Russell Beck and Michael Rosen, whose non-compete blogs can be found [here](#) and [here](#)).



Brownsberger and Ehrlich described the long process that has led to their most recent (and substantially watered down) bill, discussed below, along with the myriad interests with which they have had to contend on a hot-button issue such as this. Both seemed genuinely interested in getting to a result that was equitable to both employers and employees, but expressed frustration with the amount of time and effort it has taken to get there. Ms. Lawrence indicated that the Patrick administration is strongly opposed to non-compete agreements in general, and she repeatedly referenced the impact of restrictive covenants on both single mothers who are kept out of work and high tech companies, which purportedly will not relocate to Massachusetts due to its enforcement of non-compete agreements (despite the fact that 46 other states also permit them in one form or another, and that there are several other laws on the books in Massachusetts under which companies find it exceedingly difficult to do business, including the [wage and hour laws](#)).

There are currently three bills pending in the Massachusetts legislature that could affect the enforceability of non-compete agreements in the Commonwealth: Senator Brownsberger and Representative Ehrlich's compromise bill and two bills that would prohibit non-compete agreements altogether. Recall from these [previous posts](#) that Senator Brownsberger and Representative Ehrlich each introduced competing non-compete legislation in 2008 — Brownsberger's would have gone the way of California and a few other states and banned all non-compete agreements, whereas Ehrlich's would have been far less restrictive. In the spring of 2009, the legislators collaborated on a compromise bill, Massachusetts House Bill 2293, entitled "An Act Relative to Noncompetition Agreements." House Bill 2293 aimed to codify existing common law while affording greater procedural protections to those subject to contractual restrictions on employment mobility. After several revisions, House Bill 2293 ultimately failed to pass. According to Brownsberger and Ehrlich, this failure was due, in part, to the bill being weighed down and made too complicated by new provisions that were intended to mollify critics on both sides of the issue.

**The Noncompetition Agreement Duration Act.** The "Noncompetition Agreement Duration Act" (on which we previously reported [here](#), introduced by Senator Brownsberger and Representative Ehrlich, leaves intact much of the existing common law, but creates a presumption that a non-compete agreement of up to six months is reasonable, whereas a non-compete agreement that lasts longer than





# Trading Secrets



six months is presumed unreasonable. If a court determines that the duration of the non-compete agreement is unreasonable, the non-compete agreement will be unenforceable in its entirety, with three exceptions (in which case the court may enforce the non-compete for any duration it deems appropriate): (i) “the employee has breached his or her fiduciary duty to the employer;” (ii) “the employee has unlawfully taken, physically or electronically, property belonging to the employer;” or (iii) “the employee has, at any time, received annualized taxable compensation from the employer of \$250,000 or more.” This represents a significant departure from existing Massachusetts law, which permits the court to reform an unenforceable agreement to make it enforceable. Like House Bill 2293, the Noncompete Agreement Duration Act does not impact non-disclosure agreements, non-solicitation agreements, non-competes in connection with the sale of a business (where the party to be restricted is an owner of at least a 10% interest of the business who receives significant consideration for the sale), non-competes outside of the employment context, forfeiture agreements, or existing trade secrets law. A [hearing](#) on this bill is currently scheduled for **September 10, 2013** before the Joint Committee on Labor & Workforce Development. We plan to attend and will report back with any material updates.

**An Act Relative to the Prohibition of Noncompete Agreements.** Representative Sheila Harrington filed a competing bill to the Noncompetition Agreement Duration Act on January 18, 2013, entitled “An Act Relative to the Prohibition of Noncompete Agreements,” that would prohibit the use of non-compete agreements altogether, much like California has done. Specifically, the bill states: “Except as provided in this section, any contract that serves to restrict an employee or former employee from engaging in a lawful profession, trade, or business of any kind is deemed unlawful.” The only exceptions are for the sale of a business or the dissolution of a partnership or LLC, which have substantial limitations. Unlike Senator Brownsberger and Representative Ehrlich’s previous and current compromise bills, this bill would seemingly apply to non-solicitation agreements as well. Indeed, the bill explicitly states that it does not apply to non-disclosure agreements, but is silent about non-solicitation agreements.

**The Uniform Trade Secrets Act.** Finally, snuck into a bill that seeks to make Massachusetts the 49<sup>th</sup> state to adopt the Uniform Trade Secrets Act (on which we previously reported [here](#)), is a provision that would ban non-compete agreements altogether, much like the bill filed by Representative Harrington. This bill, filed by Representatives Garrett Bradley and Thomas Calter, would similarly bring Massachusetts in line with California and a small group of other states that prohibit the use of non-compete agreements. It is interesting that this provision is included in the Uniform Trade Secrets Act, which in its original form does not include such a prohibition.

Based upon Ms. Lawrence’s comments at the symposium (as well as Governor Patrick’s own statement earlier this year, on which we previously reported [here](#)), these latter two bills would be more favorable to the Patrick administration than Senator Brownsberger and Representative Ehrlich’s Noncompetition Agreement Duration Act. As the panelists at the symposium discussed, however, prohibiting non-compete agreements would not necessarily reduce the amount of litigation in Massachusetts; instead, it may just shift to disputes over misappropriation of trade secrets and breaches of non-solicitation agreements, which can be just as costly and time-consuming, if not more so. In fact, as trade secret misappropriation can be quite difficult to allege absent strong indicators of such misappropriation (e.g., proof of large transfers or deletion of data), in the absence of the protections afforded by non-compete provisions many employers may find themselves in the unenviable position of being unable to prevent irreparable harm to their business when a key employee leaves for a competitor until there is solid proof of misappropriation, at which point it may simply be too late to protect the employer’s assets.

So, as we said back in 2009, [Massachusetts Is Not California; At Least Not Yet!](#) Nothing has changed since that time, however, and it may very well be heading in that direction if compromise legislation



# Trading Secrets



cannot be passed. That would seem to be Governor Patrick's preference. In any event, this healthy and productive debate continues, and we will continue to monitor it and report any material updates. If you missed our recent webinar on significant legislative updates across the country, you can watch it [here](#).

# Trading Secrets



## Employment Agreement Mandating Arbitration With Exclusion To Seek Equitable Relief From Court For Non-Compete Violations Found Unconscionable

By Paul Freehling (July 29th, 2013)

### Summary

Tatum, an employee of ProBuild, purportedly blew the whistle on her subordinate for allegedly stealing from ProBuild. Shortly thereafter, she was fired, but alleged similarly situated male employees were not. She filed a gender discrimination suit in a New Mexico state court. ProBuild removed the case to federal court and then moved to compel arbitration based on the mandatory arbitration clause in ProBuild's employment agreement. That clause provided, however, that equitable relief could be sought in a court for violation of the non-competition, non-solicitation, and confidentiality covenants in the agreement. Since those were allegations ProBuild could be expected to assert, whereas the claims employees would tend to file (such as employment discrimination) had to be arbitrated, "common sense" led the federal court to hold that the agreement was one-sided and unfair. [Tatum v. ProBuild Co., No. Civ. 12001060 LH/LFG \(D.N.M., July 17, 2013\).](#)



### The Agreement

The parties' agreement required them to attempt to settle their disputes but, if not resolved amicably, to proceed to final and binding arbitration. However:

1. The parties had "the right to seek an injunction or other equitable relief from a court in connection with a claim for breach or violation of a non-competition, non-solicitation, non-disclosure or similar protection of business and confidential information obligation." Nevertheless, "the enforceability of any such obligation and merits of the underlying claim of breach or violation shall . . . be resolved through arbitration."
2. If a party instituted "court action against the other with respect to any Dispute required to be arbitrated . . . , the responding party shall be entitled to recover from the initiating party all damages, costs, expenses, and attorneys' fees incurred as a result of such action."

### The Court's Holdings

The New Mexico federal court concluded that the agreement was a contract of adhesion since ProBuild drafted it, all employees were required to sign it, and its terms were not negotiable. Under New Mexico law, adhesion contracts are enforceable except if "the terms are patently unfair to the weaker party." Relying primarily on "common sense" (but also mentioning a 2002 California Appellate Court decision, and dicta in a 2010 federal court opinion in a case based on California law), the court in *Tatum* held that the agreement was unconscionable because "ProBuild has exempted from arbitration



# Trading Secrets



the claims it is most likely to bring . . . and confined to arbitration the claims its employees are most likely to bring.”

ProBuild protested that the agreement was not one-sided because after a judge rules on a request for equitable relief, the parties could proceed to arbitrate the enforceability of the covenants. But the New Mexico federal court explained that this supposed opportunity to obtain an arbitrator’s ruling is illusory. If ProBuild seeks and obtains an injunction from a court, necessarily the court will have made at least a preliminary determination that the covenants are enforceable, and an arbitrator is unlikely to challenge that determination. On the other hand, if an employee asks a court for equitable relief and it is denied, few employees would then initiate arbitration and run the risk of having the arbitrator shift to the employee ProBuild’s costs and attorneys’ fees relating to the court proceeding. For these reasons, too, the district court concluded that the agreement was unconscionable.

The court’s decision runs contrary to [a recent California appellate decision](#) which reached a different result. Special care should be given in using such exclusions in employment agreements and counsel should analyze applicable state law, including any recent decisions, before using such provisions.

# Trading Secrets



## Georgia Court Rules That Non-Compete Does Not Bind Seller's Agents

*By Paul Freehling (August 2nd, 2013)*

### Summary

Marguerite and her two daughters were the members and managers of an LLC. On behalf of the LLC, Marguerite negotiated and executed a contract to sell its assets to N&N Holdings. The contract contained a covenant providing that “neither Seller nor its agents” would compete with, or solicit customers or employees of, the buyer during specified periods in a designated geographical area. Within that period and area, however, Marguerite and her daughters created a new LLC. It began competing with N&N which sued everybody — the seller, the new LLC, Marguerite, and her daughters — in a Georgia state court for violation of the covenant.



The trial court granted summary judgment to N&N. The judgment was reversed on appeal on the grounds that the seller was not competing with N&N, and none of the other defendants had agreed to be bound individually by the covenant. [Primary Investments, LLC v. Wee Tender Care III, Inc., Case No. A13A0412 \(Ga. App., 7/16/13\)](#) (notice of intention to petition the Supreme Court of Georgia for a writ of certiorari filed 7/19/13).

### The contract

Primary Prep Academy operated a childcare facility. In a multi-million dollar transaction, Primary sold its assets to N&N which continued Primary’s business under a new name. The purchase and sale contract contained a three-year covenant pursuant to which “Seller agrees that neither Seller nor its agents will” (a) solicit Primary’s employees who become employees of N&N at the same location, (b) solicit parents of a child enrolled at Primary’s facility during the 12 months preceding the closing, or (c) open a child care center within a 10-mile radius of any location being sold.

### Litigation commences

During the relevant time period, Marguerite and her two children formed a new LLC which opened a childcare facility within the 10-mile radius. After they were sued, the defendants filed a counterclaim for rescission and equitable reformation of the non-competition clause. All parties moved for summary judgment.

### Trial and Appellate Court rulings

The trial court granted the buyer’s summary judgment motion with regard to the defendants’ alleged violation of the non-compete covenant and denied the defendants’ summary judgment motion with respect to their counterclaim for rescission or reformation. On appeal, the lower court’s ruling that



# Trading Secrets



defendants violated the non-compete covenant was reversed, but the lower court's decision declining to order rescission or reformation of the covenant was affirmed.

The Appellate Court held that none of the defendants was liable for improper competition with N&N. The seller was not liable because it did not engage in business, much less in competition with N&N, after the sale. The new LLC and Marguerite's children were not liable because none of them was a party to the asset purchase agreement. Marguerite was not liable because she was not a party to the agreement as an individual. She negotiated and signed the agreement solely in her representative capacity on behalf of the seller, a disclosed principal, thereby binding the principal. Ordinarily, an agent who executes a contract on behalf of a disclosed principal does not bind herself individually absent an express agreement to do so.

## **Takeaway**

In support of its holding that only the principal was bound by the covenant, the Appellate Court cited several Georgia court decisions. But none involved interpretation of a contract provision purporting expressly to bind a principal and "its agents." Further, reading the contractual provision "neither Seller nor its agents will" as meaning, simply, "Seller will not," the words "nor its agents" appear to have been given no force or effect.

The ruling undoubtedly would have been different if the parties had identified each of the persons they intended to include within the reference in the covenant to the seller's "agents," and had insisted that all of those persons agree unequivocally to be bound by the covenant.



# Trading Secrets



## New Hampshire Court Voids Non-Compete Clause in Independent Contractor Agreement

*By Paul Freehling (August 21st, 2013)*

A recent New Hampshire decision serves as a reminder that courts may treat non-compete provisions differently in the context of independent contractor agreements compared to employment agreements.

### Summary

The Presiding Justice of the New Hampshire Superior Court [held](#) earlier this month that, under the circumstances of the case before him, a non-compete covenant imposed restraints on an independent contractor “greater than necessary to protect the legitimate interests” of the plaintiff.



### The covenant

Woodward was a personal trainer. His relationship with Brian's 1:1 Fitness, a training facility, began as an employee. Subsequently, he executed annual independent contractor agreements. He paid Brian's a “rental” fee in exchange for use of the employer's space and equipment for training his clients. He alone determined the training regimen of his clients, he kept 100% of the fees they paid, and he was not subject to any control by Brian's.

Like each other trainer at Brian's, Woodward was subject to a non-competition agreement. It provided that for two years after the end of his relationship with Brian's, he would not compete within 25 miles of places where it conducted business. In addition, he was precluded from providing personal training services to any client who had been served by Brian's within two years prior to his termination.

### The lawsuit

Shortly after he resigned from Brian's, Woodward opened his own facility. Three trainers and a number of clients left Brian's and joined him. Brian's sued him and asked the court to issue a preliminary injunction enforcing the non-compete. The court refused.

### Reasons for the ruling in favor of Woodward

There is no New Hampshire Supreme Court precedent regarding the standards to apply in determining the reasonableness of a non-compete covenant in an independent contractor agreement. According to a 2006 Delaware Chancery opinion cited by the New Hampshire Superior Court justice, the subject has not been discussed in many reported rulings, but most jurisdictions addressing it have held that those standards parallel the ones used in analyzing similar clauses in employer-employee contracts. However, both the Delaware Chancery Court judge and the New Hampshire justice rejected those holdings.



# Trading Secrets



According to the New Hampshire justice, as compared with employees, “[I]ndependent contractors have less access to legitimately confidential information of their employers.” Moreover, according to the court, independent contractors are more likely to bring their own strengths and abilities to the enterprise, have a less intimate relationship with the employer (for example, an employee may be expected to perform other reasonable tasks as needed), and traditionally work with less supervision. Also, the court reasoned that the employer typically would not be responsible for torts committed by an independent contractor but would be liable for damages caused to others in the course of an employee’s employment.

In the justice’s view, the covenant Woodward signed exceeded Brian’s legitimate interests. It was “simply a restraint of trade which is not in the public interest.” [\*Brian’s 1:1 Fitness v. Woodward\*, No. 2012-CV-00838 \(Merrimack, SS \(NH\) Superior Court, 8/8/13\).](#)

## **Takeaways**

Not many reported cases deal with the standards to be applied in determining the enforceability of a non-competition clause in an independent contractor agreement. Some judges simply state that the rules should be the same as for an employee and employer.

Other courts analyze the relationship to determine how dissimilar it is to the employer-employee model. In those jurisdictions, if the contractor truly is independent, receiving no salary, wages or benefits from the employer, and not subject to the employer’s control in any respect, a restrictive covenant is more challenging to enforce. Thus, an employer whose agreement with an independent contractor contains a non-compete clause may be able to avoid the costs and risks that would be incurred if the individual were denominated an employee, but the price may be invalidation of the covenant. Accordingly, add non-compete enforcement to the checklist that companies should analyze when deciding between employee or independent contractor classification.

# Trading Secrets



## Missouri Federal Court Finds Forfeiture-For-Competition Provision in Stock Option Agreement Enforceable

*By Paul Freehling (September 4th, 2013)*

A recent Missouri federal court decision highlights the different standards that courts employ in evaluating forfeiture-for-competition provisions contained in stock option plans.

Summary. Many courts testing the validity of a contractual forfeiture-for-competition provision use a “reasonableness” standard. Recently, however, a Missouri district court judge aligned himself with the minority view and held that regardless of whether the provision in an employee’s stock option plan is fair or unfair, it is enforceable. The reason: the plan provided that the Board of Directors, which was not shown (or even alleged) to have engaged in fraud or bad faith, had the right to decide whether to exercise the company’s rights. [Smythe v. Raycom Media, Inc., Case No. 1-13-CV-12 \(CEJ\) \(E.D. Mo., Aug. 15, 2013\).](#)



### The relevant provision

Smythe worked for Raycom for 14 years before he retired. His final position was general manager of the company’s Cape Girardeau, Missouri television station. During his employment, he was a participant in two stock option plans. Each plan provided for forfeiture of unpaid awards if “in the opinion of [Raycom’s Board of Directors], the Participant, without the prior written consent of the Company, engages directly or indirectly” in competition with Raycom or any subsidiary. The plan also stated that “[T]he decisions of the Board and its action with respect to the Plan shall be final, binding and conclusive upon all persons having or claiming to have any right or interest under the Plan.” The forfeiture provision contained neither a time nor a geographic limitation.

### Violation

A scant three months after retiring from Raycom, Smythe accepted employment with another Cape Girardeau TV station. Raycom notified him that, as a result, he forfeited all awards issued pursuant to one of the two stock plans. He filed a declaratory judgment action in a state court challenging the notification. Raycom removed to federal court based on diversity jurisdiction.

Delaware law applied, but there were no reported appellate decisions on point from courts in that state. However, in a 1989 case concerning a forfeiture-for-competition clause applied against an employee who was terminated without cause, the Third Circuit Court of Appeals predicted that Delaware appellate courts would apply a “reasonableness” test. Subsequently, in 2005, a Delaware Superior Court judge used the “fraud-or-bad-faith” standard.



# Trading Secrets



## Ruling in favor of Raycom

The Missouri federal court decision accords with the minority of rulings concerning the enforceability of a forfeiture clause. The court held that, because the Board of Raycom was vested with discretion to determine Smythe's eligibility under the stock plans, the Board's decision cannot be overturned unless the Board acted fraudulently or in bad faith (neither of which were alleged).

## Takeaways

The primary purpose of covenants not to (a) compete with the former employer, (b) solicit the former employer's clients/customers or other employees, and (c) disclose the former employer's confidential information, is to *prevent* an employee from engaging in or facilitating *unfair* competition. By contrast, while a forfeiture clause might have that effect, its primary purpose is to *discourage* an employee — by imposing as a penalty the loss of future retirement benefits, contingent bonuses, or stock options — from engaging in competition, *fair or unfair*, with the employer.

Like Raycom, an employer in a jurisdiction where a court has not selected the “reasonableness” test for use in forfeiture-for-competition clause litigation may be able, by careful draftsmanship of the clause, to maximize the probability that a “fraud-or-bad-faith” standard will be employed. In addition to an unequivocal delegation to the Board of Directors of authority to interpret the plan, a forfeiture-for-competition provision might also:

- a. Identify expressly the post-employment benefits that are conditional,
- b. Spell out the circumstances (such as the employee's violation of post-employment covenants) under which the employer has no obligation to provide those benefits, and
- c. State that the employee will not challenge enforceability of the clause unless a showing can be made that the employer engaged in fraud or bad faith in drafting or invoking the clause.

Finally, to be amply cautious, the employer should exercise the power of forfeiture in an even-handed and non-discriminatory manner, emphasizing cogent reasons for believing that the employee's competition will damage the employer. In that event, the action probably may pass the “reasonableness” test if a court adjudicating the validity of the provision decides to apply that standard.

# Trading Secrets



## Is Massachusetts Inching Closer to California? Governor Deval Patrick Issues Public Support for the “Outright Elimination” of Non-Compete Agreements

*By Erik Weibust (September 10th, 2013)*

We attended a hearing today before the Massachusetts Legislature’s Joint Committee on Labor and Workforce Development regarding the pending non-compete legislation on which we have previously [posted](#).

Among others who testified about the issue was Governor Deval Patrick’s Secretary of Housing and Economic Development, Gregory Bialecki.

Mr. Bialecki finally acknowledged publicly what the Patrick Administration has been dancing around for some time now (see our recent post on the issue [here](#)), and which we believed was inevitable: that it supports the “outright elimination of enforceability” of all non-compete agreements in Massachusetts, regardless of their duration or geographic scope. Mr. Bialecki also said that the Patrick Administration wants to see Massachusetts adopt the Uniform Trade Secrets Act, which it believes provides sufficient protection to companies (see our previous [post](#) on this issue).



If the legislature were to adopt the Patrick Administration’s suggestions, Massachusetts may be [the next California](#) as it relates to non-compete and trade secret law.

Below is Secretary Bialecki’s [full testimony](#) (with our **emphasis added** to the most notable points). We will provide a more detailed report on the legislative hearing in the coming days.

*Dear Chairman Conroy and Senator Wolf,*

*Thank you for the opportunity to appear before you today. I am here to express the strong support of the Patrick Administration for substantial reform of the current rules on the enforceability of non-competition agreements in Massachusetts.*

*I gave very similar testimony to this committee almost two years ago. Now, as then, there are bills in the Legislature that call for changes to our current rules regarding the enforceability of non-competes and bills that call for the end to such enforceability.*

*I suggested two years ago that it seemed increasingly unlikely that we could achieve any meaningful consensus among the stakeholders on changes to our current system that left non-competes in place. I think that this has turned out to be the case, as the debates and disagreements that you will hear today are almost exactly the same as those that you heard two years ago.*





# Trading Secrets



*I also suggested two years ago that if we could not achieve any meaningful consensus among the stakeholders on changes to our current system, then the best course for Massachusetts would be the outright elimination of enforceability of non-competition agreements. **I am here today to affirm that the Patrick Administration now supports such outright elimination, combined with adoption of the Uniform Trade Secrets Act**, which has been demonstrated in other states to protect the loss or disclosure of proprietary information by departing employees.*

*A key element of the Patrick Administration's economic development strategy has been to build on the strength of our world-class innovation economy. A key measure of success for our economic development and job creation policies and programs considers whether our policies and programs effectively support the innovation and entrepreneurship that has given us our critical competitive advantage for so many years. If our policies and programs do not provide this support then we should simply re-consider them. Our policy on non-compete agreements needs reform because Massachusetts should do everything it can to (1) retain talented entrepreneurs; (2) support individual career growth and flexibility; and (3) encourage new innovative businesses that are the engines of economic growth. Massachusetts employers currently have tools to protect the stability of their businesses.*

*Retention is Key: We do an excellent job of educating talented people here in the Commonwealth. However, if they work here and sign a non-compete agreement, we are essentially asking those same talented people to leave and to become entrepreneurs elsewhere. If Massachusetts is not able to create an environment that gives entrepreneurial talent a chance to thrive, then the most effective job creating companies may be pushed to grow to scale in states like California. In fact, we have heard examples of entrepreneurs at MIT who were advised to start their businesses outside of Massachusetts as a result of non-compete agreements laws. **Non-competes stifle movement and inhibit competition and we do not want that. The evidence is clear—we are not seeing the kind of spin-offs and starts up at the same rate that previously made Massachusetts an enviable model.***

***Individual career growth is good for the Commonwealth: We encourage our talent to be creative, to be innovative, and to network with other talented people. Furthermore, we encourage employers to recruit talented people. However, we send a mixed message: providing the talent needed to support the kind of explosive growth we want in the innovation economy is considerably more difficult if employees are legally unable to move between jobs in the innovation economy.** The current law makes it considerably harder for employees to leave their current employers, whether due to the actual enforcement of a non-competition agreement, or more frequently, just due to the threat of enforcement. The individual has no effective recourse. The only thing to do is to suspend relevant work until the term of the non-compete agreement expires. Most individuals are not in a financial position to afford not working for the term of the non-compete. Being out of the market for the term is a major liability to the individual's career and future development. An individual who has 10 or 20 or 30 years of experience and expertise is forced to avoid using their expertise during the term of their non-compete agreement. We do not want this mixed message to continue.*

*We want innovative businesses. A priority of this Administration has been to support and enhance the innovation economy. Massachusetts has long had a vibrant and leading edge in research and the innovative community. Many of the fundamental technological advances like the Internet economy and digital media had beginnings in Massachusetts in the past couple of decades. However, we could do more. We need more start-ups, especially in the technology and bio-tech sectors. Start-ups are good; they create jobs, push innovation to new heights, and retain talent. Many of our current employers, larger and small, report they are unable to attract lateral or advanced talent due to our current laws limiting the mobility of our workforce.*





# Trading Secrets



*Current employers should not feel threatened: Senators Brownsberger, Vice-Chairman Ehrlich, and Leader Bradley have championed the efforts in the legislature to reform the current system. While, we understand employers concerns that protecting their proprietary information is critical, non-compete agreements are neither the best option nor the only available vehicle to protect companies. By adopting the Uniform Trade Secrets Protection Act, and limiting or abolishing non-compete agreements, we will have an opportunity to both grow our economy and protect a company's proprietary information.*

*The Uniform Trade Secret Act (UTSA) has been adopted in 47 other states and the District of Columbia. The UTSA and other tools protect an employer's trade secrets and proprietary information, which is fundamentally important. Patents, confidentiality agreements, and trade secrets are more than sufficient to protect legitimate company interests against former employees. **Even without non-compete agreements, companies still have a disproportionate ability to litigate against the individual.***

*You will certainly hear today from businesses and business groups who would prefer to keep the current legal arrangements regarding non-competes intact. While holding onto their current employees may be convenient for employers, it is not at all clear that it is necessary to their business success. Our businesses could recruit the very talent they need without a non-compete agreement impeding the opportunity.*

***For these reasons, we support outright elimination of enforceability of non-completive agreements in Massachusetts combined with adoption of the Uniform Trade Secrets Act.***

# Trading Secrets



## Referring Former Employer's Customers To New Employer Held Violation Of Injunction, Resulting In Finding Of Criminal Contempt

*By Paul Freehling (September 12th, 2013)*

A recent Louisiana non-compete case involving two appellate decisions addresses three significant issues in non-compete litigation: 1) whether a former employee's referral of customers to a new employer violated the employee's non-solicitation of customer covenant; 2) the consequences of violating the covenant and court injunction; and 3) the appropriate standard of proof for contempt proceedings.



### **Summary of decision**

Five years into her employment with Acadian Cypress & Hardwoods as a sales representative, Acadian had Joy Stewart sign a non-solicitation agreement. It provided that for two years after her employment terminated, Stewart would not solicit Acadian's customers in more than 20 specified Louisiana parishes, eight identified counties in Mississippi, and two specific counties in Alabama. Several years later, she resigned from Acadian and went to work as a sales representative for one of its competitor.

Acadian sued Stewart and obtained a preliminary injunction against soliciting sales in the restricted territory. The new employer's headquarters was in one of the restricted parishes, and she lived in another one. Because of the covenant and injunction, she scrupulously avoided selling her new employer's products to Acadian's customers, or even calling on them. However, she phoned other customers from her home, and she had materials shipped to them. Further, if Acadian's customers contacted her, she invited them to communicate with her new employer's other salespersons or its warehouse. Acadian accused her of violating the injunction and committing contempt of court. The trial court agreed with Acadian. She appealed but, in a 2-1 decision last week, the Louisiana Court of Appeal affirmed. [Acadian Cypress & Hardwoods, Inc. v. Stewart, 2012 CA 2002 \(La. App., 1st Circ., Sept. 3, 2013\) \(McClendon, J.\) \(not for publication\).](#)

### **The first appellate court ruling**

This case went to the Court of Appeal twice. The first time was when Stewart appealed from issuance of the preliminary injunction. She argued that the covenant was ambiguous and lacked consideration. Those arguments were rejected. Perhaps because the applicable statute provided a temporal limitation on restrictive covenants (two years) but was silent with respect to the maximum allowable territory, she did not take issue — at the injunction hearing or on appeal — with the breadth of the non-solicitation's territorial restriction.

The injunction order was affirmed. [Case No. 2012 CA 1425 \(La. App., 1st Circ., Mar. 22, 2013\) \(McClendon, J.\) \(also not for publication\).](#) Judge Whipple, concurring in the result, expressed concern with regard to "the extensive geographic area set forth in the agreement, which I find comes perilously close to rendering such a contract unenforceable as an overly broad restriction on the interests of free



# Trading Secrets



enterprise. However, this issue was not specifically challenged on appeal.” Judge Whipple did see merit in Stewart’s argument regarding a lack of consideration for the covenant, and cited “the well-reasoned dissenting opinion” in an earlier Court of Appeal case, but concluded that the court was required to follow the majority’s ruling in that older case to the effect that continued employment was adequate consideration.

## **The second appellate court ruling**

The second appeal was taken from Stewart’s appeal of the finding of contempt. After an evidentiary hearing regarding the motion for contempt, the trial court ordered her “to pay all costs regarding the motion.” No conditions were attached to the order, apart from paying those costs, and there was nothing else that she was required to do to purge herself of the contempt.

In a 2-1 decision on her appeal, the majority voiced misgivings about the proceedings below but nonetheless again affirmed the lower court. The initial problem dealt with was whether Stewart was properly charged with criminal contempt for which the relevant standard of proof is “beyond a reasonable doubt.” A “preponderance of the evidence” would suffice for civil contempt. The majority reasoned that because the judgment below ordered payment of court costs and “is an unconditional penalty, one that Ms. Stewart cannot affect or end, it is criminal in nature.”

The majority agreed with Stewart that the trial court’s interpretation of the injunction — seemingly prohibiting her from (a) speaking with customers outside the area by phone from her home (which was within the restricted territory), and (b) asking the home office (also within the territory) to send materials to those customers — “could effectively prevent her from engaging in her business anywhere in the United States.” Still, the majority found that referring Acadian’s customers to her new employer “constituted a violation of the non-solicitation provisions of the injunction. Therefore, based on the record before us, we conclude that any rational trier of fact could find the essential elements of criminal contempt beyond a reasonable doubt.” The dissenting judge did not write an opinion.

## **Takeaways**

Stewart may have made two mistakes. First, at the injunction hearing, she could have challenged the scope of the non-solicitation covenant’s territorial restriction. Her challenge below might or might not have succeeded, but at least she would have preserved the issue for appeal. Second, at the time the injunction was issued, and before engaging in any sales activities, she probably should have insisted on clarification with respect to permissible and impermissible conduct. In sum, the case demonstrates that there can be serious consequences for violating a customer non-solicitation provision, including criminal contempt.

# Trading Secrets



## First Circuit Holds that Solicitation is Barred by Non-Compete Agreement Regardless of Who Initiates Contact

*By Erik Weibust (September 24th, 2013)*

In *Corporate Technologies, Inc. v. Harnett, et al.*, U.S. Court of Appeals for the First Circuit recently [upheld](#) the issuance of a preliminary injunction barring a former employee (Harnett) from doing business with his former employer's (CTI) customers, even if the customers initiated the contact.



CTI had employed Harnett as an account executive/salesman for nearly a decade, and required that he sign an agreement when he joined the company that contained non-solicitation and non-disclosure provisions. In October 2012, Harnett “jumped ship” to work for a competitor, OnX Enterprise Solutions. As the court noted, “following his departure from CTI, Harnett participated in sales-related communications and activities with certain of his former CTI customers on behalf of OnX.” CTI quickly filed suit in state court, which Harnett removed to the U.S. District Court for the District of Massachusetts. CTI sought, and obtained, a preliminary injunction that prohibited Harnett from engaging “in any marketing or sales efforts . . . for a period of twelve months” with respect to several CTI customers whom he formerly had serviced. “With regard to those customers, [the preliminary injunction] also compelled [Harnett and OnX] to withdraw any bids that Harnett had helped to develop.” Harnett and OnX appealed.

The First Circuit (Selya, J.) opened its [decision](#) with the following statement:

Businesses commonly try to protect their good will by asking key employees to sign agreements that prohibit them from soliciting existing customers for a reasonable period of time after joining a rival firm. When a valid non-solicitation covenant is in place and an employee departs for greener pastures, the employer ordinarily has the right to enforce the covenant according to its tenor. That right cannot be thwarted by easy evasions, such as piquing customers' curiosity and inciting them to make the initial contact with the employee's new firm. As we shall explain, this is such a case.

The Court went on to note that “[t]he dispute between the parties turns on the distinction between actively soliciting and merely accepting business — a distinction that the Massachusetts Appeals Court aptly termed ‘metaphysical’” in *Alexander & Alexander, Inc. v. Danahy*, 488 N.E.2d 22, 30 (Mass. App. Ct. 1986). Harnett argued that “because the customers in question initiated contact with Harnett, he was thereafter free to deal with them without being guilty of solicitation.” The First Circuit disagreed, noting that “the customers only contacted Harnett following their receipt of a blast email announcing his hiring by OnX.” After recognizing that “Massachusetts trial courts have accorded varying degrees of significance to initial contact depending on the facts at hand,” and that the Supreme Judicial Court has not addressed the issue directly, the First Circuit concluded:

After careful consideration, we conclude that the Massachusetts Supreme Judicial Court, if confronted with the question, would hold that a per se rule vis-à-vis initial contact has no place in this equation. . .



# Trading Secrets



. In the employment context, restrictive covenants are meant to afford the original employer bargained-for protection of its accrued good will. . . . According decretory significance to who makes the first contact would undermine this protection because that factor, standing alone, will rarely tell the whole tale. And because initial contact can easily be manipulated — say, by a targeted announcement that piques customers’ curiosity— a per se rule would deprive the employer of its bargained-for protection.

\* \* \* \*

In the last analysis, we believe that the better view holds that the identity of the party making initial contact is just one factor among many that the trial court should consider in drawing the line between solicitation and acceptance in a given case. This flexible formulation not only reflects sound policy but also comports with well-reasoned case law from other jurisdictions. . . . Thus, we decline the defendants’ invitation to assign talismanic importance to initial contact.

Discerning no error of law, we need not tarry over the district court’s weighing of the facts. This is a situation in which the initial contacts by customers are necessarily preliminary, the sales process is sophisticated, and the products are custom-tailored. Viewed against this backdrop, the evidence of record is adequate to underpin the lower court’s binary determination that Harnett violated the non-solicitation covenant and that the plaintiff is therefore likely to succeed on the merits.

As no opinion by Judge Selya is complete without an extra helping of [erudition](#), the Court went on:

There is no need for us to wax longiloquent. Solicitation can take many forms, and common usage suggests that the word has a protean quality. See, e.g., The Compact Edition of the Oxford English Dictionary 2911 (1971) (“To entreat or petition (a person) for, or to do, something; to urge, importune; to ask earnestly or persistently.”). Here, moreover, the non-solicitation provision specifically forbids Harnett from “entic[ing] away” customers of CTI.

Harnett’s own words and actions with respect to customers covered by the non-solicitation provision lend considerable credence to the district court’s tentative conclusion that he violated that provision. His calendar, email, and testimony show significant business communications with at least four of his former CTI customers on behalf of OnX. This persistent pattern of pursuing patronage permits a plausible inference that he was urging those customers to do business with OnX rather than CTI (in other words, an inference that he was trying to entice them away)

What is perhaps most interesting about this case is that Harnett’s agreement did not even include a non-acceptance provision, which are oftentimes included in non-solicitation provisions as an additional safeguard against an argument, like that raised by Harnett, that the customers initiated contact.

# Trading Secrets



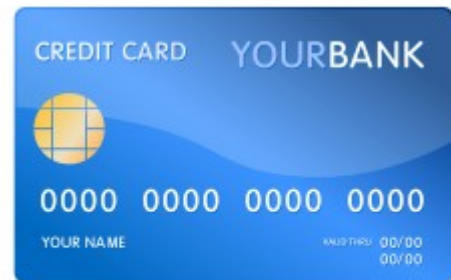
## Federal Appellate Court Lacks Jurisdiction To Hear Appeal of Expired Non-Compete Preliminary Injunction

*By Paul Freehling (October 2nd, 2013)*

The Eleventh Circuit recently dismissed an appeal of a preliminary injunction order on the grounds that the appeal was moot because the injunction had expired.

### Summary of the case

Leedom Management, a credit card processing company serving automobile dealers, sued a former employee and charged her with violating covenants not to (a) compete with Leedom, (b) solicit its clients, and (c) disclose its trade secrets and confidential information. Leedom sought and obtained a preliminary injunction, but the order contained a very limited territorial restriction and was to expire in December 2012, six months after it was entered rather than the one year provision in the covenants. Leedom appealed.



Last week, while the appellate proceedings were pending, the Eleventh Circuit Court of Appeals granted the former employee's motion to dismiss the appeal as moot because the injunction had expired. [\*Leedom Management Group, Inc. v. Perlmutter\*](#), Case No. 12-13017 (11th Cir., Sept. 25, 2013) (not for publication).

### The injunction and the ruling below

After Leedom terminated Perlmutter in December 2011, she established a Tennessee company in the same line of business. Leedom sued her and her company in a Florida district court, accusing her of violating covenants which restricted her activities for one year "within a 50 mile radius of any location in which Leedom is conducting its business." The district court granted Leedom's motion for entry of a preliminary injunction. However, the order was silent regarding its geographic limits. The parties were directed to negotiate those limits. When they could not agree, the case was referred to a magistrate judge for a ruling.

Interpreting the phrase in the covenant "any location in which Leedom is conducting its business," the magistrate judge concluded that the appropriate territorial scope of the non-competition and non-solicitation restrictions was all zip codes in which Leedom had a client. Perlmutter filed an objection in the district court. In June 2012, the district court overruled the magistrate judge and held that the covenants applied only within 50 miles of Sarasota, Florida, where Leedom had its sole place of business. The injunction's December 2012 termination date, 12 months after Perlmutter left Leedom but only six months after the order was entered, was not changed. Leedom filed an interlocutory appeal.





# Trading Secrets



## **Proceedings on appeal**

In January 2013, while the appeal was pending, Perlmutter moved to dismiss it as moot because the subject of the appeal was an injunction which had expired. Leedom responded that, notwithstanding expiration of the injunction, the appeal remained viable since the district court could equitably extend the time period of the injunction in order to give Leedom the benefit of its 12-month bargain. Further, Leedom argued that the appeal was not moot because it presented an issue capable of repetition. The appellate court was not persuaded. It held that Leedom was free to make the same arguments below in support of a motion for entry of a new preliminary injunction, after the case was remanded. The case below was not moot, obviously, and the grant or denial of a new injunction, or a final decision resolving all disputes, could be appealed.

## **Takeaways**

The phrase “location in which Leedom is conducting its business,” as used in the covenants, seems ambiguous in the circumstances of a company having clients or customers in diverse locales distant from its physical assets. More precise drafting might have led the district court to enter an injunction more to Leedom’s liking.

With regard to Leedom’s appeal becoming moot before it could be decided, that potentiality often is present when the duration of the covenant is short, for example one year or less. In a contested case such as this one, with a subsequent district court decision likely and with little risk that that decision would evade review, a claim that prejudice will result from dismissal of the initial appeal on the ground of mootness can be expected to fail.

# Trading Secrets



## How Do I Get a TRO Against a Former Employee If Arbitration in FINRA Is Mandatory?

*By Nicholas De Baun (October 4th, 2013)*

Occasionally, you may need emergency relief against a former employee who has absconded with a client list, your confidential information, and the clients themselves. If you are very unlucky, you may need to get a TRO against his new employer as well. If you, the former employee, and the new employer are all required to arbitrate any claims before FINRA, how do you get your TRO?



### **FINRA Rule 13804**

FINRA is well aware that its members and registered representatives may occasionally need emergency relief, and may need limited recourse to the courts to obtain a TRO. FINRA Arbitration Rule 13804 permits parties to obtain a TRO in court in conjunction with filing a statement of claim with FINRA. Under the rule, the parties obtaining a TRO must immediately submit their case to FINRA, which will appoint a panel on an expedited basis for summary adjudication on a preliminary injunction.

### **Procedure**

Under the rule, a party seeking a TRO may obtain one from any court of competent jurisdiction. If the court issues the TRO, the party must immediately submit a statement of claim to the Director of Arbitration of FINRA requesting injunctive relief as well as all other relief sought, and must serve the statement of claim on all other parties at the same time. The rule requires a hearing on the request for injunctive relief to commence within fifteen days, and provides an expedited process for selecting the panel that will hear the request. The process is the same if an arbitration claim has already been filed and the request for injunctive relief is being brought as a counterclaim.

Although the rule does not require it, it is prudent to file your statement of claim simultaneously with the TRO. You can supplement the statement if the court modifies the relief you are seeking. In addition, it is wise to attach the statement of claim to your court pleadings and the court pleadings to your statement of claim so that your adversary cannot argue to either tribunal that you are pulling the wool over its eyes.

### **Pitfalls**

A TRO can be a tricky thing to get, and courts seldom grant all of the relief you are seeking. Bear this in mind as you craft your TRO and argue for it in court – you will need a TRO that remains in place until FINRA can convene a hearing on injunctive relief. Allowing the court to provide a specific expiration date on the TRO is perilous, and numerous factors outside of your control could cause the hearing to be postponed beyond the court's deadline, leaving you without injunctive protection. If possible, you



# Trading Secrets



should request that the court order the matter to arbitration, and direct that the TRO will remain in place until the arbitration hearing can occur.

By the same token, if you are on the receiving end of a TRO, be sensitive to the fact that a FINRA hearing on an injunction may not be convened as quickly as you would like. Be prepared to argue in court for a specific expiration date on the TRO, and if the court declines to order one, be prepared to return to court for further relief if the FINRA process takes longer than you anticipated.

# Trading Secrets



## Virginia Supreme Court Rules Enforceability of Non-Competes Cannot Be Determined in a Factual Vacuum

*By Sarah Izfar (October 14th, 2013)*

A recent Supreme Court of Virginia [decision](#) will make it more difficult to challenge non-compete restrictions through early pleading challenges.

In *Assurance Data, Inc. v. Malyevac*, the Supreme Court of Virginia [reversed](#) the Circuit Court of Fairfax County, which sustained a demurrer, and, in doing so, determined the enforceability of certain restraints on competition contained in an employment agreement on the pleadings. In remanding the action back to the lower court, the Supreme Court of Virginia held that any finding regarding the enforceability of the agreement must be made on the facts, and certainly not at the demurrer stage.



### **Background**

Plaintiff Assurance Data, Inc. (“ADI”) is a company which provides information technology consulting and design services. It retained defendant John Malyevac to sell its computer products and services to its customers and required Malyevac to execute an employment agreement containing various restraints on competition. Pursuant to the employment agreement, upon termination of his employment with ADI, Malyevac was prohibited from selling products also sold by ADI for six months, disclosing confidential information, and soliciting ADI customers. In particular, the non-solicitation provision provided Malyevac would not solicit any ADI customers “[e]xcept for the sole benefit of [ADI] . . . for a period of twelve (12) after the date of termination.”

A few months after Malyevac entered into the agreement, he resigned. Shortly thereafter, ADI filed a complaint alleging that Malyevac had violated a number of the provisions contained in the employment agreement.

### **Demurrer and Appeal**

Malyevac filed a demurrer claiming that the agreement’s non-compete and non-solicitation clauses were overbroad and thus unenforceable. He pointed to the “twelve” contained in the non-solicitation clause, arguing that it was unenforceable because no increment of time, *i.e.* days, weeks, months, or years, was specified. The Circuit Court of Fairfax County sustained the demurrer finding that, as a matter of law, the non-compete and non-solicitation provisions were unenforceable.

The Supreme Court of Virginia reversed, finding that the lower court erred in sustaining the demurrer. It explained that the only purpose of a demurrer is to determine whether a party has stated a cause of



# Trading Secrets



action upon which relief can be granted. A demurrer should never be used to determine whether the restraints on competition are actually enforceable. The Supreme Court observed that, in sustaining the demurrer, the lower court improperly deprived ADI of the opportunity to present evidence to meet its burden of showing that the contract's restraints on competition were reasonable.

## **Takeaway**

In reversing the lower court, the Virginia Supreme Court reaffirmed a long line of cases which requires that an agreement that restrains competition be evaluated on its own merits and determined on its own facts. This ruling is helpful for employers seeking to enforce non-compete provisions in that it preserves the opportunity for the employer to present evidence regarding the enforceability of its non-compete agreements. Nevertheless, an employer must be prepared to meet its burden of showing that a non-compete is enforceable because it (i) restrains a former employee no more than is necessary to protect a legitimate business interest; (ii) is not unduly harsh or oppressive in curtailing an employee's ability to earn a livelihood; and (iii) is reasonable in light of sound public policy.

# Trading Secrets



## Illinois Supreme Court Won't Take Up Non-Compete Case, Adequate Consideration Questions Remain

*By Michael Wexler (October 18th, 2013)*

Once a stalwart of adequate consideration in exchange for a restrictive covenant, new employment, remains in flux after the *Fifield v. Premier* case [was not taken up](#) by the Illinois Supreme Court recently.

*Fifield*, decided in the summer of 2013 by the First District Appellate Court, [held](#) that in order for employment to be adequate consideration for a non-compete, employment must last at least two years. The fact pattern of the case was somewhat unique in that *Fifield*, an employee of a subsidiary of Great American, signed a new covenant agreement with Premier, a company that purchased *Fifield*'s employer and offered him employment at the newly acquired business. Hence, *Fifield*'s employment appeared more similar to continued employment than actual new employment. However, in making its decision, the Appellate Court treated new employment and continued employment the same resulting in what appears to be a significant departure from traditional notions of adequate consideration in Illinois and elsewhere.



Typically, in the vast majority of states in the U.S., a new employee's employment is contingent upon signing a restrictive covenant agreement. Therefore, new employment is adequate consideration for a covenant agreement. Many times, additional consideration is also recited in the body of the covenant agreement also in exchange for the covenants. These items include equity grants, monies, bonuses, benefits, and the provision of trade secrets or confidential information. The *Fifield* appellate opinion did not address these items.

Consequently, courts and employers are faced with numerous consideration questions not addressed by *Fifield* or elaborated on by the Illinois Supreme Court. Was other consideration provided to *Fifield* besides employment? What other consideration is still recognized in Illinois as adequate? What should an employer do about current employees employed less than two years? What consideration should be offered new employees? How far is the reach of this decision? A conversation with a legal professional may be in order.



# Trading Secrets



## 13 Scary Years Ago Court Issued Death Sentences In Horrid Dispute Over Vampire Fangs.

*By Erik von Zeipel (October 30th, 2013)*

Once upon a midnight dreary, in the *annus horribilis* of 2000, the United States District Court for the District of Colorado issued its terrifying decision in what is the seminal artificial vampire fangs case entitled [\*Nutting v. RAM Southwest, Inc.\*, 106 F. Supp. 2d 1121 \(D. Col. July 10, 2000\)](#).

The plaintiff in this chilling tale, Mr. Nutting, was the inventor of a creepy artificial vampire fang product called “Custom Dracula Fangs.” The defendants, Mr. and Mrs. Sheppard, also sold and manufactured artificial vampire fangs, including a frightening product called “Original Fangtastics.”



Mr. Nutting and Mr. Sheppard met at an abhorrent Halloween trade show and entered into a union whereby it was agreed that the Sheppards would distribute Mr. Nutting’s “Custom Dracula Fangs.” As part of that agreement, the parties also signed (in blood?) a ghastly non-competition agreement covering the entire world (including, presumably, the underworld). As so often happens in cases involving artificial vampire fangs, bad blood soon brewed and the distributor relationship started decomposing after the Sheppards began to package their “Professional Fangtastics” fangs (an evolution of their “Original Fangtastics”) in a coffin-shaped display box similar to that used for “Custom Dracula Fangs.”

Mr. Nutting then sued the defendants asserting gruesome claims for infringement of his trollish patent on the “Custom Dracula Fangs,” inducing infringement of the patent, deceptive trade practices, and breach of the bloody non-competition contract. In turn, the defendants asserted spooky counterclaims for interference with business and contractual relations and deceptive trade practices.

The defendants fiendishly moved for summary judgment on Mr. Nutting’s festering claim of breach of the non-competition agreement. Mr. Nutting cross-moved for summary judgment on the defendants’ ghoulish counterclaims. The court granted both motions without oral argument, sending the litigants’ claims to a certain doom.

### **The Haunted Non-Competition Agreement**

The court thrust a wooden stake through the heart of the bloody non-competition agreement, holding it void as a matter of law because: (1) it was a naked restraint on competition that failed to protect a legally cognizable interest and, as such, was void against public policy; and (2) the scope of the restraint embodied in the agreement went beyond any protectable interest. In so ruling, the court essentially found that Mr. Nutting’s argument that his patented vampire fangs was a trade secret “sucked.” Finally, the court proclaimed that the non-compete was horrifyingly overbroad, both as to time and geographic scope, and therefore pronounced dead on arrival.



# Trading Secrets



## **Defendants' Putrid Counterclaims**

The court completely gutted the defendants' rotting counterclaims. The court dismembered the claim for interference with business or contractual relations, finding that no reasonable juror, dead or alive, could find for the defendants because they failed to present competent evidence in support, including that Mr. Nutting had any evil intent. The court also held that defendants' claim for deceptive trade practices, based on the plaintiff's alleged disparagement of their vampire fangs, did not survive the light of day.

## **Fun size take home**

I'm being deadly serious when I say that this case is an oft-cited case of first impression under Colorado law addressing the reasonableness of a perpetual and worldwide covenant not to compete.

Happy Halloween! Remember to brush your fangs after candy!

# Trading Secrets



## Top Five Trends in Georgia Restrictive Covenants Law Three Years After Constitutional Amendment

*By Bob Stevens and Daniel Hart (November 11th, 2013)*

Three years ago last week, Georgia voters [overwhelmingly approved](#) a constitutional amendment that substantially altered Georgia's public policy on restrictive covenants.

Prior to enactment of the amendment, Georgia's public policy was actively hostile to restrictive covenants in employment agreements — so much so that a provision of the state constitution enshrined the state's public policy and declared covenants that defeat or lessen competition to be “unlawful and void.” Applying this constitutional provision, Georgia courts developed a number of drafting rules that rendered all but the most limited restrictive covenants unenforceable. This was the case even when the employee subject to the covenant was a high-ranking executive like the former vice chairman of a Fortune 500 telecommunications company who successfully challenged his non-compete agreement in the Georgia Court of Appeals' 2004 decision in [BellSouth Corp. v. Forsee](#), 595 S.E.2d 99 (Ga. Ct. App. 2004). As a practical consequence, Georgia was one of the most difficult jurisdictions in the country for employers to enforce restrictive covenants against former employees. Making matters worse for the state's business community, the Georgia constitutional provision against restrictive covenants thwarted legislative attempts to reform and modernize Georgia law on restrictive covenants.



Voters' approval of a constitutional amendment in November, 2010 removed the constitutional roadblocks, reversed the state's longstanding public policy against restrictive covenants, and ultimately paved the way for Georgia's enactment of its new [Restrictive Covenants Act](#), which the Georgia General Assembly enacted after a tortuous legislative history that we previously reported [here](#), [here](#), and [here](#). As we previously reported, Georgia's new Restrictive Covenants Act makes it much easier for employers to enforce restrictive covenants against former employees than was permitted by prior Georgia law and arguably reverses decades of Georgia court decisions.

The new law only applies to contracts entered into on or after May 11, 2011, the date that the Act became law. As a result, judicial decisions interpreting the new statute are still limited in number. Nevertheless, with the passage of three years since voters approved the constitutional amendment that made the new law possible, we can now identify general trends in judicial decisions. Although lawyers might disagree on which trends are the most notable, the following are, in our view, the top five trends about which Georgia employers and their counsel should be aware.

**1. Covenants dated on or after May 11, 2011 are more likely to be enforced.** Our first trend is a no-brainer, but we would be remiss in not stating it: employers will have less difficulty enforcing covenants executed on or after the effective date of the Restrictive Covenant Act than they will have in enforcing covenants entered into before passage of the new Act. Because continued at-will employment is usually considered sufficient consideration in Georgia for a new restrictive covenant agreement,



# Trading Secrets



employers in Georgia would be wise to update their existing agreements with employees if they have not already done so.

**2. Georgia courts will continue to apply old law to covenants dated before May 11, 2011.** Our second trend is a corollary of the first: because the law applies only to agreements entered into on or before May 11, 2011, courts continue to apply pre-Act Georgia law to covenants made before the effective date of the Act (May 11, 2011). As we discussed [here](#), this appears to be the case even where the covenant was signed before the 2011 Act but after voters approved the constitutional amendment that made way for the new Act. As courts continue to interpret contracts that predate the new Act, courts will likely continue to apply the old law in a number of cases. Anticipating the new law when voters approved the constitutional amendment, some Georgia employers immediately updated their agreements with employees between November 2, 2010 and May 11, 2011. Because these agreements may actually be subject to old Georgia law, employers in this situation should consider updating their agreements again to avoid application of old Georgia law.

**3. Georgia courts will continue to apply Georgia's old public policy in cases involving pre-Act covenants, even though Georgia's old public policy is inconsistent with the current public policy.** Although this trend is also a corollary of the first two trends, it's not as obvious. When courts are asked to enforce choice-of-law provisions in pre-Act agreements, courts have to consider whether application of the chosen state's law would violate Georgia's public policy. But what public policy do courts apply: the public policy as it exists now, or the public policy that existed when the agreement was executed? As demonstrated by the *Boone* case discussed [here](#), Georgia courts appear to have settled on the latter option and continue to invoke old (and now rejected) public policy when reviewing choice-of-law provisions in pre-Act covenants. This is the case even though the chosen state's law may be consistent with Georgia public policy as it exists now. We expect Georgia courts to continue to reject choice-of-law provisions in pre-Act agreements that are inconsistent with Georgia public policy as it existed pre-Act.

**4. Georgia courts will "blue-pencil" overbroad restrictive covenants that are entered into on or after May 11, 2011.** The new Restrictive Covenant Act provides that, "if a court finds that a contractually specified restraint does not comply with the provisions of [the Restrictive Covenant Act], then the court may modify the restraint provision and grant only the relief reasonably necessary to protect such interest or interests and to achieve the original intent of the contracting parties to the extent possible." O.C.G.A. § 13-8-55(b). As demonstrated by the *Pointenorth Insurance Group* decision that we discussed [here](#), Georgia courts can and will apply their power to "blue-pencil" overbroad restrictive covenants executed on or after the effective date of the Act. Nevertheless, it is not yet clear whether Georgia courts may only excise grammatically severable language or if they can effectively rewrite the parties' agreement by adding or inferring terms. Over the next few years, Georgia courts will likely better clarify the scope of their power to modify overbroad restrictive covenants and explain the situations in which they will exercise that power. Until the courts rule otherwise, prudent employers should assume that Georgia courts can only excise grammatically severable language and that they will use this power sparingly.

**5. Georgia courts will enforce true non-compete covenants only against employees who meet one or more of statutory definitions.** Although the new Restrictive Covenant Act is most favorable to employers who seek to enforce restrictive covenants, in one area the new law is arguably more restrictive than prior Georgia law. The new Act provides that "enforcement of contracts that restrict competition after the term of employment, as distinguished from a customer nonsolicitation provision . . . or a nondisclosure of confidential information provision . . . shall not be permitted against any employee who does not, in the course of his or her employment:



# Trading Secrets



- (1) Customarily and regularly solicit for the employer customers or prospective customers;
- (2) Customarily and regularly engage in making sales or obtaining orders or contracts for products or services to be performed by others;
- (3) Perform the following duties:
  - (A) Have a primary duty of managing the enterprise in which the employee is employed or of a customarily recognized department or subdivision thereof;
  - (B) Customarily and regularly direct the work of two or more other employees; and
  - (C) Have the authority to hire or fire other employees or have particular weight given to suggestions and recommendations as to the hiring, firing, advancement, promotion, or any other change of status of other employees; or
- (4) Perform the duties of a key employee or of a professional [which are defined elsewhere in the statute].

O.C.G.A. § 13-8-53(a). To date, very few (if any) reported decisions have construed these statutory definitions. Over the next few years, Georgia courts likely will be called upon to apply these statutory definitions and determine whether certain classes of employees are appropriately subject to true non-competes (as opposed to non-solicitation or non-disclosure covenants). Until the Georgia courts provide clearer guidance, Georgia employers should pay close attention to the language of the new statute when deciding which employees should have true non-competes in their agreements.

# Trading Secrets



## Georgia Federal Court Disregards Forum Selection Clause In Non-Compete And Non-Solicitation Covenant Dispute

*By Paul Freehling (November 12th, 2013)*

Notwithstanding a forum-selection provision in the parties' consulting agreement designating the Northern District of Georgia as the place for litigating non-competition and non-solicitation covenants disputes, a Georgia federal judge transferred covenant violation litigation to the Middle District of Florida. Also, the judge explained why he thought that an arbitration clause was unenforceable, but he said that the Florida court should make the decision. [Direct Response Products, Inc. v. Roderick, Case No. 1:11-cv-0945-WSD \(N.D. GA, Nov. 1, 2013\).](#)



### **Summary of the case**

Direct Response, a DeKalb County, Georgia company, stages sales events for automobile dealerships. Roderick was an independent contractor who marketed the events to dealers. After Roderick terminated the relationship, and allegedly began competing with Direct Response and soliciting members of Direct Response's sales team to join him, Direct Response filed a diversity jurisdiction case against him in the federal court in DeKalb County. The parties' agreement included a forum selection clause specifying that county as the place for litigating any dispute. At all relevant times, Roderick lived and worked in Florida. He moved to dismiss on various grounds including supposedly improper venue. In the alternative, he moved to stay the action because, he claimed, the agreement contained a mandatory arbitration provision. All of his motions to dismiss were denied but, on the court's own motion, the case was transferred to Florida "in the interest of justice." The Georgia judge declined to rule on Roderick's alternative motion but suggested that it should be denied by the transferee court.

### **The parties' contentions and court's decision regarding venue**

Roderick asserted that his territory did not include Georgia and that, if the breach he is alleged to have committed took place at all, it was in Florida and not in Georgia. Direct Response countered that the effects of the alleged breach would be manifested in DeKalb County. Further, the agreement was executed there, Roderick was trained in Georgia, and he was given access to confidential and proprietary information there. Finally, the agreement provided that all civil actions regarding Direct Response "must be processed in" DeKalb County; under the circumstances, that provision seems reasonable.

The Georgia federal judge denied Roderick's venue motion but, nonetheless, held that the "required focus" in determining the proper venue for this case is the site of the alleged breach, where Roderick is allegedly competing. Exercising the court's discretion under 28 U.S.C. § 1406(a), the case was transferred to Florida





# Trading Secrets



## **Arbitration**

The arbitration provision consisted of only two sentences. The first merely specifies what discovery rules are applicable in the arbitration proceeding and states, without any attachment or explanation: “Use the standard ‘one shot’ provision.” The second sentence simply reserves the parties’ “right to apply to a court of competent jurisdiction for equitable relief as necessary to preserve and enforce their rights under this Agreement.”

The court cited “the strong federal policy supporting arbitration” and said Georgia law provides that “an arbitration clause does not need to be detailed to be enforceable.” However, it “must have sufficient specificity to show what is to be arbitrated.” Here, the arbitration provision was silent in that regard as well as where the proceedings were to take place, what process was to be used for selecting a neutral, etc. Thus, it is not surprising that the Georgia judge was skeptical about Roderick’s claim that arbitration was mandated. Moreover, the parties’ testimony was diametrically opposite. The president and owner of Direct Response insisted that his intent was to delete the arbitration provision altogether but it was accidentally left in the agreement. Roderick asserted that he initialed the page with the arbitration clause and intended to include it. The Florida judge will have to decide whether the case is to be litigated or arbitrated.

## **Takeaways**

This case makes clear that even a reasonable forum selection clause might be disregarded if the court decides that transfer to a different venue serves “the interest of justice.” Further, the opinion here reminds us that a judge may disclose how he or she would resolve certain contested issues and yet leave the actual ruling to a different decision-maker.



# Trading Secrets



## Legislation

# Trading Secrets



## Employers Take Note: Michigan Adopts Social Media Privacy Legislation

*By Robert Milligan and Jessica Mendelson (January 8th, 2013)*

The Michigan Legislature recently passed the [Internet Privacy Protection Act](#) ("IPPA"), otherwise known as House Bill 5523. On December 28, 2012, Michigan Governor Rick Snyder signed the IPPA, making Michigan the fourth state to enact a social media privacy law regulating employers. In explaining the reasoning behind the law, Governor Snyder stated, "Cyber security is important to the reinvention of Michigan, and protecting the private internet accounts of residents is a part of that. Potential employees and students should be judged on their skills and abilities, not private online activity."



The IPPA prohibits both educational institutions and employers from requesting access to personal internet or social media accounts of employees or students. Furthermore, the act prohibits employers and educational institutions from retaliating against a person who fails to disclose such information.

The act broadly defines the terms employer and educational institution. "Employer" includes both public and private employees, as well as representatives and agents of an employer. Similarly, educational institutions include both "public or private educational institutions" ranging from nursery school through graduate school, and the term is construed "broadly to include . . . institutions of higher education to the greatest extent consistent with constitutional limitations." The law defines the phrase "personal internet account" as an "account created via a bounded system established by an internet-based service that requires a user to input or store access information via an electronic device to view, create, utilize, or edit the user's account information, profile, display, communications, or stored data."

IPPA prohibits employers from requesting employees or applicants for employment grant access to or disclose information permitting the employer to access the employee or applicant's personal email account. Furthermore, employers are prohibited from engaging in retaliatory behavior for an employee or applicant's failure to provide access to his or her personal email account. Similarly, educational institutions cannot require students or prospective students to grant access to or disclose information allowing access to his or her personal internet account, nor can these institutions penalize a student or prospective student for failure to disclose this information.

IPPA does not prohibit an employer from requesting an employee provide access to an electronic communications device paid, in whole or in part by the employer, or an account or service "provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes." Furthermore, the law does not prevent employers for disciplining or discharging an employee who obtains confidential or proprietary information from his or her employer without authorization. In addition, there is an investigation exception allowing employers to request an employee divulge social media information to ensure compliance with laws or regulatory requirements, to prevent unauthorized transfer of the employer's proprietary or confidential information, restricting access to certain websites on employer's communication devices. Finally, the IPPA does not prohibit or restrict an employer from "complying with a duty to screen employees or applicants prior to



# Trading Secrets



hiring or to monitor or retain employee communications that is established under federal law or viewing information available in the public domain.

With respect to educational institutions, the IPPA does not prohibit an educational institution from requesting or requiring a student to disclose access information to electronic communications devices paid for by the institution, or account or services provided by the institution used for educational purposes. Nor are educational institutions prohibited from viewing information available in the public domain.

The IPPA does not create a duty for an employer to monitor the activity of an employee's personal internet account, nor is an employer liable for failing to request access to a personal internet account. The IPPA also provides for criminal and civil penalties: violators can be found guilty of a misdemeanor and may suffer financial penalties of a maximum of \$1000, plus reasonable attorney fees and court costs in the case of a civil action.

Unlike the [California social media law](#), which we previously blogged on, the Michigan social media law more clearly differentiates between personal and employer-owned social media accounts. There may be still be issues regarding who is the owner of certain information but the statute at least attempts to provide clarity on the meaning of "personal" and excludes from its prohibitions devices paid for by the employer from its prohibitions, as well as accounts or services "provided by the employer, obtained by virtue of the employee's employment relationship with the employer, or used for the employer's business purposes." We have previously blogged about cases concerning the ownership of "social media assets" on [Twitter](#), [Facebook](#), [LinkedIn](#), and [Myspace](#), each of which illustrate the importance of clear policies regarding the ownership of company social media accounts. Here, the law focuses on who owns the account in order to determine whether there is a privacy right. As a result, both public and private employers will need to make sure that they employ social media ownership agreements with their employees to ensure that company social media accounts stay with the company and that the employer has the username and password for the account when the employee departs.

The enactment of this statute makes Michigan the fourth state, along with California, Maryland, and Illinois to restrict employers from accessing employees' and applicants' social media accounts (Delaware and New Jersey have passed social media privacy legislation protecting students' social media accounts). In all likelihood, 2013 will see additional social media laws passed throughout the country. Vermont, Texas, Missouri, and California (to apply to public employers) are considering [social media privacy legislation](#). We will continue to keep you apprised of future developments in social media legislation.

# Trading Secrets



## President Obama Signs Economic Espionage Act Amendments That Significantly Enhance The Penalties For Trade Secret Theft By Foreigners

*By Robert Milligan (January 15th, 2013)*

On January 14, 2013, President Obama signed the [Foreign and Economic Espionage Penalty Enhancement Act of 2012](#).

The Act enhances the penalties for certain violations of the Economic Espionage Act.

The purpose of the Act was to amend title 18, United States Code, to provide for increased penalties for foreign and economic espionage.

Under the Act, the upper limit of penalties for individual offenses of Section 1831(a) are increased from \$500,000 to \$5,000,000 and the upper limit for corporate offenses of Section 1831(b) are increased from \$10,000,000 to the greater of \$10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.



Prior to the amendment, Section 1831 provided:

(a) In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined not more than \$500,000 or imprisoned not more than 15 years, or both.



# Trading Secrets



(b) Organizations.— Any organization that commits any offense described in subsection (a) shall be fined not more than \$10,000,000.

Accordingly, the penalties for individuals have increased from \$500,000 to \$5,000,000, and the penalties for organizations have increased from \$10,000,000 to the greater of \$10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

The [Act](#) also directs the U.S. Sentencing Commission to review and amend the federal sentencing guidelines and policy statements applicable to offenses relating to the transmission of a stolen trade secret outside of the United States or economic espionage in order to reflect the intent of Congress that penalties for such offenses reflect the seriousness of, and potential and actual harm caused by, such offenses and provide adequate deterrence. It directs the Commission to: (1) consider the extent to which such guidelines and statements appropriately account for the simple misappropriation of a trade secret; (2) consider whether additional enhancements are appropriate to account for any transmission of a stolen trade secret outside of the United States and any such transmission that is committed for the benefit of a foreign government, instrumentality, or agent; and (3) ensure reasonable consistency with other relevant directives, guidelines and statements, and related federal statutes.

The President's approval of this Act comes after [his approval](#) in late December 2012 of other amendments to the Economic Espionage Act which broaden Section 1832(a) to apply to a trade secret "*that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof.*" (emphasis added).

The Department of Justice recently issued a [report](#) identifying some of its significant prosecutions under the Economic Espionage Act.

Some legal commentators, such as [John Marsh](#), believe that the bipartisan support of these amendments may provide some momentum for the passage of additional federal legislation which would provide for a civil cause of action for certain violations of the Act. In July 2012, the [Protecting American Trade Secrets and Innovation Act of 2012](#), S. 3389, which sought to federalize civil trade secret misappropriation in certain factual scenarios, was introduced in Congress, but the Senate Judiciary Committee ultimately did not act on the bill.

It remains to be seen whether the recent legislation will lead to the further strengthening of trade secret protections under federal law in 2013.

We will keep you updated on any significant new developments.



# Trading Secrets



## President Obama Signs Significant Cybersecurity Executive Order

*By Misty Blair and Ken Wilton (February 15th, 2013)*

Cybersecurity is at the forefront of the public and private sectors alike, as daily news reports warn of cyberattacks on American institutions such as [media](#), [banks](#), and [governmental agencies](#).

It is in this spirit that, just Tuesday, President Obama signed the long-awaited [Executive Order](#) on “Improving Critical Infrastructure Cybersecurity” and devoted a portion of his [State of the Union address](#) to the topic:



*America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.*

*That's why, earlier today, I signed a new executive order that will strengthen our cyber defenses by increasing information sharing, and developing standards to protect our national security, our jobs, and our privacy. Now, Congress must act as well, by passing legislation to give our government a greater capacity to secure our networks and deter attacks.*

In the Executive Order, President Obama uses his powers to direct the manner in which the federal agencies interact with the industries they regulate, and with one another, for the protection of the “Nation's critical infrastructure.” At its core, the Executive Order is based on the assumption that the more a critical infrastructure provider knows about the current threats to their systems the better and more robust the response will be. As a result, like its predecessor failed legislation, the Executive Order is intended to encourage the sharing of information regarding cyber threats among those providers.

The Executive Order defines “critical infrastructure” as those “systems and assets, whether physical or virtual, so vital to the United States that [their] incapacity or destruction... would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”

American companies should carefully consider whether they are likely to fall under the designation of “critical infrastructure,” or whether they otherwise provide goods or services to companies likely to fall under that designation, and are thus likely to be impacted by the Executive Order. Even if they do not, they may want to consider the incentives provided for participation in the voluntary information sharing programs established by the Executive Order.



# Trading Secrets



The Executive Order relies on a multi-prong approach to orchestrate the actions and interactions of the subject agencies. It is made up of a dozen individual sections, including sections:

- Directing the Department of Homeland Security (DHS), the Attorney General (AG) and the Office of the Director of National Intelligence (DNI) to work together to create a “Cybersecurity Information Sharing” program, under which these agencies will issue unclassified reports regarding specific threats and, where necessary, issue classified reports to authorized critical infrastructure entities; to expand the Enhanced Cybersecurity Services Program for voluntary information sharing among participating critical infrastructure entities and their private sector security providers; and to expedite the processing of security clearances for certain personnel of critical infrastructure entities.

- Directing federal agencies carrying out the President’s directives under the Executive Order to “ensure that privacy and civil liberties protections are incorporated into such activities”; to consider reports, issued by the DHS Privacy Officer and the DHS Officer for Civil Rights and Civil Liberties, regarding the risks to privacy and civil liberties from the agencies’ actions; and to protect information submitted by private entities “to the fullest extent permitted by law.”

- Directing the National Institute of Standards and Technology (NIST) and the Secretary of Commerce to develop a “Baseline Framework,” or “Cybersecurity Framework,” for the reduction of risks to critical infrastructure; to incorporate standards and procedures into the framework that are voluntary, proven, cost-effective, measurable, technology-neutral, adaptable to a competitive market, and applicable across sectors; to address impacts of the framework on business confidentiality, individual privacy, and civil liberties; to engage in a “Consultative Process” with other federal agencies and the public in the development of “preliminary” and “final” versions of the framework; and to update the framework as needed.

- Directing DHS and “Sector-Specific Agencies” (SSA) to establish a “Voluntary Critical Infrastructure Cybersecurity Program,” under which the owners and operators of critical infrastructure and “any other interested entities” are encouraged to adopt the Cybersecurity Framework; to coordinate establishment of incentives for participation in the program; and to report to the President regarding the benefits and effectiveness of such incentives, along with any legislation that may be required for such incentives.

- Directing DHS and SSA to identify and designate entities for which “a cybersecurity incident could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security” (excluding “commercial information technology products” and “consumer information technology services”); to engage in a “Consultative Process” with other federal agencies regarding information necessary for the designations; to allow “other relevant stakeholders” to submit information to assist in making the designations; and to confidentially notify the owners and operators of those entities designated as critical infrastructure, with a process by which the owners and operators may challenge the designation.

- Directing federal agencies responsible for regulating the security of critical infrastructure entities to engage in a “Consultative Process” with DHS and others to determine whether current cybersecurity regulations are sufficient for their agency-specific needs; to report to the President whether the agency believes it “has clear authority” to establish cybersecurity requirements; to propose actions to mitigate cyber risk if current requirements are deemed to be insufficient; and to consult with owners and operators regarding ineffective or overly burdensome requirements.

In his State of the Union address, President Obama made clear that the Executive Order is not a substitute for comprehensive cybersecurity legislation, but is instead a sort of stopgap measure



# Trading Secrets



designed to address the immediate threats faced by the Nation's most important institutions. Congress continues its long and tortured attempts at passing such legislation, as the House revisits the [Cyber Intelligence Sharing and Protection Act](#) (CISPA, re-introduced Wednesday) and the Senate considers the [Cybersecurity and American Cyber Competitiveness Act of 2013](#) (introduced in January).

Some argue that only legislation can offer the civil liability protections and other key components necessary for a successful national cybersecurity scheme. Regardless, the President has used the powers within his grasp to start putting the scheme in place. We will continue to monitor developments as the Executive Order is implemented and legislation is debated.

# Trading Secrets



## Is Massachusetts Next to Adopt the Uniform Trade Secrets Act?

*By Ryan Malloy (February 20th, 2013)*

Will Massachusetts join 46 states, District of Columbia, Puerto Rico, and the U.S. Virgin Islands in adopting the Uniform Trade Secrets Act (the “UTSA”)?

In January 2013, the Massachusetts Legislature proposed [House Bill No. 27: An Act Making Uniform the Law Regarding Trade Secrets](#). The bill seeks to repeal Sections 42 and 42A of chapter 93 of the Massachusetts General Laws and insert a form of the UTSA as chapter 93K. Only New York, Texas, North Carolina, and Massachusetts have not yet adopted the UTSA. New Jersey was the last state to adopt the UTSA last year. The bill was referred to the Joint Committee on the Judiciary on January 2, 2013, and the Massachusetts Senate concurred on February 14, 2013.



According to proponents of the bill, the adoption of the UTSA would improve fair, competitive innovation in the Commonwealth by providing enforceable rules to protect against the misappropriation of confidential information that are more inclusive and predictable than the antiquated measures currently available. Specifically, the bill seeks to replace the definitions, procedures, and remedies set forth in chapter 93A (the Massachusetts unfair competition statute) with respect to claims for misappropriation of trade secrets.

The Massachusetts bill follows the text of the 1985 Official Text of the UTSA, with modifications first developed by the Intellectual Property Committee of the Business Section of the Boston Bar Association. The bill departs from the Official Text of the UTSA in several significant ways. First, it makes clear that all types of confidential business information can be protected as a “trade secret,” but such information must derive actual or potential economic value *at the time of alleged misappropriation*. Second, only information that at all times has been the subject of reasonable efforts to give notice that it should not be and to ensure that it is not acquired, disclosed or used without the owner’s consent will benefit from trade secret status. Thus, information that is readily ascertainable from public records cannot be a trade secret and cannot be misappropriated under the bill.

The Massachusetts version of the UTSA provides for both injunctive and monetary remedies. Under the current Massachusetts Trade Secrets Act, chapter 93 § 42, and the unfair competition statute, chapter 93A, only actual damages, which may be doubled or trebled, are recoverable for the misappropriation of trade secrets. In contrast, the UTSA authorizes awards of twice the entire recovery for “willful and malicious misappropriation,” which could include “actual loss caused by misappropriation and unjust enrichment [to a competitor] caused by misappropriation that is not taken into account in computing actual loss.” In lieu of damages measured by other methods, the damages caused by misappropriation under the UTSA may be measured by the imposition of a liability for a reasonable royalty based on the unauthorized disclosure or use of a trade secret. Finally, the UTSA also provides for the recovery of attorney’s fees. The bill therefore adopts an authorization for exemplary damages that may exceed that of the current law.



# Trading Secrets



With the possibility for increased protection of confidential business information, improved predictability in the outcome of judicial proceedings, and higher financial stakes, enactment of the UTSA may soon garner increased attention from litigators in the Commonwealth. This is particularly true given the pending [non-compete legislation](#) in Massachusetts, which many expect to be passed this year.

# Trading Secrets



## Texas Considers Adopting the Uniform Trade Secrets Act

*By Randy Bruchmiller (March 12th, 2013)*

Texas, New York, North Carolina, and Massachusetts are the only states that do not subscribe to some version of the Uniform Trade Secrets Act ("UTSA").

Common law presently governs misappropriation of trade secrets lawsuits in Texas.

Legislation was [recently proposed](#) that, if enacted, would adopt a version of the UTSA for the State of Texas. The common law of Texas is very similar to the UTSA in many ways.



The biggest change that adoption of the UTSA could bring about has to do with the recovery of attorneys' fees. There is currently no basis for recovery of attorneys' fees in Texas for the misappropriation of trade secrets, absent a separate cause of action (such as breach of a confidentiality agreement or recovery under the Texas Theft Liability Act ("TTLA")).

The ability to recover attorneys' fees in trade secret cases is significant. First, these cases can easily involve attorneys' fees well into the six figure range for both the company trying to protect its trade secrets as well as the individual or company defending the lawsuit. Second, proof of actual damages can be problematic because it is difficult to put a value on a stolen trade secret or put a value on the benefit a competitor obtained from the trade secret. Some defendants successfully take the approach in litigation that, "Yes, we took it, but it did not help us [or hurt the owner or the trade secret]." Therefore, a plaintiff many times ends up spending a large amount of money only to get no damages and an injunction telling the competitor not to use the trade secret. There is significant value in getting the injunction, but there would be more value if the plaintiff could also get its attorneys' fees.

It is not entirely clear how the attorneys' fees provisions of the UTSA, if enacted, would be enforced in Texas. The proposed legislation allows only a "prevailing party" to recover under certain circumstances. It is unclear whether obtaining an injunction and no actual damages would be sufficient to allow someone to be a prevailing party, which it is not under the TTLA. In addition to being a prevailing party, one of the following must also be true: (1) a claim for misappropriation is made in bad faith; (2) a motion to terminate an injunction is made or resisted in bad faith; or (3) willful and malicious misappropriation exists.

There are a few other provisions worth highlighting from the proposed legislation. The proposed legislation in Texas provides for a presumption in favor of granting protective orders to preserve the secrecy of trade secrets during the pending litigation. This change could do away with occasional disputes over whether to enter a protective order, which many attorneys in trade secret litigation now agree to put in place without the need for court intervention. The proposed statutory language also provides that reverse engineering is allowed in certain circumstances, which is also true under Texas common law. Finally, the proposed statutory language departs from the model UTSA and Texas common law by specifically including customer lists in the definition of a trade secret. Under Texas





# Trading Secrets



common law, some customer lists and other compilations of information are considered proprietary, but a fact intensive inquiry is involved to determine if a specific list is worthy of trade secret protection.

For more information and analysis on the proposed legislation please see the excellent articles from [Law360](#) and [John Marsh](#).

We will keep you posted on this proposed legislation.



# Trading Secrets

## Utah, New Mexico, and Arkansas Pass Social Media Legislation Restricting Employer Access to Personal Social Media Accounts

*By Robert Milligan and Jessica Mendelson (April 23rd, 2013)*

Social media legislation restricting access to personal social media accounts has been a hot topic in recent months, and as 2013 progresses, more and more states seem poised to pass such legislation. Here's a roundup of some of the more recent social media legislation passed in Utah, New Mexico, and Arkansas:



### Utah

With the passage of the Internet Employment Privacy Act (IEPA) last month, [Utah became the fifth state in the country](#) to pass legislation restricting employers' access to their employees' social media accounts. Under the terms of the legislation, neither public nor private employers [can](#) "ask an employee or job applicant to disclose a username and password or a password that allows access to the employee's or applicant's personal Internet account" or retaliate against an employee or job applicant who fails to disclose such information. However, employers [can still](#) request the disclosure of account information to gain access to the employer's "electronic communications device, account or service." Employers can also investigate employee misconduct involving an employee's personal email account, restrict or prohibit access to certain website on the employer's devices or networks, and block certain access and communications on the employer's device or network. Employers are also still entitled to screen employees and job applicants. The law also provides penalties for failure to comply: employees and job applicants are entitled to up to \$500 in damages from employers for violations of the law.

### New Mexico

With the [passage](#) of [SB 371](#), New Mexico joined a handful of others states to impose restrictions on employers' access to social networking accounts. Under this law, which was signed by Governor Susana Martinez on April 5, an employer is prohibited from requesting or demanding access to a job applicant's social networking account. However, unlike similar laws passed in other states, such as [California](#), [Illinois](#), [Maryland](#), [Michigan](#), and Utah, New Mexico's law does not prohibit employers from accessing the accounts of current employees. Furthermore, the law does not prohibit employers from instituting workplace restrictions on access to the internet or social media websites, nor does it restrict an employer's right to view information found in the public domain.

The legislation prohibits an employer from requesting or demanding a job applicant divulge a password to allow access to his or her social networking accounts or from demanding access to such accounts in any other manner. There are, however, exceptions to this rule. Employers can still monitor the usage of company electronic equipment or email without requesting or requiring a prospective employee to provide a password.



# Trading Secrets



New Mexico's law [does not](#) contain a remedial plan for damages or penalties. The New Mexico law will take effect on June 14, 2013.

## **Arkansas**

On April 22, 2013, Arkansas' governor signed [Act 1480](#), a law which prohibits an employer from requiring or requesting a current or prospective employee from disclosing his or her username or password for a social media account to provide access to the contents. However, the Act does not regulate the following types of social media accounts: (1) accounts opened by employees at their employer's request, (2) accounts provided to an employee by an employer, (3) accounts setup on behalf of an employer, or (4) accounts setup to impersonate an employer. Employers are prohibited from requesting, requiring, suggesting, or causing current or prospective employees to disclose their usernames and passwords, adding employees or supervisors to their social media contacts, or changing privacy settings. Employers are not liable for inadvertently receiving such information, and employers are entitled to obtain such information if it is reasonably believed to be relevant to a formal investigation of allegations of the employee's breach of federal, state, or local laws or the employer's written policies.

## **Conclusion**

As of April 2013, [thirty-five states](#) were considering (or had already introduced) social media legislation. States throughout the country are currently considering this hot topic, and we will likely see additional states pass similar social media legislation before the year is out. [Social media legislation](#) has been submitted to Governor Christie in New Jersey for signature. We have previously provided our critique of this [type of legislation](#), and we will continue to notify you of future developments.

# Trading Secrets



## Federal Legislation Proposed To Combat Cyber-Espionage

*By Jessica Mendelson (June 14th, 2013)*

Cybersecurity has become a growing concern in the United States. Legislation impacting this topic covers a variety of fields, including national security and defense, trade and international relations, intellectual property, and even privacy and civil liberties. As technology is constantly changing, so too are the types of restrictions in place.



A group of prominent American Senators recently introduced the [Deter Cyber Theft Act](#), a bill designed to reduce the threat of foreign cyber-espionage and trade secret theft. The bill is a bipartisan effort, sponsored by Carl Levin, John McCain, Jay Rockefeller, and Tom Coburn. The proposed legislation would create a registry of stolen technology and also provide for punitives for foreign firms attempting to sell products which make use of this stolen technology. The bill would require the Director of National Intelligence to provide annual reports regarding trade secret theft, and countries and individuals involved in cyber-espionage or trade secret theft. The Director of National Intelligence's records would also include a list of the worst offenders, as well as the particular technologies targeted by espionage. Furthermore, the [report would list](#) countries and companies which "benefitted from the theft and the action taken by the U.S. government to combat cyber espionage." The President would also be [required](#) to block those imports that involve the use of stolen American technology or made by "state-owned enterprises of nations on the DNI's priority watch list that are similar to items identified as being made using stolen technology."

According to [Senator Levin's official announcement](#), this act would combat "the theft of valuable intellectual property from U.S. companies, which invest billions every year in research and development, only to be targeted by foreign countries and companies that illegally access valuable data and then use it to compete against American companies and workers." Senator McCain [adds](#), "Some foreign governments, businesses and state-owned enterprises are today using cyber-espionage to steal American intellectual property and rob US ingenuity and innovation in order to gain competitive advantage. This kills American jobs, undermines the competitiveness of our businesses and compromises US economic and national security interests, and it must stop now."

The introduction of the legislation follows the recent release of a Pentagon report [discussing](#) "the links between the Chinese government and military" and recent cyber thefts of American trade secrets. [According to](#) the Pentagon report, these cyber attacks "appear to be attributable directly to the Chinese government and military" and the stolen information "could potentially be used to benefit China's defense industry, high-technology industries, [and] policymaker[s]". China has denied involvement, however, independent forensic evidence has [suggested otherwise](#). Although the American government has utilized diplomacy to address the Chinese government's involvement in cyber attacks, hacker occupations continue.

A similar bill was recently [introduced](#) in the House of Representatives. The House bill is intended to go after hackers from "offending nations" with "real consequences and punishments." The bill was recently introduced to the House of Representatives Intelligence Committee by Representatives Mike



# Trading Secrets



Rogers, Tim Ryan and Ron Johnson. While both bills are still in the early stages, we will continue to keep you updated regarding both bills as they progress through the Legislature.

# Trading Secrets



## Representative Zoe Lofgren Introduces Bill to Create Private Civil Claim for Trade Secrets Theft Under the Economic Espionage Act

*By Josh Salinas and Robert Milligan (June 26th, 2013)*

Representative Zoe Lofgren (D- CA) has been very active in the technology and innovation legislation space of late. Last week, Representative Lofgren and Senator Ron Wyden (D-OR) [formally introduced companion bills](#), nicknamed “Aaron’s Law,” in the House and Senate seeking to amend the Computer Fraud and Abuse Act. Almost unnoticed was the fact that Representative Lofgren also introduced last week a potentially significant bill that would provide a private civil claim for trade secrets theft under the Economic Espionage Act (“EEA”).



Specifically, Representative Lofgren introduced H.R. 2466, which is titled “[Private Right of Action Against Theft of Trade Secrets Act of 2013](#)” (“PRATSA”). Similar to the [PATRIA](#) legislation that was proposed last year, PRATSA provides a private civil action for trade secrets theft by amending the EEA.

PRATSA is much simpler than PATRIA, however, and adds only the following two subsections to [18 U.S.C. Section 1832](#):

‘(c) Any person who suffers injury by reason of a violation of this section may maintain a civil action against the violator to obtain appropriate compensatory damages and injunctive relief or other equitable relief. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

‘(d) For purposes of this section, the term ‘without authorization’ shall not mean independent derivation or working backwards from a lawfully obtained known product or service to divine the process which aided its development or manufacture.’

Section 1832 presently provides:

(a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;





# Trading Secrets



(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy, shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than \$5,000,000.

PRATSA has some key distinctions from PATSIA:

(1) it does not require a complaint describing in specificity reasonable secrecy measures or a declaration regarding the substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country;

(2) it does not provide for civil ex parte seizure orders;

(3) the statute of limitations is two years, not three;

(4) it provides for a more narrow civil claim by just providing a claim for a violation of Section 1832 rather than a violation of Section 1831 or a stand-alone misappropriation claim (e.g. a misappropriation of a trade secret that is related to or included in a product that is produced for or placed in interstate or foreign commerce); and

(5) it does not provide for a comprehensive list of remedies such as exemplary damages or attorneys' fees.

These deviations may help PRATSA where PATSIA struggled as some members of the legal community [contested](#) some of PATSIA's provisions, including the definition of nationwide service of process and the scope and procedures regarding [ex parte seizure orders](#).

It is important to recognize that by amending the EEA, PRATSA may inherently lead to conflicts with state trade secret laws. In particular, [Section 1838](#) provides that the EEA "shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret...." Thus, a trade secret holder could potential bring claims under both their state's respective trade secret laws and the EEA.

One benefit of PRATSA is that it attempts to resolve a deficiency under the current EEA. Specifically, PRATSA expressly exempts "reverse engineering" from violation of Section 1832. While the legislative history of the EEA suggests that traditional defenses available in a civil action for theft of trade secrets



# Trading Secrets



are equally applicable to a criminal violation, the EEA's lack of specific language providing for a reverse engineering defense has troubled some commentators because the statute arguably implicates certain reverse engineering activities previously thought to be lawful. Regardless of its amendment for a private civil claim, PRATSA's reverse engineering exemption will provide clarity to the existing statute.

Finally, one important implication of providing a private civil claim under the EEA is the extraterritoriality provision in [Section 1837](#), which provides that the EEA also applies to conduct occurring outside the United States if the offender is a (a) citizen or permanent resident alien of U.S., or (b) organization organized under U.S. law. This may strengthen companies' abilities to protect against trade secrets theft to or for foreign individuals, companies or governments provided either of these above requirements are satisfied. In the criminal context, however, prosecutors have recently struggled in [effectuating service of process over foreign companies](#) under the Federal Criminal Rules of Procedure. Accordingly, additional modifications may be needed to this proposed legislation to ensure that it adequately addresses the threat posed to U.S. companies by foreign trade secret theft.

After a first reading of the proposed bill and recognizing it is likely a work in progress, we like PRATSA, particularly if it is modified to include Section 1831 claims in addition to Section 1832 claims (as well as possibly a stand-alone misappropriation claim), appropriate remedies (e.g. exemplary damages and attorneys' fees), and it more adequately addresses trade secret theft by foreign actors. Its simple approach may contribute to its success. It left alone a lot of the hotly debated provisions from PATSIA upon which many legal commentators were unable to reach an agreement. Yet, PRATSA's true value lies in its potential to provide a private civil claim for trade secret theft in federal court which may have certain advantages over state court, such as the ability to obtain discovery through the federal subpoena power and the potential to more adequately address trade secret theft by foreign individuals, companies, or governments.

# Trading Secrets



## Texas Uniform Trade Secrets Act Now Applicable

*By Randy Bruchmiller (September 2nd, 2013)*

Texas recently [adopted](#) a version of the Uniform Trade Secrets Act ("UTSA"). The new act will be known as the [Texas Uniform Trade Secrets Act](#) ("TUTSA"). New York and Massachusetts are now the only two states to not adopt some form or variation of the UTSA.

The TUTSA takes effect during the Labor Day weekend on September 1, 2013. However, the TUTSA does not necessarily apply to all cases filed in Texas after September 1, 2013. The TUTSA applies only if the alleged misappropriation began on or after September 1, 2013. Any misappropriation or continuing misappropriation that began before September 1, 2013 will continue to be governed by Texas common law.



I highlighted the most significant changes in my [prior blog post](#) that was made while the new law was being considered. As previously discussed, the ability to obtain attorneys' fees in trade secrets cases is the change that will have the greatest impact on litigants. Another significant change is that there will be a presumption that a protective order needs to be put in place by the trial court to protect the trade secrets at issue in the litigation. Both of these changes provide increased protection for businesses because they allow businesses to protect their trade secrets at a lower cost (if they can recover their attorneys' fees) and keep the trade secrets from being divulged when they bring litigation.

Please see my prior [blog post](#) for more information regarding the details of the TUTSA, which specifically discusses the scenarios when an attorneys' fee award is possible.

We will keep you posted of any material cases discussing the new TUTSA.

# Trading Secrets



## Texas Changes Law To Strengthen The Ability Of Companies To Protect Their Information

*By Randy Bruchmiller (September 18th, 2013)*

Until recently, Texas common law governed misappropriation of trade secrets lawsuits in Texas. That changed when the 2013 Texas legislature adopted a version of the Uniform Trade Secrets Act ("UTSA"). The new act is known as the Texas Uniform Trade Secrets Act ("TUTSA"). New York and Massachusetts are now the only two states to not adopt some form or variation of the UTSA.

Trade secret laws protect companies from having their confidential information stolen and used by competitors. The most common way information is taken by a competitor is when an employee leaves one company and takes significant information, either in hard-copy or saved electronically, to the competitor. The confidential information taken may include items like customer lists, financial data, proprietary information about new projects, sales and marketing strategies and the like. Trade secret laws generally protect any formula, pattern, device, or compilation of information used in the company's trade or business that gives the company a competitive advantage over those who do not know or use it and that is in fact a secret.



### The Major Changes

**Customer Lists Protected** – The new statutory language departs from the model UTSA and Texas common law by specifically including customer lists in the definition of a trade secret. Under Texas common law, some customer lists and other compilations of information are considered proprietary, but a fact intensive inquiry is involved to determine if a specific list is worthy of trade secret protection. Most customer lists should qualify for trade secret protection under the TUTSA so long as reasonable efforts are taken to maintain their secrecy and so long as the lists are not readily ascertainable by proper means.

**Recovery of Attorneys' Fees** – The ability to obtain attorneys' fees in trade secrets cases is the change that will likely have the greatest impact on litigants. Prior to the TUTSA, there was no basis for recovery of attorneys' fees in Texas for the misappropriation of trade secrets, absent a separate cause of action authorizing an award of attorneys' fees (such as breach of a confidentiality agreement or recovery under the Texas Theft Liability Act ("TTLA")).

The ability to recover attorneys' fees in trade secret cases is significant. First, these cases can easily involve attorneys' fees well into the six figure range for both the company trying to protect its trade secrets as well as the individual or company defending the lawsuit. Second, proof of actual damages can be problematic because it is difficult to put a value on a stolen trade secret or put a value on the benefit a competitor obtained from the trade secret. Some defendants successfully take the approach in litigation that, "Yes, we took it, but it did not help us [or hurt the owner or the trade secret]." Therefore, a plaintiff many times ends up spending a large amount of money only to get no damages.



# Trading Secrets

and an injunction telling the competitor not to use the trade secret. There is significant value in getting the injunction, but there is more value now that the plaintiff can also get its attorneys' fees.

It is not yet entirely clear how the attorneys' fees provisions of the TUTSA will be enforced in Texas. The new law allows only a "prevailing party" to recover under certain circumstances. It is unclear whether obtaining an injunction and no actual damages will be sufficient to allow someone to be a prevailing party, which it is not under the TTLA. In addition to being a prevailing party, one of the following must also be true: (1) a claim for misappropriation is made in bad faith; (2) a motion to terminate an injunction is made or resisted in bad faith; or (3) willful and malicious misappropriation exists.

**Protective Orders** – There are a few other provisions in the new law that are worth highlighting. There is now a presumption that a protective order needs to be put in place by the trial court to protect the trade secrets at issue in the litigation. The new law provides for a presumption in favor of granting protective orders to preserve the secrecy of trade secrets during the pending litigation. This change should do away with occasional disputes over whether to enter a protective order, which many attorneys in trade secret litigation now agree to put in place without the need for court intervention.

**Reverse Engineering** – The statutory language also provides that information obtained by reverse engineering does not meet the definition of a trade secret in certain circumstances, which was also true under Texas common law. Reverse engineering is defined under the statute as "the process of studying, analyzing, or disassembling a product or device to discover its design, structure, construction, or source code provided that the produce or device was acquired lawfully or from a person having the legal right to convey it." There are situations when reverse engineering is not allowed, such as when there is a patent or other protections for the product or information.

These changes provide increased protection for businesses because they allow businesses to protect their trade secrets at a lower cost (if they can recover their attorneys' fees) and keep the trade secrets from being divulged when they bring litigation.

## **When The New Law Applies**

The TUTSA took effect during the Labor Day weekend on September 1, 2013. However, the TUTSA does not necessarily apply to all cases filed in Texas after September 1, 2013. The TUTSA applies only if the alleged misappropriation began on or after September 1, 2013. Any misappropriation or continuing misappropriation that began before September 1, 2013 will continue to be governed by Texas common law.

## **General Practices Regarding Trade Secrets**

### **Practices to Consider To Protect Information**

There are many ways to protect your confidential information. For example, a company can:

- Make all confidential information password protected.
- Make access to highly sensitive information restricted to only those specific employees in the company that need it to carry out their job functions.



# Trading Secrets



- Have employees enter into agreements with the company such as confidentiality agreements, non-competition agreements and/or IP assignment and protection agreements.

There are many more practices and technological solutions available that can help a company protect the company's confidential information. Seyfarth Shaw LLP regularly provides trade secrets audits of the confidential information policies and practices of companies in order to better assist them in protecting their information.

## **Practices to Consider When Hiring Employees**

In addition to protecting the company's own information, companies want to make sure they do not end up being a defendant in a trade secrets lawsuit. These are a few general practices that should be considered:

- Make it clear to job candidates that the company is not interested in information from the competitor.
- Tell prospective employees that they are forbidden from bringing information from their prior employment and also forbidden from using a prior employer's confidential information.
- Make sure that prospective employees are not subject to a non-competition or non-solicitation agreement with a prior employer that inhibits their ability to work for the company.



# Trading Secrets



## Obama Administration Releases Draft Voluntary Cybersecurity Framework for U.S. Business

*By John Tomaszewski (October 28th, 2013)*

The U.S. Department of Commerce's National Institute of Standards and Technology (NIST) released its [draft](#) of a voluntary cybersecurity framework last Tuesday that provides a means to better evaluate cyber risk, and prepare better defenses against ever-increasing online attacks.



[NIST's "Preliminary Cybersecurity Framework"](#), to be finalized in February 2014 after a period for public comment, originated with Executive Order 13636 from President Barack Obama, which identified cyber threats to critical infrastructure as "one of the most serious national security challenges". The Executive Order specified that NIST should produce a framework document. The new framework sets out specific steps and best practices for organizations of all sizes so they can better protect the country's critical infrastructure.

However, protecting the country's critical infrastructure isn't the only use of this Framework. With the pervasiveness of cyber-threats to a company's information assets, officers and directors of companies who rely heavily on those assets have a duty to protect them. The challenge is that while the security knowledge domain is fairly mature and robust, that knowledge domain is normally not in the Board or C-Suite. Consequently, it is difficult for business leaders and management to effectively understand what risks they face and how they might be able to mitigate them.

The government's document sets out a risk-based approach to understanding and mitigating cyber-threats. IT starts by outlining five basic functions for security strategies: identify, protect, detect, respond, and recover. This serves as a model that companies can use to tailor to their own, more specific cybersecurity response strategies. The framework sets out standards and best practices at a high level, but it remains up to companies and their cybersecurity teams to create their own risk profiles and determine what are the gravest threats they face.

The framework is a good start. In structure, it resembles other business oriented risk matrices. The framework is broken into a "Core" (the desired outcomes of any strategy) a "Profile" (a means to describe the current state of the strategy, and the desired target state – thus allowing for an easy gap analysis), and "Tiers" (a description of the maturity level of the strategy). These three components of the framework give a common language for non-security business leaders to discuss and address cybersecurity.

The framework does have some limitations. Currently, the content which comes bundled in the framework doesn't fully explore the heavily interconnected nature of modern business and technology delivery models. Traditionally, business or technology delivery were "point-to-point" (e.g. you bought a computer, or you received a service from, \*a\* company. You knew who you were dealing with at any given point in a transaction). Now, most businesses have a multi-layered delivery model – even for hard goods like phones and network gear.



# Trading Secrets



Consequently, supply-chain management is much more a risk vector than it has been in the past. Any security framework will need to recognize this ecosystem and provide techniques to deal with it. At present, additional content will need to be added to the Framework to take into account the non-linear and multi-layer delivery models of a public or hybrid cloud service provider.

Regardless, the Framework gives a good starting point for a “management-friendly” tool to attack the risks inherent in the information age. Historically, an “ideology of plausible deniability” seemed to be the norm in board rooms. This is no longer the case. The minimum standards of care established by the government’s plan help show that information security is a risk that needs to be managed just like financial reporting. At the end of the day, this may lead to an increase in class actions against companies over their real or perceived cybersecurity shortcomings. It is not merely an issue left to the folks in IT – it is now a Board responsibility, and this Framework actually does provide a good starting point for the Board to take up that responsibility.



# Trading Secrets



## International

# Trading Secrets



## International Update: Recent Decisions by UK Courts Highlight Protection of Confidential and Proprietary Information in Employment Context — Part I

*By Daniel Hart, Peter Talibart and Georgina McAdam (August 5th, 2013)*

As many employers have experienced, guarding against misuse of confidential and proprietary information by former employees can be a challenge in an increasingly digitalized and globalized marketplace. For companies with operations in the United Kingdom, recent court decisions provide some helpful guidance on protecting confidential and proprietary information in the international context.



Earlier this year, the relatively new [Supreme Court of the United Kingdom](#) (which has been in operation since only 2009) addressed whether a former employee can be liable for breach of confidence for starting a competitive business with others who, unbeknownst to the former employee, have misused the former employer's confidential information. In [Vestergaard Frandsen and others v. Bestnet Europe Ltd. and others, \[2013\] UKSC 31](#), the Supreme Court held that a former employee cannot be held liable for breach of confidence in such a scenario in the absence of evidence that the former employee was aware of the confidential information or its misuse.

The *Vestergaard* case involved a former employee of Vestergaard, one Mrs. Sig, who left her employment with Vestergaard (a manufacturer of insecticidal fabrics for mosquito nets) to start a competing business in Denmark with another former employee of Vestergaard, Mr. Larsen, and a former consultant for Vestergaard, Dr. Skovmand. Although Dr. Skovmand had no formal service contract with Vestergaard, both Sig and Larsen were subject to employment agreements with Vestergaard containing covenants requiring them to maintain the confidentiality of Vestergaard's confidential information and trade secrets.

After Vestergaard initiated legal proceedings in Denmark against Sig, Larsen, Skovmand, and their new company, Sig resigned from the board of the Danish company but immediately set up two new English companies to conduct the same business, through which Sig marketed a competing product designed by Skovmand that, unbeknownst to Sig, incorporated Vestergaard's trade secrets. Thereafter, Vestergaard initiated legal proceedings in England against Sig, Larsen, and the two new English companies.

Following a 16-day hearing, a judge in the Chancery Division of the High Court (one of the major courts for civil business litigation in England and Wales) ruled against the defendants. Although Skovmand was not a party to those proceedings, the High Court judge (Arnold J) found that Skovmand had used Vestergaard's trade secrets to develop the competing product and that Larsen was aware of Skovmand's use of Vestergaard's trade secrets. Moreover, the High Court judge found that Skovmand and Larsen had put forward false evidence including forged documents. In contrast, the High Court judge accepted Sig's explanation that she did not have access to or knowledge of the trade secrets of Vestergaard that Skovmand misappropriated, did not know that Skovmand had developed the competing products using Vestergaard's trade secrets, and had no involvement in the forged



# Trading Secrets



documents that Skovmand and Larsen had presented. Nevertheless, the High Court judge still found Sig liable for breach of confidence, explaining that “[a] person can be liable for breach of confidence even if he is not conscious of the fact that what he is doing amounts to misuse of confidential information.” Sig appealed to the Court of Appeal, which disagreed and reversed the judgment of the High Court judge, reasoning that Sig could not be liable for breach of confidence, as imposing liability on Sig in this situation would amount to strict liability.

On appeal by Vestergaard, the Supreme Court agreed with the Court of Appeal. In an opinion given by Lord Justice Neuberger (with which four other justices agreed), the Supreme Court held that Sig could not be liable for breaching Vestergaard’s rights of confidence through the misuse of trade secrets because (i) she did not know the identity of the trade secrets and (ii) did not know that they were being, or had been used, let alone misused. Although Sig’s employment contract contained a nondisclosure covenant, the Supreme Court reasoned that the nondisclosure covenant was irrelevant because the information in question was not information that Sig gained in the course of her employment with Vestergaard but, rather, was information that Skovmand had gained in the course of his consultancy for Vestergaard. There was no implied term into Sig’s employment contract that she would not assist others to abuse Vestergaard’s trade secrets when she did not know the trade secrets and was unaware they were being misused. This was wrong in principle, as it is (i) inconsistent with the express terms of Sig’s contract of employment, (ii) unnecessary to give the employment contract effect, and (iii) almost penal in nature. Likewise, the Supreme Court reasoned that, although individuals can be liable for breach of confidence through a common design with others, Sig could not be liable under such a theory given her state of mind and lack of knowledge of the features of the design which make it wrong. Moreover, although Vestergaard argued that Sig had “blind-eye knowledge” of the trade secrets and must have understood that she was “playing with fire” when her company employed Skovmand to design the competing product, the Supreme Court rejected this argument because there was no evidence that Sig had acted dishonestly. Accordingly, the Supreme Court dismissed Vestergaard’s appeal.

Because the Supreme Court is the highest court of appeals in the UK for civil matters, the Supreme Court’s decision in *Vestergaard* is particularly notable and is binding precedent throughout the UK, including Scotland and Northern Ireland (whose judicial systems are largely separate from those in England and Wales). In the wake of the decision, it is now clear that employers in the UK who assert claims for breach of confidence against former employees based on misuse of confidential information must prove that the former employee either personally misused the confidential information in question or received confidential information from another person with the knowledge that the other person had obtained the information unlawfully. To provide a stronger platform for recovery against former employees, employers should consider inserting clauses in UK employment contracts (and restrictive covenants in US proprietary information agreements) that impose on employees an affirmative obligation to (i) inform new employers (or others with whom they are acting in concert) of their continuing obligations to their former employer and (ii) to refrain from assisting others in misusing their former employer’s trade secrets and confidential information.

In Part II of this post, we will focus on recent decisions from two lower courts in England and Wales that provide other helpful guidance to employers in protecting their confidential and proprietary information.

*With its international platform and offices in the United States, United Kingdom, China, and Australia, Seyfarth Shaw’s experienced team of lawyers assists companies with large multi-jurisdictional employment law projects of a strategic, compliance and transactional nature, including issues involving noncompetes and trade secrets. If you have any questions about the above, please contact Peter Talibart in the Firm’s London Office or your Seyfarth attorney.*

# Trading Secrets



## International Update: Recent Decisions by UK Courts Highlight Protection of Confidential and Proprietary Information in Employment Context — Part II

By Daniel Hart, Peter Talibart and Georgina McAdam (August 6th, 2013)

In [Part I](#) of this post, we focused on the UK Supreme Court's recent decision in [Vestergaard Frandsen and others v. Bestnet Europe Ltd. and others](#), [2013] UKSC 31.

Although not binding authorities throughout the UK, two other recent decisions from lower courts in England and Wales are also notable with respect to employers' protection of confidential or proprietary information in relation to former employees, particularly in the international context.

First, the Court of Appeal's recent judgment in [Fairstar Heavy Transport N.V. v. Adkins](#), [2013] EWCA Civ 886, provides a notable illustration of an employer's right to access emails relating to its business affairs that are in the possession of a former agent, even when those emails are stored on the former agent's home computer.



In keeping with the multi-national context in which many businesses operate, Fairstar, a Dutch company, employed Adkins, an American citizen living in England, as its CEO. Although no express contract of employment existed between Fairstar and Adkins, Fairstar contracted for Adkins's services under a written agreement with a company controlled by Adkins and registered in Jersey. (For our readers in the Garden State, that's the Crown Dependency in the English Channel, not the home of Bon Jovi and Tony Soprano.) Following the termination of Adkins's appointment as CEO, Fairstar initiated legal proceedings against Adkins in England, seeking access to the business-related emails on Adkins's personal computer in England.

Following a hearing, a High Court judge granted judgment for Adkins, reasoning that Fairstar did not have a "proprietary right" to the emails on Adkins's home computer under English law. On appeal by Fairstar, the Court of Appeal overturned the High Court's decision. The principal judgment given by Mummery LJ. As the Court of Appeal reasoned, the issue of whether Fairstar had a "proprietary right" to the emails on Adkins's home computer was irrelevant. Rather, the central issue in the case was Adkins's agency relationship with Fairstar and its attendant legal obligations. According to the Court of Appeal, because Adkins was an agent of Fairstar, Fairstar, as principal, was entitled to require its agent to provide it with documents relating to its affairs, regardless of whether those documents resided on his home computer and regardless of whether the emails were "confidential." Accordingly, the Court of Appeal concluded that the High Court judge should have issued an order for inspection of the emails on Adkins's computer.

The *Fairstar* case well illustrates a remedy that employers can seek documents/emails where their former agents are in possession of emails and other documents that they created in the course of their relationship with the company. While it is always prudent to include clauses requiring the return of company property in any employment or agency contract, *Fairstar* is valuable precedent for companies





# Trading Secrets



who seek the return of company-related emails and other documents from their agents even in situations where no such return-of-property clause exists.

Second, the recent order from the High Court's Chancery Division in [\*Whitmar Publications Ltd. v. Gamage & Ors.\* \[2013\] WHC 1881 \(Ch\)](#) provides a helpful example of the factors that English courts consider when considering requests for injunctive relief against former employees who are alleged to have taken steps to compete with their employer while they were still employees. In that case, Whitmar, a publishing company, sought an interlocutory (i.e., preliminary) injunction against three former employees who had set up a competing company that Whitmar believed the employees had set-up while still employed by Whitmar.

At the hearing on its application for an injunction, Whitmar presented evidence that the former employees took impermissible "preparatory steps" to compete with Whitmar while still employed by Whitmar, including creating a new business entity of which they became shareholders and directors, identifying premises for the new business in the same town as Whitmar, and registering an internet domain name. In addition, Whitmar presented evidence that the former employees solicited two Whitmar employees to join their new venture, solicited business from Whitmar's clients, misrepresented their intentions to Whitmar, informed an industry colleague that they would be setting up a competing business, removed a large number of business cards that they had obtained during their employment with Whitmar and then returned the business cards only after surreptitiously copying them, and used Linked-In contact information that they had gathered for Whitmar during their employment.

Issuing an order in favor of Whitmar, Peter Leaver QC, sitting as Deputy Judge of the High Court, concluded that, based on the preliminary evidence presented by Whitmar, Whitmar was entitled to injunctive relief. American lawyers may be familiar with the standard for obtaining a preliminary injunction under the Federal Rules of Civil Procedure, which generally requires the movant to show: (1) a substantial likelihood of success on the merits; (2) irreparable harm to the plaintiff unless the injunction issues; (3) that the threatened injury to the plaintiff outweighs the harm to the defendant if the injunction issues; and (4) that the injunction will not disserve the public interest. See, e.g., *Ferrero v. Associated Materials, Inc.*, 923 F.2d 1441, 1448 (11th Cir. 1991). Under English law, the standard for granting an interlocutory injunction is similar, requiring the court to determine, as Peter Leaver QC articulated, "first . . . whether or not there is a serious issue to be tried, and, if there is, whether damages would be an adequate remedy, or whether the balance of convenience is in favour of granting the injunction sought."

Applying these factors, Peter Leaver QC reasoned that, although he could only make a "preliminary assessment," he had "no doubt that, looking at the evidence as a whole, there was a strong case that the Defendants were taking steps to compete against Whitmar for over a year. The steps that they were taking were not just preparatory steps. They were steps taken with more than just the intention to set up another company. They were active steps to compete." Moreover, Peter Leaver QC observed that "[o]ne of the badges of competition in cases such as this is the secrecy with which those who are competing go about their business" and noted evidence in the record reflecting the former employees' attempts to hide their activities. Accordingly, Peter Leaver QC held that Whitmar had a "very good chance" of succeeding at trial and granted Whitmar's application for injunctive relief.

The *Whitmar* decision provides a helpful example of the type of evidence that can warrant injunctive relief under English law. As in any jurisdiction, employers with operations in the UK should take proactive and timely measures to investigate the activities of former employees who may be engaged in competition and consult with their legal counsel about appropriate litigation or non-litigation strategies to deter misuse of confidential or proprietary information.



# Trading Secrets



*With its international platform and offices in the United States, United Kingdom, China, and Australia, Seyfarth Shaw's experienced team of lawyers assists companies with large multi-jurisdictional employment law projects of a strategic, compliance and transactional nature, including issues involving noncompetes and trade secrets. If you have any questions about the above, please contact Peter Talibart in the Firm's London Office or your Seyfarth attorney.*



# Trading Secrets



## AMSC/Sinovel Industrial Espionage Thriller Takes a Procedural Detour, Threatening U.S. Criminal Prosecution

*By Justin Beyer (September 9th, 2013)*

In a story that Hollywood would love to script, the U.S. Government charged Sinovel and its executives with soliciting the then-head of the Automation Engineering Department of AMSC's Austrian subsidiary, AMSC Windtec GmbH, to steal AMSC's source code in order that Sinovel might bypass a commercial relationship with AMSC and utilize AMSC's trade secrets without paying for ongoing software licenses.



On June 27, 2013, a grand jury in the United States District Court for the Western District of Wisconsin charged Chinese-wind-turbine-manufacturer Sinovel Wind Group Co., Ltd. ("Sinovel"), two of its high-ranking executives, Su Liying and Zhao Haichun, and a former high-level AMSC engineer, Dejan Karabasevic, of conspiring to steal and actually stealing AMSC's trade secrets, engaging in criminal copyright infringement, and engaging in wire fraud. The following facts are taken from the United States' complaint and indictment.

AMSC, formerly known as American Superconductor, Inc., is a Delaware corporation, headquartered in Massachusetts. AMSC's core business is the development, support, and production of equipment and software for wind turbines and electrical grids. Amongst its products is software utilized to regulate the flow of electricity from wind turbines to electrical grids. One issue over which wind turbine manufacturers have had to overcome in this emerging technology is how to maintain operation when a temporary sag or dip in the flow of electricity occurs over the electrical grid. Attempting to solve that issue, AMSC developed its Low Voltage Ride Through (LVRT) software, which it licensed to, among other companies, Sinovel. Sinovel sold and serviced wind turbines worldwide, including in China and the United States.

Until March 2011, Sinovel purchased software and equipment from AMSC. At that point, Sinovel owed AMSC over 100 million dollars and had contracted with AMSC to purchase another 700 million dollars' worth of AMSC software, products, and services in the future. [See, e.g., Daniel Cusick, Chinese wind power giant faces U.S. indictment on economic espionage charges, Environment & Energy Publishing \(August 22, 2013, 9:23 a.m.\)](#)

In March 2011, without prior warning, Sinovel suddenly ceased accepting products from AMSC. Around the same time, specifically on March 10, 2011, Karabasevic submitted his resignation to AMSC, which was accepted on March 11, 2011. Karabasevic's final day with AMSC was June 30, 2011.

In June 2011, while servicing wind turbines in China, AMSC engineers discovered that Sinovel was utilizing a version of AMSC's LVRT software in a wind turbine in China, software which AMSC had not sold or licensed to Sinovel. Notably, fearing international espionage and unauthorized use of its software, AMSC previously developed an encryption code to prevent unauthorized use and a separate software code allowing only a two-week trial period of the software before the LVRT software stopped functioning. Inspecting the code more closely, AMSC determined that the code had been modified in



# Trading Secrets



two particular ways: (1) bypassing the encryption code by deactivating it; and (2) disabling the two-week test period software-use limitation.

Within the following weeks, AMSC investigated the activities of Karabasevic—in some instances utilizing a private investigative firm—discovering a host of email and Skype communications between Karabasevic and various Sinovel employees. Those communications outlined a plan between Sinovel and Karabasevic whereby Karabasevic would download, provide, and, when necessary, modify and/or repair the AMSC LVRT software to work within Sinovel's turbines. For his work, Sinovel and Karabasevic agreed to a six-year, \$1.7 million dollar contract, beginning in May 2011, which also allegedly included Sinovel providing Karabasevic with a Beijing apartment and sending funds to Karabasevic's girlfriend in August 2011, a month before Karabasevic was convicted by an Austrian court of industrial espionage in September 2011. [See, e.g., Carl Sears and Michael Isikoff, Chinese firm paid insider 'to kill my company,' American CEO says, NBC News \(September 9, 2013, 3:31 p.m.\)](#) Karabasevic was confronted by AMSC on June 30, 2011, and provided a signed statement on July 28, 2011. In his statement, Karabasevic admitted to the above. Karabasevic also gave written permission to search the Beijing apartment secured for him by Sinovel. During that search, two notebook computers, an external hard drive, and other documents were obtained. Subsequent review of those devices and materials corroborated that Karabasevic stored, possessed, and manipulated AMSC's LVRT software.

Based on the FBI's investigation, the FBI subsequently obtained a warrant to search various Sinovel wind turbines that Lumus Construction was scheduled to install in Massachusetts. In March 2012, May 2012, and December 2012, FBI agents searched such turbines and determined that AMSC's pirated software was found within these Sinovel-manufactured turbines.

Since the United States obtained the indictments in late June—and in what bears particular attention for companies doing international business—Sinovel is attacking the efficacy of the United States' summons, arguing that the United States' service attempts are faulty inasmuch as the United States improperly (and ineffectively) served Sinovel's U.S.-based subsidiary, Sinovel Wind Group (USA) Co., Ltd., but not its Chinese parent, Sinovel Wind Group Co., Ltd. Sinovel argues that it is not subject to the United States' summons power as a Chinese corporation and that service of Sinovel USA (dissolved in early July 2013) is not proper under Federal Rule of Civil Procedure 4.

On September 6, 2013, the United States filed its response in opposition to the motion to quash, arguing that Sinovel USA is the alter ego of the parent corporation. At the heart of this argument, the United States is claiming that Sinovel's recent closure of its US subsidiary was made to avoid service of process and a direct result of the United States' case against Sinovel.

This case—beyond providing an interesting alleged story of corporate espionage—should also present a bellwether, of sorts, for the United States' prosecution of foreign corporations and may cause U.S. corporations to further evaluate their international business ventures with certain companies. As noted in Sinovel's moving papers, the United States has not had much, if any, success in properly serving foreign corporations in matters in which the United States seeks to bring criminal charges (Sinovel Mem. of Law in Support of Mot. to Quash Service at p. 4 (Dkt. 51).) If the United States cannot hale foreign corporations accused of international espionage into its courts, then—no matter the investigative lengths to which the United States goes—United States corporations may continue to lack adequate protections against foreign corporations accused of stealing their trade secrets. This is particularly the case whereas here the indicted individuals are all foreign nationals whom the United States has little, to no chance, to ever extradite and is further exacerbated by AMSC's repeated losses against Sinovel for its business losses before Chinese Courts.



# Trading Secrets



While failure to prosecute Sinoval is a worse-case scenario for the United States, this case continues to highlight why companies must monitor the access its employees have to secure databases and to a company's trade secret and confidential information. Companies should consider using additional preventive means to prohibit employees from stealing trade secrets, such as configuring the operating system to restrict access to external devices, thus, restricting the ability to download information to an external device; blocking a user from uploading information to a web-based site; and/or utilizing software that blocks employees from sending emails to certain domain names. In situations like this, companies may also wish to consider placing blocks on the ability of its employees to email certain domain names that are known to be used for personal email accounts. In an era in which data is becoming increasingly portable, companies much increase their vigilance in monitoring use and exporting of its data and trade secrets.



# Trading Secrets



## U.S. Counsels Cross-Border Consistency In Criminal Consequences For Trade Secret Theft

*By Mark Hansen (October 3rd, 2013)*

What do the laws of the United States, Peru and Australia have in common when it comes to imposing similar criminal penalties for trade secret misappropriation? Virtually nothing!

In the U.S., criminal penalties for misappropriating trade secrets range from 10 to 15 years. In Peru, the maximum criminal sentence for stealing trade secrets is 2 years. And in Australia, there is no law expressly criminalizing trade secret theft.

These cross-border inconsistencies are significantly undercutting global efforts to deal with the ever-expanding problem of trade secret misappropriation. The U.S. Chamber of Commerce has recently come out with a proposal intended to address this problem.



### **A. The Problem**

As a result of the growing interdependence among the world's economies, the fight against trade secret misappropriation has gone global, stretching far beyond national borders. This is especially true in the Asia-Pacific region, where there has been a marked increase in the theft of trade secrets in recent years.

Complicating efforts to fight this problem is the fact that the laws of countries directed to this cross-border issue are anything but consistent. In many countries — both developing and developed — there are no criminal penalties for trade secret theft, only civil remedies. However, empirical data strongly suggests that even very large civil awards provide little deterrent for would-be trade secret thieves.

Even in those nations where trade secret misappropriation is a criminal offense, the actual penalties contained in such statutes, and indeed the enforcement of such laws, vary dramatically from country to country.

This lack of consistency makes the prosecution of cross-border trade secret theft very expensive, and greatly reduces the deterrent effect of such laws.

### **B. The Proposed Solution**

Currently, the United States and eleven other countries (Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam) are negotiating a huge



# Trading Secrets

multilateral free-trade agreement known as the Trans-Pacific Partnership (“TPP”). The TPP is intended to join and integrate the economies of Pacific Rim countries.

The twelve countries presently participating in the TPP negotiations make up 40% of the world’s gross domestic product, and account for approximately one third of all world trade. In addition, each of these nations, to different degrees, has seen a tremendous uptick in trade secret theft. Such thefts obviously impact trade development and expansion at which the TPP is aimed.

In response, the U.S., through the U.S. Chamber of Commerce, has [proposed](#) that the twelve negotiating countries each commit to include in the TPP criminal and civil penalties that would provide “uniform, statutory and cost efficient protection of trade secrets.” The Chamber envisions commitments that would establish robust trade secret protection, with criminal penalties designed to sufficiently deter a growing problem.”

Among other things, the proposal takes aim at those countries that have no statutes expressly criminalizing trade secret misappropriation, including Canada, Australia, Malaysia and Singapore.

In addition, the Chamber proposes that the TPP require member nations to provide justification for conditioning a company’s access to its markets on disclosure by the company of its trade secret and confidential information.

## **C. The Prospects for Success**

Although the Chamber’s proposal is strongly supported by U.S. businesses, the likelihood that the other negotiating countries will agree to include it in the TPP is not great. In some countries, trade secret misappropriation has only recently become a significant problem, and the need for criminal penalties is not recognized. In others, there is a reluctance to commit to changing existing laws because of the difficulty of doing so, or because imposing or increasing criminal penalties through trade agreements is domestically unpopular. The fact that the Chamber has made this proposal late in the negotiations of the TPP also undercuts the chances of it being adopted.

## **D. What to Do**

Given these circumstances, you should not look for any significant changes in the trade secret misappropriation laws of TPP countries that would make such laws more consistent with comparable U.S. laws any time soon. A more uniform body of law in this area may ultimately be achieved, but that will not happen for many years, at best. For now, you should continue to step up your efforts to protect your trade secrets and confidential information, and address possible misappropriation before the perpetrator has the opportunity to evade American justice.

# Trading Secrets

# Two Former Eli Lilly Scientists Accused of Stealing \$55 Million in Trade Secrets on Behalf of Chinese Pharmaceutical Company In Southern District of Indiana Indictment

*By Justin Beyer (October 28th, 2013)*

In a year in which the United States has brought and prosecuted a series of high-profile criminal cases under the Economic Espionage Act (“EEA”), another one was recently added to the roll call in the Southern District of Indiana, this time against two former high-level scientists with pharmaceutical giant, Eli Lilly.



On August 14, 2013, a grand jury in the Southern District of Indiana returned a superseding indictment against Guoqing Cao (“Cao”) and Shuyu “Dan” Li (“Li”), stemming from Cao and Li’s alleged multi-year plot to steal Eli Lilly trade secrets and transfer those secrets to one of Eli Lilly’s Chinese-based competitors, Jiangsu Hengrui Medicine Co., Ltd., located in Shanghai, China. Cao and Li are accused—along with an unnamed former Lilly scientist, and current Hengrui official—with stealing nine separate trade secrets (relating to Lilly’s work on cardiovascular disease prevention, diabetes treatment, and cancer treatment) starting in 2011 and continuing until this year. Cao and Li are both currently being held, awaiting a further hearing on their pretrial detention.

According to testimony provided by Eli Lilly's Senior Vice President of Product and Clinical Design, Delivery & Development, William Heath, Jr., at Cao and Li's detention hearing, Hengrui is: "the largest supplier of oncology and pain relief medicines in China", having "received FDA approval for ... a cancer drug in the United States", which "is actually the first sterile parenteral injectable that has been approved from a Chinese company to be brought into the United States, and is quite a significant accomplishment." (*United States v. Cao*, 13-cr-00150-WTI-TAB (S.D. Ind. Oct. 22, 2012), Dkt. No. 95-1 at p. 42 (ID#570).)

According to the indictment, in February 2010, Cao allegedly submitted his resume to Individual No. 1 at Hengrui. Over the next few months, Cao allegedly expressed his displeasure to Individual No. 1 with his job with Lilly and explained that he would be traveling to China in the near term. On May 18, 2010, Individual No. 1 allegedly emailed Cao about a meeting with a Hengrui official on Cao's upcoming trip to China. That same day, Cao allegedly inserted four separate external media devices into his Lilly computer. Following Cao's meeting with Hengrui in China and in the ensuing months, Cao and Individual No. 1 allegedly continued their communications and Individual No. 1 encouraged Cao to recruit scientists to present at a conference in China on Individual No. 1's behalf.

On October 15, 2010, Cao allegedly began emailing Lilly authored papers to his personal email account. Over the next year, Cao allegedly either downloaded to external media devices or forwarded to his personal email account various Lilly trade secret information on no less than six occasions. Additionally, on August 11, 2011, Cao allegedly forwarded Individual No. 1 via email Lilly's trade secret information relating to Lilly's research into LDL cholesterol, diabetes, and dyslipidemia.



# Trading Secrets



During this time that Cao was allegedly acting as a double agent for Hengrui, he accepted a job with Hengrui on August 18, 2011. He did not resign from Lilly until January 11, 2012.

After Cao resigned, Cao and Li allegedly conspired for Li, still a Lilly employee, to send Cao Lilly's trade secrets. On February 21, 2012, Li sent emails to Cao attaching a Lilly PowerPoint divulging Lilly trade secrets relating to Lilly's research into metabolic disorders and testing. Several months later in November 2012, Cao allegedly contacted Li again and provided a list of five research areas Cao was interested in. Less than a week later, on November 8, 2012, Li allegedly emailed Cao, attaching documents revealing Lilly trade secrets pertaining to its oncology research.

Most problematic in Cao and Li's alleged disclosures (and Individual No. 1's solicitations), Lilly utilized common, industry-accepted measures to protect its trade secrets and confidential information. Indeed, like most companies, Lilly limited access through security cards, required employee confidentiality agreements, restricted access to Lilly confidential information on a need-to-know basis, limited access to computer networks, and utilized data security banners and policies. Above industry standards, Lilly also monitored entrance points, recorded campus entry access, required recurrent training and instruction on safeguarding Lilly confidential and trade secret information, and had restrictive guidelines and required specific authorization to publish or discuss Lilly confidential material outside the company. Cao, Li, and Individual No. 1 all had confidentiality agreements and each participated in annual training on Lilly's code of conduct, including its confidentiality policies.

Despite those safeguards, Cao and Li are accused of brazenly downloading from their own Lilly computers and emailing Lilly's trade secrets away through their own Lilly email addresses. If the government's accusations prove true, this was not a case where employees did not realize what they were doing was prohibited.

This case is important for two reasons. First, it continues a year-long upswing in cases in which the United States brought charges under the EEA. According to Matthew Levine's article, ["With Expansion of Economic Espionage Act, Will More Prosecutions Follow?"](#), through November 2012, the United States brought 12 prosecutions under the Act. Since the enactment of the Theft of Trade Secrets Clarification Act of 2012 and only through July 2013, the United States brought 15 cases. (Transactional Records Access Clearinghouse, TRAC Reports, Prosecutions and Convictions for 2013, Lead Charges of 18 U.S.C. 1831 & 1832.)

Second, this case continues to highlight why companies must monitor the access its employees have to secure databases and restrict the ability of its employees from exfiltrating its trade secret and confidential information. Here, despite Lilly utilizing password protections, yearly training, and confidentiality agreements, two trusted long-time employees still allegedly misappropriated and transferred trade secrets allegedly worth \$55 million dollars to a foreign competitor over a multi-year period. Companies should consider using additional preventive means to prohibit employees from stealing trade secrets, such as configuring the operating system to restrict access to external devices, thus, restricting the ability to download information to an external device; blocking a user from uploading information to a web-based site; and/or utilizing software that blocks employees from sending emails to certain domain names, including to certain domain names that are known to be used for personal email accounts. This case, like the Sinovel and Snowden cases before it continually highlight why in an era in which data is portable, companies much continue to increase their information technology security to prevent theft of their trade secrets and confidential information.

# Trading Secrets



## Sino Legend Urges U.S. International Trade Commission (ITC) to Consider Parallel Chinese Court Proceeding in Ongoing Trade Secret Litigation Brought by SI Group

*By Matthew Werber (November 11th, 2013)*

Bringing to light the fact that US and Chinese forums can reach opposite conclusions on the same trade secret misappropriation allegations, China-based rubber and tire resin manufacturer Sino Legend urged the U.S. International Trade Commission (ITC) to consider a parallel Chinese court proceeding seeking to convince the Commission to overturn an unfavorable initial determination by the Administrative Law Judge (“ALJ”).



Last month the U.S. International Trade Commission (ITC) notified parties it will review an initial determination that China-based Sino Legend (Zhangjiagang) Chemical Co., Ltd. and a group of related respondents (“SI Group”) unlawfully imported rubber resins made with the misappropriated trade secret process of New York-based SI Group. The investigation — captioned *In the Matter of Certain Rubber Resins and Processes for Manufacturing Same* (Inv. No. 337-TA-849) — is based on allegations that Sino Legend poached a manager from one of SI Group’s Chinese facilities who disclosed SI Group’s trade secrets to Sino Legend. SI Group contends Sino Legend used these trade secrets to make rubber resins that were ultimately imported into the United States. Like the now well-known 337-TA-655 Investigation involving steel railcar wheel manufacturers Amsted and TianRui, SI Group’s allegations in the ITC are based on acts of misappropriation occurring entirely in China, allegations for which a US District court lacks jurisdiction. You can find our previous post on the *TianRui* case [here](#).

An interesting twist overshadowing SI Group’s litigation in the ITC is the co-pending litigation SI Group initiated in China, which resulted in a much different outcome. SI Group sued in a Chinese court claiming Sino Legend published SI Group’s trade secrets in a Chinese patent application. SI Group’s efforts in the Chinese court system were unsuccessful. On October 12, 2013 the Shanghai Higher People’s Court [rejected](#) a final appeal by SI Group Inc. seeking to overturn rulings in favor of Sino Legend. According to a recent Sino Legend [press release](#), the Shanghai Higher People’s Court “ruled that SI [group’s] appeal lacked factual and legal basis, and reiterated there is no infringement of any trade secrets by Sino Legend.”

Sino Legend has attempted to introduce evidence of the Chinese Court proceedings on several occasions, contending the ITC should show deference to the Chinese court system:

Complainant has affirmatively chosen to avail itself of the Chinese courts and legal system to resolve the dispute at issue. The Chinese court proceedings culminated in a Judgment adverse to Complainant. See Respondents’ Notice of New Authority. Under these circumstances, deference should be shown to the Chinese court ruling, based on the principles of abstention and comity.



# Trading Secrets



SI Group responded it “sued in China only because it had no choice: no US court had personal jurisdiction over Respondents then (as they had not yet imported), or subject matter jurisdiction to adjudicate inventorship of a patent application filed in China.” SI Group also asserted Sino Legend “fail[ed] to offer any evidence that the Chinese court was fair or competent.” According to SI Group “[t]he inability of U.S. trade secret plaintiffs to obtain fair trials in China has been independently confirmed by the U.S.” The ALJ excluded all evidence of the Chinese court proceedings in the evidentiary hearing and the Commission has not signaled any intention to consider such evidence on review.

Regardless, Sino Legend expressed optimism concerning the ITC litigation in a [press release](#) announcing the recent decision of the Shanghai Higher People’s Court. According to Sino Legend, “the initial determination in favor of SI [Group] made by the ITC Administrative Law Judge will be reviewed by the Commission in its entirety ... signaling a turning point in this investigation.”

For valuable insight on protecting trade secrets and confidential information in China and other Asian countries, including the effective use of non-compete and non-disclosure agreements, please check out our recent webinar titled, “[Trade Secret and Non-Compete Considerations in Asia](#).”





# Trading Secrets



## Social Media

# Trading Secrets



## Hands Off My Tweets: Washington State Senate Proposes Ban on Mandatory Disclosure of Employee Social Networking Passwords

*By Scott Schaefer (February 6th, 2013)*

On January 30th, the Washington state senate introduced a [bill](#) which would prohibit public and private employers within the state from requiring employees to turn over their online social-network account passwords. [Senate Bill 5211](#). As we previously blogged, a number of states have [passed](#) or are considering similar legislation, which ostensibly is aimed at protecting employees' privacy in their online but non-public social networking profiles. Though well-intentioned, the Washington legislature and those of other states must carefully tailor such privacy laws to prevent unfair consequences. Employers will be strained, for example, to monitor or enforce current employees' use of employer intellectual or other property in employees' networking profiles.



SB 5211 as currently written is quite broad. It would prohibit an employer from “directly or indirectly” requiring any employee or applicant to submit “any password or other related account information” regarding his/her social networking website profile. “Social networking web site” is also broadly defined to include:

“an internet-based service that allows individuals to construct a public or semi-public profile within a system created by the service; create a list of other users with whom they share a connection within the system; and view and navigate their list of connections and those made by others within the system.”

The bill does not carve out any exceptions for:

- Employer-owned or -paid devices,
- Employee profiles which use or display the employer's trademarks, copyrights, or other intellectual property, or
- Profiles for which the employer provided the employee with significant assistance and resources to develop and maintain.

As our previous bloggers have noted, there is a potential conflict between SB 5211 and those court decisions which suggest a degree of employer ownership of employee online networking profiles that incorporate employer intellectual property, or in which the employer invested significant development and maintenance resources. See, e.g., *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D. Pa. Dec. 22, 2011) (employer may have ownership of former employee's LinkedIn profile); and *PhoneDog v. Noah Kravitz*, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D.Cal.) (November 8, 2011)



# Trading Secrets



(employer may have interest in former employee's Twitter account). As noted above, SB 5211 makes no distinction for such profiles. Some might ask, "how will employers with court-recognized interests in employee online profiles enforce their rights in them, if by law they cannot effectively monitor those accounts?"

Yet another possible conflict is with the common law claims of negligent hiring and retention. That is, injured plaintiffs may use as evidence that an employee was negligently hired or kept on even after his/her social networking activity generated some kind of notice that the employee was not to be trusted (i.e. an employee delivery man posts on his Facebook account, "boy, another DUI last night." Six months later, that employee runs over someone while drunk). Now, the defense might be that an employer cannot be found to have legal notice of the employee's dangerousness, if not get such notice the employer would have had to break the law. But because the bill is broadly written, employers might shy away from even permissible online intelligence gathering regarding its current or prospective employees to avoid the appearance of unlawful searching and significant legal exposure.

Lastly, the law may be very expensive for employers, even for inadvertent violations. Aggrieved plaintiffs may file civil lawsuits for violations, and the court "may" award actual damages, \$500 per-violation kickers, and attorneys' fees to the prevailing employee / applicant. Of course, the awards are discretionary, not mandatory (hence the quotes in the preceding sentence), but the mere possibility of actual and bonus damages and fees is encouragement enough for perhaps an avalanche of lawsuits.

In the end, like any legislation, serious thought and consideration must be given to whether the law will do more good than bad. Such laws must be carefully written to achieve their intended purpose without doing too much collateral damage. We will monitor SB 5211 as it proceeds through the Washington legislature.

# Trading Secrets



## Federal Court Rules That Twitter Invites and Facebook Posts Do Not Constitute Impermissible Employee Solicitations

*By Justin Beyer (February 19th, 2013)*

On January 22, 2013, United States Magistrate Judge Steven Shreder of the Eastern District of Oklahoma issued a report and recommendation, following Plaintiff Pre-Paid Legal Services, Inc.'s motion for preliminary injunction against its former employee Todd Cahill, concerning whether certain social media communications constituted impermissible employee solicitations in violation of a restrictive covenant agreement. [Pre-Paid Legal Services, Inc. v. Cahill](#), Case No. CIV-12-346-JHP, 2013 U.S. Dist. LEXIS 19323 (E.D. Okla., Jan. 22, 2013).



In its motion, Pre-Paid Legal Services, now known as LegalShield, sought a preliminary injunction seeking to enjoin Cahill's misappropriation of trade secrets and solicitation of its workforce. LegalShield sought to prevent certain social media communications made by Cahill through Twitter and Facebook, which LegalShield argued constituted impermissible solicitations. Notably, Magistrate Judge Shreder held that these communications were neither solicitations nor impermissible conduct under the terms of the agreement.

To summarize the facts of the case, LegalShield sells legal service plans to its customers, providing access to legal services. LegalShield seeks to sell these plans utilizing a network marketing sales model, where sales associates recruit and build a sales organization, which is referred to as a recruiter's "downline." LegalShield makes "downline" information—made up of the contact and performance information of sales associates—available to sales associates through a password protected site.

Cahill was originally hired as a sales associate, built a significant downline network. In building his network, Cahill created private Facebook pages, which Cahill used to communicate with his most successful associates. Cahill was eventually promoted to a Regional Manager over the Southern California region and Regional Vice President of Illinois. Concurrent with his promotion to Regional Manager, he executed the Regional Manager Agreement. Included within that agreement were both confidentiality provisions and a non-solicitation provision, prohibiting solicitation of LegalShield employees.

On August 10, 2012, allegedly under false pretenses, Cahill allegedly called a meeting of a number of high ranking sales associates. Prior to the meeting, Cahill allegedly met with certain sales associates and solicited and sought to convince those persons to leave LegalShield's employ for Nerium, a skin care company, which also operated a multi-level marketing company. At the meeting, Cahill allegedly told the employees that he was leaving LegalShield and, if the employees were interested in where he was going and what he was doing, they should email Cahill.

Following the meeting, Cahill emailed his resignation letter to LegalShield. After his resignation, LegalShield shut off his access to his downline information. Three days later, Cahill allegedly posted



# Trading Secrets



information about Nerium on the private Facebook pages he created during his employment with LegalShield. Cahill did not post any information to those pages after August 13, 2012. Cahill, however, allegedly continued to post information about Nerium on his personal Facebook page and sent general requests to LegalShield employees to join Twitter.

In moving for a preliminary injunction, LegalShield argued that Cahill should be preliminarily enjoined from utilizing, disclosing or misappropriating LegalShield's trade secrets, which LegalShield argued was its downline information. Cahill argued that he did not have access to the information, with which the court agreed and the court denied LegalShield's motion with respect to its misappropriation claim.

LegalShield also argued that Cahill should be enjoined from directly soliciting LegalShield's employees. Citing Cahill's undisputed solicitations of LegalShield's employees, the court found that LegalShield satisfied its burden and Cahill was enjoined from initiating contact with LegalShield's employees.

In the most interesting piece of the case from a legal development standpoint, the court gave careful consideration to LegalShield's argument that Cahill's general posts to his personal Facebook page about Nerium constituted impermissible solicitations. Noting that such an argument constituted a "novel issue", the court analyzed other court decisions in which similar arguments were made regarding alleged social media solicitations.

Specifically, the court analyzed *Enhanced Network Solutions Group, Inc. v. Hypersonic Technologies Corp.*, 951 N.E.2d 265 (Ind. Ct. App. 2011) and *Invidia, LLC v. DiFonzo*, 2012 WL 5576406 (Mass. Super. Oct. 22, 2012). In *Enhanced Network*, the Indiana Court of Appeals considered whether a job posting on a LinkedIn page constituted an improper solicitation. The court found that the posting did not constitute a solicitation because the Enhanced Network employee "made the initial contact with Hypersonic after reading the job posting on a publicly available portal of LinkedIn." 951 N.E.2d at 268.

In *Invidia*, the plaintiff argued that its former hairstylist violated a non-solicitation provision by friending certain of plaintiff's customers on Facebook after leaving plaintiff's employ. Finding that such friending was not a solicitation, the Massachusetts court held that: "one can be Facebook friends with others without soliciting those friends to change hair salons, and [Plaintiff] has presented no evidence of any communications, through Facebook or otherwise, in which [Defendant] has suggested to these Facebook friends that they should take their business to her chair at David Paul Salons." 2012 WL 5576406, at \*6.

Discussing the facts of the instant case, the court found that Cahill's acts were even less explicit than those of the defendants in *Enhanced Network* or *Invidia*. The court also found that LegalShield presented no evidence that it would suffer irreparable harm if Cahill was not enjoined from posting on his personal Facebook page or that Cahill's Facebook posts had caused a LegalShield employee left as a result of such posts. 2013 U.S. Dist. Lexis 19323 at \*30-31.

The import of this decision and others like it is that courts do not appear convinced that simply providing information in a public forum, to which a former employee's coworkers or customers may visit constitutes improper solicitation. That said, no court appears to have been confronted with the question of whether an improper solicitation occurs when the former employee communicate with a former employer's workforce or customers directly through a social media site or speaks ill of the former employer through such a site. Despite no court being confronted directly with these questions, the *Cahill*, *Enhanced Network*, and *Invidia* decisions all foreshadow that courts will enjoin solicitations



# Trading Secrets



through social media if those communications rise to the level of traditional solicitations, such as emails, etc.

The important takeaway from this case is that courts are treating social media solicitations argument as legitimate. This development offers an area of discovery that all employers should seek to explore (and an area that defense counsel must be sure to caution their clients to preserve).

But, though it is now being recognized by courts as a possible means by which a former employee could breach a non-solicitation provision, employers are still required to show more than a former employee provides mere access to information, even where that information is likely to be viewed by that employer's workforce or customers. Courts, instead, appear to be looking for either personalized communications to the allegedly solicited persons or generalized communications either extolling the virtues of the new employer or badmouthing the former employer. Under that factual scenario, the *Cahill* court, at least, appears to suggest that such generalized posts could constitute impermissible solicitations.

For more information on these interesting issues, please join me on February 20, 2013, for an informative complimentary webinar on Trade Secrets in the Telecommunications Industry. The webinar starts at noon CST and you can register [here](#).



# Trading Secrets



## Federal Court Questions Whether Damages Exist in LinkedIn Account Ownership Dispute

*By Jessica Mendelson and Robert Milligan (March 2nd, 2013)*

The ownership of social media accounts in the employment context remains a very hot topic.

In fact, you might remember the case of *Eagle v. Morgan*, Case No. 11-4303, E.D.Pa., a heavily disputed case regarding the ownership of a company LinkedIn account, which we've [blogged about](#) previously. In a post-trial hearing last week, the federal district court judge suggested that the LinkedIn account may have belonged to Eagle, however, there were no actual damages for her former employer's alleged unlawful access of the account, and thus, Eagle's claim against her former employer was unlikely to succeed.



Linda Eagle, the former CEO of a banking education company sued her former employer Edcomm following her termination, after Edcomm allegedly changed the password for her LinkedIn account, preventing her from accessing it, and then replaced her name and photo with that of Sandy Morgan, Eagle's replacement. In [October 2012](#), the U.S. District Court for the Eastern District of Pennsylvania granted the defendants' motion for summary judgment on Eagle's Computer Fraud and Abuse Act and Lanham Act claims. The court denied summary judgment with respect to the state claims asserted by Eagle and retained jurisdiction over state law claims for invasion of privacy by misappropriation of identity, tortious interference with contract, unauthorized use of name in violation of Pa. C.S. § 8316, misappropriation of publicity, identity theft under Pa. C.S. § 8316, conversion, civil conspiracy, and civil aiding and abetting. A bench trial was held in November 2012, however, the record is still under seal and has yet to be released to the public.

In a hearing on post-trial motions on February 20, 2013, U.S. District Court Judge Ronald Buckwalter of the Eastern District of Pennsylvania reportedly suggested EdComm likely did not have a right to prevent Eagle from accessing her LinkedIn account. In explaining this, Judge Buckwalter cited the fact that EdComm did not have a policy requiring employees to hand over ownership of their social media profiles, even if they were used to solicit new business. During the hearing Judge Buckwalter reportedly [told](#) EdComm's attorney, "These LinkedIn accounts belonged to individual employees and there's nothing to suggest otherwise. What justification did you have for doing what you did? I don't see how you can justify what you did here." Despite the lack of justification, Judge Buckwalter had difficulty finding actual damages, reportedly [calling](#) claims that she had suffered a loss of unspecified business opportunities due to her inability to access messages sent to her through her LinkedIn account "highly speculative." Judge Buckwalter reportedly stated that he had great difficulty believing Ms. Eagle had actually suffered damages from her inability to access the LinkedIn account. Although Judge Buckwalter has yet to issue a final decision, his comments at the hearing suggest he is unlikely to rule on Eagle's behalf but no final decision has been made.

The case serves as a reminder that employers need to be proactive and develop social media policies and ownership agreements concerning social media accounts before the need actually arises.



# Trading Secrets



Agreements and policies should establish who owns the company social media account, and specify a procedure for returning login information upon termination. Employees should be reminded of the agreements and policies at the time of termination and employers should ensure that they obtain the relevant usernames and passwords. Additionally, the company should register or create the account, and change the password at the time of termination in order to avoid confusion. Agreements and control over the account are key in such disputes, as they are determinative to who actually owns the account.

We will continue to keep you apprised of future developments in this case and similar social media ownership/trade secret issues.

# Trading Secrets



## New Jersey Poised To Adopt New Social Media Legislation

*By Jessica Mendelson (April 1st, 2013)*

With the passage of A2878 in the New Jersey General Assembly in March, New Jersey is poised to become the [eighth state](#) to “pass legislation preventing employers from asking prospective and current employers for passwords to their accounts on social media sites.” The proposed law, which is now being considered by Governor Chris Christie, would become the most restrictive social media legislation in the United States.



A2878 would be the first social media law to prohibit employers from even inquiring whether employees or job applicants have personal social media accounts. Any employer who violates this prohibition could be subject to a private lawsuit by the applicant or employee. Additionally, employers may face other civil penalties of up to \$1000 for the first instance and up to \$2500 for each additional violation. Under the terms of the proposed law, neither of these penalties can be waived.

The passage of the law could create significant challenges for employers trying to act within its bounds. Experts worry that employers could violate the law inadvertently, since many employees use social media to do their jobs. Furthermore, the prohibition could prove problematic with social media networks like LinkedIn, which employers commonly use. Another worry is that the law encourages an already litigious society. The bill allows an employee to file suit against his or her employer up to a year after the violation. Exacerbating the problem, an employee is entitled to recover damages and attorneys’ fees in the suit, encouraging litigious behavior. Furthermore, since the law is so easy to violate, it might encourage hawkish behavior among attorneys.

Others argue that the law could protect companies from liability by clearly allowing them to decline involvement in the activity of their employees on social media networks. Since the employer is not allowed to know about the employee’s social media involvement, employers are not placed in a position where an employee’s social media commentary or activities could be viewed as that of the employer.

Ruben Ramos, a New Jersey State Assemblyman sponsoring the bill, reportedly [argued](#) that this law is necessary to prevent invasions of privacy: “If we don’t draw this line in the sand now, who knows how far this invasion of privacy might be taken. In an economy where employers clearly have the upper hand, we need to protect the rights of job seekers from being trampled.”

New Jersey Governor Chris Christie has yet to decide whether to sign the legislation. [According to a spokesman for the governor](#), “We’ll have to see the bill in its final form and consider it, and the Governor will act within the allotted time allowed.” Governor Christie did [sign](#) a similar law in December 2012, prohibiting colleges and universities from requiring applicants and students to disclose their social media accounts and passwords.



# Trading Secrets



With the passage of the bill, New Jersey would be the eighth state with this type of protective social media legislation in place. We will continue to keep you apprised of the bill's progress as well as other developing social media legislation throughout the country.

# Trading Secrets



## Court Issues Decision in Eagle v. Morgan: Employee Owns LinkedIn Account But Fails To Recover Any Damages Against Former Employer

*By Jessica Mendelson and Robert Milligan (April 3rd, 2013)*

The ownership of social media accounts in the employment context remains a very hot topic. We've previously [blogged](#) about the case of *Eagle v. Morgan*, Case No. 11-4303, E.D.Pa.. The case went to trial in November 2012, and the court has recently issued its [trial order](#), finding that even though the plaintiff successfully proved three causes of action, she failed to prove damages with reasonable certainty, and thus, was unable to recover against her former employer.



Linda Eagle, the former CEO of a banking education company, sued her former employer EdComm following her termination from the company. After Eagle's termination, EdComm allegedly changed the password for her LinkedIn account, preventing her from accessing it, and then replaced her name and photo with that of Sandy Morgan, Eagle's replacement. In October 2012, the U.S. District Court for the Eastern District of Pennsylvania [granted](#) the defendants' motion for summary judgment on Eagle's Computer Fraud and Abuse Act and Lanham Act claims. The court denied summary judgment with respect to the state claims asserted by Eagle and retained jurisdiction over state law claims for invasion of privacy by misappropriation of identity, tortious interference with contract, unauthorized use of name in violation of Pa. C.S. § 8316, misappropriation of publicity, identity theft under Pa. C.S. § 8316, conversion, civil conspiracy, and civil aiding and abetting. A bench trial was held in November 2012.

In its most recent [ruling](#), the court found that although EdComm encouraged the use and creation of LinkedIn accounts, the company had no clear ownership policies in place. In fact, the court's order suggests that company officials were aware that the lack of such policies might prove problematic in the future, yet declined to adopt any social media ownership policies. Eagle reportedly provided her account information to other employees who assisted her in maintaining the account, allowing EdComm to gain control of the account following her departure, and allegedly to divert users searching for Eagle's account to the company account which contained Morgan's photo and information.

Although these facts enabled Eagle to successfully prove her claims of invasion of privacy by misappropriation of identity, misappropriation of identity, and unauthorized use of name in violation of 42 Pa. C.S. § 8316, the court found that Eagle had failed to plead damages with certainty, and therefore, she could not recover. Although EdComm had engaged in unauthorized use of Eagle's name, which had commercial value, Eagle's assessment of damages was too speculative. Eagle argued that she had generated approximately \$1 million in revenue annually from her 4000 LinkedIn contacts, and therefore, each contact was worth \$250 annually. She argued that she had been locked out of her LinkedIn account for three months, and therefore, was entitled to \$250,000. However, the court found this calculation was overly speculative and lacked corroborating evidence. There was no evidence that Eagle had failed to obtain any deals as a result of the loss of her LinkedIn account, nor was there any evidence that she would have actually made any deals during this time period if she had



# Trading Secrets



the account. In fact, Eagle's own expert admitted to "guesstimating" on the damages, and more importantly "failed to connect Dr. Eagle's successful sales with any use of LinkedIn."

The court [found](#) in favor of EdComm on the remaining causes of action. According to the Court, there was no identity theft, as the only information of Eagle's that was used was her name, and that was publicly available. The court similarly found conversion did not apply, as the LinkedIn profile was intangible property. Furthermore, the court rejected EdComm's counterclaims for misappropriation, as there was no evidence that Eagle's contacts were developed through an investment of EdComm time and money, as opposed to her own time and past experience. There was also no evidence of EdComm's ownership of the account. The counterclaim for unfair competition was also rejected, due to the lack of evidence of unfair competition through the use of the LinkedIn account. Finally, the court declined to award punitive damages, as the lack of an ownership agreement meant it was just as likely that EdComm was acting to protect its property rather than acting to harm Eagle.

The case serves as a reminder of the difficulties of placing social media, such as LinkedIn accounts, into existing intellectual property framework. Furthermore, the case suggests that employers need to be proactive and develop social media policies and ownership agreements concerning social media accounts before the need actually arises. Agreements and policies should establish who owns the company social media account, and specify a procedure for returning login information upon termination. Employees should be reminded of the agreements and policies at the time of termination and employers should ensure that they obtain the relevant usernames and passwords. Additionally, the company should register or create the account, and change the password at the time of termination in order to avoid confusion. Agreements and control over the account are key in such disputes, as they are determinative to who actually owns the account.

We will continue to keep you apprised of future social media ownership and trade secret issues. For more information on the Eagle v. Morgan case and social media/trade secret issues, please see our recent webinar on [Trade Secrets and Social Media](#).



# Trading Secrets



## Federal Court Allows Service On Foreign Defendants Through Facebook

*By Jessica Mendelson (April 18th, 2013)*

Did you think Facebook was just for “likes” and “status” updates? Think again! A federal district court in New York recently tackled the issue of service of process via social media head on, permitting service via Facebook as a backup means of service for serving foreign defendants.



In the case of [\*Federal Trade Commission v. PCCare247, Inc.\*](#), the Federal Trade Commission (“FTC”) sued multiple defendants, including five based in India. The foreign defendants included two businesses and three individuals. According to the FTC, the defendants had violated certain provisions of the Federal Trade Commission Act by developing a business to deceive American consumers into fixing non-existent computer problems. The FTC had already secured a temporary restraining order against the defendants, which enjoined specific business practices and froze some of the defendants’ assets.

Each defendant had been provided with the summons, complaint, and related court documents by email to their last known addresses, by Federal Express (“FedEx”), and by personal service through a process server. FedEx had confirmed delivery for some of the defendants, and the process server had confirmed delivery to all defendants.

The FTC also served the documents to the Indian Central Authority for service, pursuant to Rule 4(f)(1) of the Federal Rules of Civil Procedure and the terms of the Hague Convention. After multiple inquiries over a four month period, the Indian Central Authority had not responded to the FTC in order to confirm receipt. The Defendants were on notice of the lawsuit, and hired attorneys to represent them at the preliminary injunction. However, defendants’ attorneys withdrew a few months later for nonpayment.

Since the Indian Central Authority failed to confirm service, the FTC filed a motion seeking permission to serve additional documents via email and Facebook. In its analysis, the Court concluded that service by email and Facebook was not prohibited by international agreement, nor had India objected to this type of service. The court conducted a due process analysis, and found that Facebook service was reasonably calculated to notify the defendants of future filings.

Here, the defendants used both email and social media frequently to run their business, and therefore, service by email alone was sufficient to satisfy due process. Furthermore, the fact that two of the defendants had registered their email accounts with Facebook, included their job titles on Facebook, and were Facebook friends with one another, suggested they were highly likely to receive such messages. According to the court, “where defendants run an online business, communicated with customers via email, and advertise their business on their Facebook pages, service by email and Facebook together presents a means highly likely to reach defendants.”

Although the district court permitted service of process in PCCare247, the fact that it was merely an alternative means of service seems to have played a key role in the decision. Prior case law from the same district court suggests that we should not necessarily expect Facebook service to spread like



# Trading Secrets



wildfire, and that such service may be limited to cases where the Facebook profile can be properly authenticated. For example, in [Fortunato v. Chase Bank USA](#), the court declined to permit service of a third party complaint by Facebook message to an address found on the individual's Facebook profile, as the plaintiff failed to show the Facebook profile was authentic or that it was regularly used by the individual.

The use of social media for service is likely to become an increasingly disputed issue in the coming months and years. This past month, Texas became the first state to propose a bill allowing for service of legal process via social media. Texas State Representative Jeff Leach, a Republican, recently introduced a bill in the state's House of Representatives regarding the use of social media for service of process. If passed, [House Bill 1989](#), would permit "an electronic communication sent to the defendant through a social media website" to act as a method for service of process, provided that "the defendant maintains a social media page on that website, the profile on the social media page is the profile of the defendant, the defendant regularly accesses the social media page account, and the defendant could reasonably be expected to receive actual notice if the electronic communication were sent to the defendant's account." If the bill were to become law, Texas would be the first state to legalize social media as an alternative means of service.

Service via social media has become increasingly prevalent in other countries, suggesting the United States may not be far behind. In England, the High Court recently [approved](#) the use of Facebook for service of legal documents in a commercial dispute. Similarly, "Facebook is [routinely used](#) to serve claims in Australia and New Zealand."

The use of social media for service of process is likely to be a continuing issue in the United States, and we will keep you apprised of future developments in this rapidly changing area.



# Trading Secrets

## Utah, New Mexico, and Arkansas Pass Social Media Legislation Restricting Employer Access to Personal Social Media Accounts

*By Robert Milligan and Jessica Mendelson (April 23rd, 2013)*

Social media legislation restricting access to personal social media accounts has been a hot topic in recent months, and as 2013 progresses, more and more states seem poised to pass such legislation. Here's a roundup of some of the more recent social media legislation passed in Utah, New Mexico, and Arkansas:



### Utah

With the passage of the Internet Employment Privacy Act (IEPA) last month, [Utah became the fifth state in the country](#) to pass legislation restricting employers' access to their employees' social media accounts. Under the terms of the legislation, neither public nor private employers [can](#) "ask an employee or job applicant to disclose a username and password or a password that allows access to the employee's or applicant's personal Internet account" or retaliate against an employee or job applicant who fails to disclose such information. However, employers [can still](#) request the disclosure of account information to gain access to the employer's "electronic communications device, account or service." Employers can also investigate employee misconduct involving an employee's personal email account, restrict or prohibit access to certain website on the employer's devices or networks, and block certain access and communications on the employer's device or network. Employers are also still entitled to screen employees and job applicants. The law also provides penalties for failure to comply: employees and job applicants are entitled to up to \$500 in damages from employers for violations of the law.

### New Mexico

With the [passage](#) of [SB 371](#), New Mexico joined a handful of others states to impose restrictions on employers' access to social networking accounts. Under this law, which was signed by Governor Susana Martinez on April 5, an employer is prohibited from requesting or demanding access to a job applicant's social networking account. However, unlike similar laws passed in other states, such as [California](#), [Illinois](#), [Maryland](#), [Michigan](#), and Utah, [New Mexico's law does not prohibit employers from accessing the accounts of current employees.](#) Furthermore, the law does not prohibit employers from instituting workplace restrictions on access to the internet or social media websites, nor does it restrict an employer's right to view information found in the public domain.

The legislation prohibits an employer from requesting or demanding a job applicant divulge a password to allow access to his or her social networking accounts or from demanding access to such accounts in any other manner. There are, however, exceptions to this rule. Employers can still monitor the usage of company electronic equipment or email without requesting or requiring a prospective employee to provide a password.

New Mexico's law [does not](#) contain a remedial plan for damages or penalties. The New Mexico law will take effect on June 14, 2013.



# Trading Secrets



## **Arkansas**

On April 22, 2013, Arkansas' governor signed [Act 1480](#), a law which prohibits an employer from requiring or requesting a current or prospective employee from disclosing his or her username or password for a social media account to provide access to the contents. However, the Act does not regulate the following types of social media accounts: (1) accounts opened by employees at their employer's request, (2) accounts provided to an employee by an employer, (3) accounts setup on behalf of an employer, or (4) accounts setup to impersonate an employer. Employers are prohibited from requesting, requiring, suggesting, or causing current or prospective employees to disclose their usernames and passwords, adding employees or supervisors to their social media contacts, or changing privacy settings. Employers are not liable for inadvertently receiving such information, and employers are entitled to obtain such information if it is reasonably believed to be relevant to a formal investigation of allegations of the employee's breach of federal, state, or local laws or the employer's written policies.

## **Conclusion**

As of April 2013, [thirty-five states](#) were considering (or had already introduced) social media legislation. States throughout the country are currently considering this hot topic, and we will likely see additional states pass similar social media legislation before the year is out. [Social media legislation](#) has been submitted to Governor Christie in New Jersey for signature. We have previously provided our critique of this [type of legislation](#), and we will continue to notify you of future developments.

# Trading Secrets



## New Jersey Federal Court Issues Sanctions For Deletion of Facebook Profile

*By Jessica Mendelson and Grace Chuchla (April 30th, 2013)*

Litigants ought to think twice before deleting their Facebook profiles. Just this month, a New Jersey federal judge issued sanctions against a litigant in a personal injury case for deleting his Facebook profile after agreeing to grant defense counsel access to the profile.

In [\*Gatto v. United Air Lines\*](#), the plaintiff, Gatto was a former ground operations supervisor at John F. Kennedy International Airport in New York. Gatto sued as a result of injuries he allegedly incurred on the job. Gatto claimed a set of fueler stairs had crashed into him allegedly resulting in permanent disabilities which left him unable to work.



During the discovery phase of the case, the defendants sought discovery of Gatto's social networking sites. The parties agreed Gatto would provide his password to defense counsel after he had changed it. Defense counsel subsequently logged into Gatto's Facebook account and printed out portions of his Facebook page. Defendants also sent a signed authorization to Facebook so that they could access the account, but Facebook objected, suggesting that defendants ask Gatto to download his own account information.

Following the defendants' access of his Facebook account, Gatto allegedly received notice that his account had been accessed from an unfamiliar IP address. Gatto deactivated the account allegedly for fear it had been hacked. This led to the deletion of the contents of the account, and defendants brought a motion for spoliation sanctions.

The court held that to issue sanctions, it needed to find four factors: "(1) the evidence was within Gatto's control; (2) the evidence was actually suppressed or withheld by Gatto; (3) the destroyed evidence was relevant to claims or defenses in the case; and (4) Gatto should have reasonably foreseen that the evidence would be discoverable.

The court found that the first, third, and fourth factors were present. Gatto argued that he did not intend to destroy anything, but rather, deactivated the account because he had previously been hacked, and feared it was happening a second time. The court, however, noted that the adverse inference instruction was designed to level the playing field if one party has been prejudiced by destruction, and therefore, whether Gatto actually had intent was "largely irrelevant." No matter his excuse, Gatto "effectively caused the account to be permanently deleted," which rendered a spoliation inference appropriate. As such, the court permitted an instruction to be given to the jury that they may draw adverse consequences from the deletion of Gatto's profile.

*Gatto* is just the most recent case on the discovery of social media and the consequences for the spoliation of such of evidence, and there will likely continue to be more in the future. Recently, in



# Trading Secrets



[Lester v. Allied Concrete Co.](#), a Virginia court sanctioned a party and his lawyers in a wrongful death suit for intentionally destroying a Facebook page. In that case, the opposing party requested discovery of the contents of the plaintiff's Facebook page after it obtained a photo of the plaintiff wearing an "I ♥ hot moms" T-shirt. After the plaintiff had been questioned about the shirt at deposition, his attorney instructed him to "clean up" the account to prevent "blowups of this stuff at trial." The account was removed, and defense counsel was told that the plaintiff had no Facebook page. The account was later reactivated and the contents were produced, with the exception of a number of objectionable photos. Although the jury found in favor of the plaintiff, the court sanctioned plaintiff and his attorney for spoliation as a result of the deletion of the page.

*Gatto* and *Lester* are important as both cases suggest the changing face of discovery as a result of the prevalence of social media in today's world. A social media profile is by no means safe from discovery, and as a result, parties [should be careful](#) about what is being revealed online. Parties to ongoing litigation should be careful not to delete or deactivate their accounts, as they may be fair game for discovery. Social media profiles have become the source of highly relevant and discoverable evidence and should be treated with the same preservation care that any other hard copy documents and traditional forms of electronically stored information are given during litigation.





# Trading Secrets



## New Jersey Assembly Passes Revised Employee Social Media Privacy Bill

*By Guest Authors Carl Lopez, Caroline Keller and Chris Lower (May 20th, 2013)*

The New Jersey General Assembly voted today on a new version of an employee social media privacy bill which incorporates revisions suggested by Governor Chris Christie when he conditionally vetoed the bill on May 6, 2013. The Assembly passed the revised version with an overwhelming vote of 74-0. The bill is expected to receive similar support in the Senate, where the earlier version passed 28-0, and from Governor Christie.



Like its predecessor, the revised bill prohibits employers from requiring employees and candidates to disclose user names, passwords, or other login information for accessing their social media accounts like Facebook or Twitter. The revised bill, however, attempts to balance employee privacy concerns against the needs of employers to hire appropriate personnel, manage their operations, and protect their proprietary information. Governor Christie signed a similar law in December 2012, prohibiting colleges and universities from requiring applicants and students to disclose their social media accounts and passwords.

### **The Requirements of the Bill**

Under the proposed law, employers are prohibited from requiring or requesting employees or job candidates to disclose login information for their personal social media accounts. Any agreement between an employer and an employee or candidate to waive the privacy protections of the bill would be void and unenforceable.

The revised bill also prohibits employers from retaliating or discriminating against any employee or candidate who:

- Refuses to provide login information for his or her social media accounts;
- Reports an alleged violation of the law to the Commissioner of Labor and Workforce Development;
- Testifies, assists, or participates in an investigation concerning a violation of the law; or
- Otherwise opposes a violation of the law.

The revised bill eliminates a controversial provision that would have prohibited employers even from asking an employee or candidate if he or she has any social media accounts. In his conditional veto statement, Governor Christie recommended that this provision be removed because it “paint[ed] with too broad a brush.” For example, the Governor worried that, as written, the bill would have prohibited an employer interviewing a candidate for a marketing job from inquiring as to the candidate’s use of social networking so as to gauge his or her technology skills and media savvy.



# Trading Secrets



## **Enforcement**

Perhaps the most significant revision in the new bill is the elimination of a provision that would have allowed employees or candidates to bring civil suits seeking money damages, injunctive relief and attorneys' fees against employers for alleged violations. This provision raised the specter of frivolous lawsuits by employees or candidates that would nevertheless prove costly for employers to defend against.

The revised bill limits enforcement to a civil penalty of up to \$1,000 for the first violation and up to \$2,500 for each subsequent violation.

## **Employer Protections**

In addition to scaling back some of the prior bill's more onerous aspects, the revised bill contains provisions that affirmatively protect employers' ability to continue to use social media and comply with other laws and regulations:

The previous version of the bill prohibited employers from requiring access to employee or candidate "personal account[s]" but did not define the term. That was problematic because many employers have company social media accounts that are managed or curated by particular employees. Without statutory guidance, the ambiguity between what is a "business account" and what is a "personal account" created the potential for employers to be held liable for requesting login information to accounts that they viewed as their own. The revised bill addresses this problem by defining a "personal account" as one that is used by an employee or candidate exclusively for personal communications unrelated to any business purposes of the employer. An account is not personal, and therefore not subject to the privacy protections of the bill, if it is used by an employee for the business purposes of his or her employer.

- Employers may continue to implement policies pertaining to the use of company-issued electronic devices or social media accounts used by employees for business purposes.
- Employers may continue to conduct investigations to ensure compliance with applicable laws or regulations, or prohibitions against workplace misconduct on the basis of specific information about activity on a personal account by an employee.
- Employers may continue to investigate specific allegations that an employee is transferring proprietary information or financial data to a personal account.
- Employers may continue to view and act on information pertaining to an employee that is available in the public domain.

# Trading Secrets



## Washington State Passes Social Networking Privacy Legislation

*By Scott Schaefer (May 27th, 2013)*

On May 21, 2013, Washington Governor Jay Inslee signed into law [Senate Bill 5211](#), which with certain exceptions prohibits mandatory employee disclosure of 'personal' social-networking account information and profiles. The revised bill passed the Washington house and senate unanimously, and will go into effect on July 28, 2013. Washington thus became the ninth state to pass such legislation, which is intended to protect employee privacy in their non-public social networking activities.



On February 6th, we [blogged about SB 5211's introduction and original text](#), and we expressed concern that it was too broad to protect legitimate employer interests in their proprietary and physical assets. For example, the bill as originally written did not exempt good-faith employer investigations of employee misconduct, or legitimate employer monitoring of its own networks and hardware.

Since then, the legislature re-wrote several provisions, and the final bill as passed strikes a better balance between employee privacy and employer property rights.

In its final form, the law still prohibits employers from "requesting, requiring, coercing, or causing" employees or job applicants to turn over login information, open their online profiles in the employer's presence, add an employer representative to their accounts, or alter their privacy settings. The law also prohibits employer retaliation for employees' refusals to comply with those unlawful requests. A violation of the law exposes the employer to liability for actual damages, injunctions, equitable remedies, a \$500 penalty, and paying the employee's attorneys' fees. In short, the law has teeth to protect employee privacy.

Even so, employers are protected, too. The law does not prohibit employers from requesting the content (but not logins) of its employees' profiles during legitimate employer investigations, and it allows employers to (1) access and monitor its own intra- and extra-net communities, (2) require logins for job-required social networking accounts and employer-owned devices, (3) enforce personnel policies (consistent with the law's prohibitions), and (4) require logins to comply with other applicable law. The law also has an "innocent discovery" rule, which says that an employer is not liable if it unintentionally receives protected employee logins during permitted monitoring activities.

Permitted investigations and accompanying requests for profile content (and again, not login info) must be (1) in response to the employer's receiving information regarding employee networking activity, and (2) for the purposes of determining (a) compliance with applicable law, or (b) whether employer proprietary assets or confidential data was improperly transferred to the employee's social network account.

So, the law has ingredients which both employees and employers like. If Washington had to pass this law (apparently so), it did so responsibly. Nevertheless, an unresolved issue still lurks. The law does not define what constitutes a 'personal' account. Does it apply to hybrid accounts – those used for



# Trading Secrets



personal and employment purposes? Indeed, the law permits mandatory login disclosure for “an account or service provided by virtue of the employee’s employment relationship with the employer.” RCW 49.44.\_\_\_\_§ 3(b). An employer aware of the decisions that we blogged on some time ago, including [Eagle v. Morgan](#) and [PhoneDog v. Kravitz](#), may try to end-run around the new law by writing into its employees’ job descriptions the mandatory usage of employer-‘provided’ features and services in new or pre-existing accounts. After all, in each of those cases (though neither of which were decided in Washington courts), the court held that the employer could have some level of ownership in the employee’s social-networking account, where the employer required employee usage of the account, and provided substantial assistance in developing and maintaining the account. Thus, by merely including mandatory usage in its job descriptions, and “providing” account assistance, an employer might be able to make the exception the rule.

We will keep an eye on the law as it makes its way through the Washington court system, and update you with significant developments.

# Trading Secrets



## Mobile Device Forensics – Are You in the Know?

*By Guest Authors James Whitehead and Arnold Garcia (June 5th, 2013)*

*As a special feature of our blog –special guest postings by experts, clients, and other professionals – please enjoy this blog post by digital forensics experts James Whitehead and Arnold Garcia with iDiscovery Solutions. - Editor, Robert Milligan*

Smartphones, tablets and other “Smart” mobile devices are becoming a mainstay within the corporate landscape. Today’s mobile devices are sleek, fast, secure, and highly capable within the corporate landscape. Currently it is expected mobile devices will lead all other computing devices for web access in 2013. C level executives are choosing a tablet or other mobile devices to replace the laptop in the field.



BYOD and corporate adoption of mobile devices coupled with secure policies and procedures leads us to believe that more devices such as Apple’s iPad or Samsung’s Galaxy Tab will continue to grow within corporate cultures for the next few years. There are tools currently in the market with mature development cycles providing enterprise management of both corporate owned devices and employee owned devices alike.

The increasing adoption of cloud technologies by companies both large and small stands ready to fuel the next wave of services and applications. The industry growth is likely to result in more devices showing up in active litigation matters.

### Capable Devices

As mobile device technology advances, the amount and types of data that can be stored and or accessed from a mobile device is constantly increasing. Corporate IT departments are adopting these technologies and more robust user services roll out seemingly daily. Mobile Devices used by today’s corporate end user is capable of managing several forms of communications including emails, SMS, MMS, and of course phone calls and voicemails. This however is but a limited view into the vast capability of these devices. Today’s devices coupled with cloud computing provide the capability for an end user to access, manage, or view the full catalog of enterprise applications. SAP, ERP, document management, and project management are but a few tools available on many Mobile Devices.

### Corporate Adoption

Cloud computing has pushed the paradigm of PC based computing back to “Terminal” based computing, or dummy terminals. In this instance the work is occurring on the remote cloud server, and your computer or “Mobile Device” acts as a terminal into that process. This enables the corporation to provide a fabric of support on the mobile platform similar to that of a laptop.



# Trading Secrets



Apple and Android provide robust development platforms as well as full support for corporate development of internal applications as well as volume purchases of software and hardware. Apple recently surpassed 50 billion apps downloaded.

A simple search through the medical applications on iTunes turns up several familiar names offering full product lines to doctors, hospitals and other health care professionals. Companies offer electronic records, patient management, and medical imaging support on iPhones and iPads. There are applications that provide full medical office management tools with the mobile device having functionality surpassing the laptop.

Business applications abound as well. Many large software companies provide applications for collaboration and meeting management, as well as provide applications in support of their analysis and financial packages. IT departments can provide mobile support, VPN, remote desktop management, and document management from outside software vendors as well.

## **Recoverable Data**

Evidence that can be potentially recovered from a mobile phone may come from several different sources, including the SIM card and attached memory cards. The SIM contains all information necessary to identify the subscriber plus a limited number of text messages and call log records. Most information is recorded in the handset. The memory card if present will tend to be used to store pictures, video, games, applications, and music and is generally much easier to view than the device itself.

There are forensic tools on the market today (hardware and software based) that can recover SMS and MMS messages, photos, video and audio recordings, as well as previous calls made, received and missed, contact lists and phone IMEI/ESN information. This could be considered low hanging fruit or the initial analysis reports to aid in deciding if further action need be taken. Often the market has created tools with which the owner could access this information for management of the mobile device. These tools would not be considered anti forensic tools. Rather they are the efforts of an informed consumer adapting to the evolving technology landscape.

There is further information that can be found from web browsing, wireless network settings and or locations, as well as e-mail. This includes important data now retained or replicated in corporate applications. Investigations of mobile devices can string together both the time and location of an activity of interest, often down to the GEO Location of the activity in question.

## **Mobile Analysis**

The existing generation of devices is sophisticated and increasingly difficult to examine however they can provide valuable evidence. Internal memory and external memory can be analyzed to gain an insight into the activities of the user. Information obtained from a phone or mobile device, after intensive analysis techniques can be suitable for the case.

With so much data that can be found on mobile devices it can be difficult to differentiate or associate what is valuable data. There are visualization tools to help build timelines showing when calls or messages were made and when. One can use the cell tower data to possibly pinpoint and locate where certain calls or messages were made.





# Trading Secrets



Everywhere we look we see people consistently looking at their mobile devices. As these devices continue to evolve in storage capacity, processing power and Internet capabilities, they will begin to outnumber traditional computers two to one. It is becoming apparent and clear that ESI from these devices can be a goldmine for those attempting to discover relevant and valuable evidence. Manufacturers of mobile device hardware and software are constantly updating their forensic solutions to allow examiners the ability to acquire newer devices, in addition continued support on older devices.

The area is ever expanding and allows for cutting edge technology to be used to keep up with the growing array of mobile devices on the market today and the increasing feature list and applications. Mobile forensics will continue to be a specialized field while the forensic tools and technology progress rapidly.

*Mr. James Whitehead, a Manager at iDiscovery Solutions (“iDS”), has more than 15 years of experience managing technology and projects related to computer forensics, electronic discovery, and information governance. He has extensive experience with project management, forensic data collection, computer forensic analysis, data remediation strategies, as well as consulting clients for litigation readiness across the scope of EDRM.*

*Mr. Arnold Garcia is a Senior Consultant at iDiscovery Solutions (“iDS”). Mr. Garcia holds a Bachelors Degree in Technical Management Computer Information Systems. Mr. Garcia provides services in digital forensics, electronic discovery, technical support and forensic lab management. Mr. Garcia has recorded, collected, and imaged over one thousand different data sources, as well as numerous mobile devices.*

*Please note that each case may be unique and this single blog post is not intended to fully cover everything related to mobile device computer forensics or constitute advice, legal or otherwise. It is always best to consult a qualified person to assist with any investigation.*

# Trading Secrets



## Illinois Passes Social Media Legislation To Regulate Flash Mobs

*By Jessica Mendelson (June 7th, 2013)*

Think flash mobs are innocent fun? Well if you're in Illinois, proceed with caution. The Illinois legislature recently passed a bill which provides tougher punishments for people whose social media posts result in flash mobs. The bill was recently [signed](#) into law by Illinois Governor Pat Quinn.

The new law is [intended](#) to reduce violent events in Chicago, particularly the areas along Michigan Avenue, an area well known for high end stores and shops. This area has recently been the [site of flash mobs](#), resulting in robberies, stopped traffic, and frightened bystanders.



The new law, [SB 1005](#), provides that when a defendant is convicted of “attempted mob action, solicitation to commit mob action, or conspiracy to commit mob action” where the criminal object of the actions are “mob action” under [Section 25-1 of the Criminal Code of 2012](#), the court is entitled to extend the term sentence to three to six years. Previously, the punishment for inciting violence through social media posts carried a maximum sentence of only three years in prison.

Supporters of the law believe it will reduce violence in the city, and is necessary for reducing criminal activity. Illinois [Representative Ken Dunkin](#), explained, “These are new times where people are using electronic mechanisms to communicate to commit crimes in our neighborhoods. .. when criminals change with the times we have to adjust ourselves accordingly.” Similarly, [Representative Christian Mitchell](#), who sponsored the bill, agreed, explaining, the law gives police the “ability to keep up with the changing times.” Mitchell went on to cite the increased prevalence of social media among gangs for organizing purposes, and suggested this bill would provide a means to reduce the threat.

Opponents, by contrasts, think the law may punish accidental offenders who end up caught in the flash mob's path, or who post something on a social networking site which has unintended consequences. Furthermore, they argue the law will have limited impact on reducing violence, and will result in increased costs as a result of the longer jail sentences.

The law is emblematic of the increasing regulation of social media in the United States in recent months. [See our previous posts](#) on [social media legislation](#) for more information.

# Trading Secrets



## Oregon the Latest State to Pass Social Networking Privacy Legislation; Vermont Establishes Committee to Study and Recommend Such Legislation

By Scott A. Schaefers (June 7th, 2013)

### Oregon's Social Media Account Protection Act

On May 22nd, Oregon enacted its own social networking privacy law, becoming the thirteenth state nationwide to do so. The law aims to protect employee social-networking privacy by prohibiting their employers from requiring access to employees' accounts.

We previously blogged about similar legislation passed in [Washington state](#), [Utah](#), [New Mexico](#), [Arkansas](#), [California](#), [Illinois](#), and [Maryland](#), among others. The new Oregon statute shares some of the same features. Oregon employers are now prohibited from requiring employees and job applicants to (a) turn over account logins, or (b) allowing employer access to their accounts (i.e. by adding employer reps to their accounts, or opening accounts in the presence of employer reps). Nor can employers discipline or retaliate against employees, or refuse to hire applicants, for invoking the law's protection. The law was made part of Oregon's existing employment discrimination statutes, and thus allows the Attorney General's office or aggrieved employees or applicants to sue employers for money damages, a minimum \$200 penalty, punitive damages, injunctions, attorneys' fees, reinstatement, back pay, and 'other appropriate relief.'

Yet similar to Washington state's recently passed legislation, the Oregon statute also contains a number of concessions for employers. A plaintiff employee who loses his or her lawsuit against the employer is subject to having to pay the employer's attorneys' fees, albeit likely limited to instances where the claim was frivolous or brought in bad faith. A third party may not sue an employer (i.e. for negligent hiring or retention) for its 'failing' to request or require employee account logins. The law permits employers to require employees to provide 'personal' account access (but not through login disclosure) for an investigation into work-related misconduct involving the employee's use of the account. An employer is not liable for its 'innocent discovery' of protected employee logins while monitoring its own networks and devices (but the employer may not use the logins). And an employer may require logins for those accounts 'provided by, or on behalf of, the employer, or to be used on behalf of the employer.'

Which brings us to a fairly wide gap in the law's text, as we similarly described in our Washington post. The Oregon law does not define 'personal' accounts, or on the flip side, those which are 'provided by, or on behalf of, the employer, or to be used on behalf of the employer.' Court decisions in the last few years indicate that employers may have at least some ownership rights to [LinkedIn](#), [MySpace](#), and [Twitter](#) accounts which an employee uses for **both** personal and employment purposes, where the employer had a significant hand in creating, developing, or maintaining the account. The Oregon law's exception for employment-related accounts will likely have the same result. An employer can elude the statute by writing into its job description the requirement that employees create an





# Trading Secrets



account, or use their pre-existing accounts (even personal accounts), as part of their job duties, and by taking the appropriate corresponding measures. So, will the Oregon statute really achieve its intended purpose?

## **Vermont's New Social Media Privacy Committee**

On May 24th, Vermont passed a [law](#) which established a single-purpose 'Committee' to study and recommend possible social-networking privacy legislation. The Committee would include designated representatives of the Attorney General, Commissioners of Labor, Financial Regulation, Human Resources, Human Rights,<sup>[1]</sup> and Public Safety, as well as two appointed representatives of both employers and labor-unions, and a Vermont ACLU representative. The Committee must begin meeting before September 1, 2013 (with the Labor Commissioner as its chair), and must report to the Assembly by January 15, 2014.

The Committee's stated tasks include looking at existing and proposed state and federal privacy laws, including the 'interplay' between state and federal law, and considering other factors relevant to employee social-networking privacy. As we discussed in previous blogs, among the topics the Committee should consider are (1) more precisely defining 'personal' and 'employment' social-networking accounts (lest the confusion between protected and unprotected accounts, as explained in our [post](#) on the initial Washington privacy bill), and (2) the conceptual conflict between growing state privacy legislation, on the one hand, and the recent strengthening of federal trade secrets theft [laws](#) and enforcement [policy](#), on the other, which in significant part are for the benefit of American employers.

---

<sup>[1]</sup>More precisely, the Executive Director of the Human Rights Commissio

# Trading Secrets



## Nevada and Colorado Pass Employee Social Networking Privacy Laws

*By Scott Schaefer (July 1st, 2013)*

Nevada and Colorado recently passed employee social networking privacy laws. Both laws prohibit employers from requiring disclosure of employees' or applicants' personal social-networking account login information, and from retaliating against them for refusing to provide that information. But one or both of these statutes are somewhat different from other states' social networking laws in that:



1. The [Colorado law](#) does **not** allow employees or applicants to sue employer for violations. The law only permits employees to file complaints with the Department of Labor and Employment, which after investigation may fine or sue employers on employees' behalves. It does not appear that other parts of the Colorado labor / employment code authorize employee lawsuits.
2. Similarly, it is unclear what remedies Nevada employees and applicants have under that state's new law. The social media statute itself says nothing about remedies, even though its companion law passed at the same time – which prohibits mandatory employee credit information disclosure – does contain specific administrative remedies for employer violations. Perhaps employees will be able to file complaints with the Nevada Equal Rights Commission under NRS 233, but that is unclear, and if that were the case, their remedies seem to be limited to cease-and-desist orders, reinstatement, and back pay and benefits. Perhaps the law will be amended prior to its 10/1/13 effective date to clarify its remedies.
3. The [Nevada law](#) has no exceptions for employer investigations. It only says that it does not prohibit mandatory disclosure of non-**personal**-social-media account or device passwords in order to access employer-owned devices and networks. The Colorado law, on the other hand, contains the carve-outs and exceptions we see in other states' social media laws regarding employer investigations into alleged employee misconduct, proprietary- or financial-information theft, violations of other law, for compliance purposes, and lawful personnel-policy enforcement.

In addition, both of these laws have the same problems as most other social-media laws in effect: though they both prohibit mandatory disclosure of 'personal' SM account logins and information, neither defines 'personal account.' We've [blogged](#) a number of times on these definition gaps in the other SM privacy laws, as well as on the cases which say that the employer 'owns' its employee's SM account content, at least where the employer required SM account usage and assisted in the account's development, maintenance, and monitoring. An employer may be able to circumvent the law by requiring new or existing SM account usage and maintenance as a condition of employment, even though employees may use such accounts for personal reasons as well. Legislatures would do well to clarify the difference between 'personal' and 'employment-related' accounts.



# Trading Secrets



## New Jersey Becomes the Thirteenth State to Pass Employee Social Networking Privacy Legislation

*By Scott Schaefer (August 30th, 2013)*

On August 29, 2013, New Jersey Governor Chris Christie signed into [law](#) Assembly bill no. 2878 (fourth reprint), which prohibits employers from asking or insisting that their employees provide access to their personal social networking accounts. New Jersey is the thirteenth state to enact some form of employee social media networking legislation.

Once the law goes into effect, New Jersey employers will no longer be able, subject to exceptions described below, to 'request or require' employees or job applicants to turn over their account logins, disclose account content, or sign a waiver of any rights under the statute. (Section 7 of the statute says its effective date is the 'first day of the fourth month following enactment.' Because the bill was signed on 8/29/13, December 1, 2013 is probably that day (December 29th will be the 'fourth month' after passage). At the latest, the law will take effect on January 1, 2014). Any such waiver will be void. Nor may employers discipline employees or refuse to hire applicants based on their refusal to provide account access or content, or for reporting violations. Employers found in violation of the law are subject to civil penalties of up to \$1,000 for the first violation, and up to \$2,500 for each subsequent violation.



The law has plenty of concessions for employers, though. Only employees' and applicants' "personal" accounts are off limits. The law defines such accounts as those used "exclusively for personal communications unrelated to any business purposes of the employer," and excludes accounts that are "created, maintained, used or accessed" by employees or applicants "for business purposes of the employer or to engage in business related communications." Thus, accounts are fair game when employers require that employees open and use them for company business, and even arguably when an employee or applicant posts anything employer-related on his/her otherwise "personal" account.

Further, the law will not prohibit employers from complying with state or federal law, including the rules of self-regulatory organizations (i.e. NASD and FINRA). Employers may also regulate work-device and work-account usage, and may also require personal account access when the employer receives information that employees have used such accounts for work-related misconduct or to store employer proprietary assets or financial data without authorization. And employers will be free to find and use any information about employees and applicants in the public domain.

Perhaps most importantly for employers, the law only allows employees to report violations to the state Department of Labor and Workforce Development, which may then file a 'summary proceeding.' The fines mentioned above, if levied, go to the state, not to the complaining employees or applicants. Governor Christie conditionally vetoed the original version of the law, which allowed employees and applicants to file lawsuits for their own damages, back pay, benefits, injunctions, attorneys' fees, and costs. The governor struck that provision without specific comment (he only commented on the





# Trading Secrets



exceptions for required access), and the Assembly and Senate both unanimously passed the version without the lawsuit provisions.

New Jersey's limited remedies provisions are not uncommon. Of the thirteen states with social networking privacy laws, only Oregon's and Washington's statutes authorize civil lawsuits without capping damages. Other states either cap lawsuit damages at no more than \$1,000, or do not authorize lawsuits, instead limiting remedies to complaints with state agencies and fairly nominal penalties. And New Jersey's narrow definition of "personal" accounts is also consistent with most other states' laws, which limit their reach to personal accounts either expressly or by implication.

# Trading Secrets



## Nevada District Court Finds No Reasonable Expectation of Privacy in Private Twitter Posts

*By Erik von Zeipel (September 10th, 2013)*

In dismissing a claim for violation of Fourth Amendment rights, the United States District Court for the District of Nevada in [\*Rosario v. Clark County School District\*, No. 2:13-CV-362](#), 2013 U.S. Dist. LEXIS 93963 (Nev. Jul. 3, 2013) recently became the latest court to hold there is no reasonable expectation of privacy in Twitter tweets.



This case arises out of plaintiff Juliano Rosario's tweets about his high school's basketball team. Juliano tried out for the team in his senior year, but was initially cut. After his father protested the cut, Juliano was eventually given a spot on the team. Immediately following the final game of the season, Juliano made numerous sexually and racially offensive tweets about several school officials, including coaches and the athletic director. The school disciplined Juliano for "cyberbullying" after learning of the offensive tweets. Juliano and his father then filed a 10-count complaint against the school district and six of its employees alleging, among other things, that the defendants (the school district and several officials) violated Juliano's Fourth Amendment rights by searching his Twitter account.

In ruling on the defendants' motion to dismiss the Fourth Amendment claim, the Court recited Supreme Court [precedent](#) providing that a person has a constitutionally protected reasonable expectation of privacy when that person has both a subjective expectation of privacy and that expectation is one that [society recognizes as reasonable](#). The plaintiffs argued that Juliano had such a reasonable expectation of privacy in his tweets. The Court disagreed and explained that Twitter has two privacy settings: (1) "private," where tweets can arguably only be read by a tweeter's "followers"; and (2) "public," where tweets can be read by anyone. The Court reasoned that tweeters using the "public" setting intend that anyone who wants to read the tweet may do so, and there can therefore be no reasonable expectation of privacy. The Court opined that tweeters using the "private" setting have a "more colorable argument about the reasonable expectation of privacy in his or her tweets," but nevertheless held that such users are still "disseminating [] postings and information to the public, [and] they are not protected by the Fourth Amendment." [United States v. Meregildo](#), 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (relating to Facebook posts).

For purposes of ruling on the defendants' motion to dismiss, the Court assumed as true the plaintiffs' allegations that Juliano's Twitter account was "private," and not "public." The Court nevertheless concluded that Juliano had no reasonable expectation of privacy in his tweets, and that there was no Fourth Amendment violation when the school accessed his tweets through a follower's account after that follower gave the tweets to school officials. The Court concluded that it is [well-established](#) that a person who shares information with a third party takes the risk that that third party will share it with the government, and that the same logic applies in the social media context.

This decision may also help support the notion that social media followers may not constitute protectable trade secrets. (See also our previous blogs regarding trade secret protection for followers on [Twitter](#), [MySpace](#), and [LinkedIn](#)).

# Trading Secrets



## California Legislature Passes Bill To Extend Social Media Privacy Laws To Public Employers

*By Robert Milligan (September 17th, 2013)*

Big Brother can't ask for access to your "personal" social media accounts in the public hiring and employment setting except in certain narrow circumstances if Governor Jerry Brown signs a new social media privacy bill recently passed by the California legislature.

The California Senate [passed a bill](#) to extend California's social media privacy law to public employers last week.

The California Assembly previously passed the bill in May 2013.



The state sheriffs' association and probation officers [opposed the bill](#) because they argued it could hamper their ability to investigate potential employees.

They argued that they want to ensure that departments can appropriately screen applicants as necessary and requested an amendment that would exempt any position within a criminal justice agency from the provisions of the bill. No amendment was included in the bill that passed.

The legislation [will now go to](#) Governor Brown's desk for signature.

[Labor Code Section 980](#), which the California legislature passed last year and went into effect on January 1, 2013, prohibits employers from demanding access to job applicants' and employees' social media user names or passwords for the purpose of accessing personal social media, to access personal social media in the presence of the employer, or to divulge any personal social media content.

The new legislation adds language specifying that it applies to public employers. Specifically, "employer" means a private employer or a public employer and "public employer" means the state, a city and county, or a district. Additionally, the new legislation provides that **"[b]ecause of the crucial privacy rights at issue and the growing abuse of those rights, the Legislature finds and declares that this act addresses a matter of statewide interest and applies to public employers generally, including, but not limited to, charter cities and counties."** (emphasis added).

Unfortunately, while many have [questioned the need](#) for the previous legislation in California and other states, the new legislation does not address the deficiencies in Labor Code Section 980 that we have [blogged on](#), including a definition of "social media" that is far too broad because it governs effectively all digital content and activity and the lack of a definition of "personal" social media. Other states have provided more [narrow definitions of social media](#) and/or [provided](#) a definition of "personal" social media.

We will keep you posted on any material developments with the legislation.

# Trading Secrets



## District Court of New Jersey Continues Growing National Trend Permitting Employers to View “Publicly” Available Social Media Posts

*By Justin Beyer (September 19th, 2013)*

Following a growing recent national trend, Judge Martini of the District Court of New Jersey [issued summary judgment](#) to Defendants Monmouth-Ocean Hospital Service Corporation (“MONOC”) and two of its senior management employees on August 20, 2013, in a claim brought by a former nurse and EMT, Deborah Ehling, who accused MONOC of retaliation and other claims.

Ehling’s claims, in part, arose from MONOC’s alleged improper access of Ehling’s private Facebook posts. Holding that MONOC did not improperly access those posts under the Federal Stored Communications Act, 18 U.S.C. §§2701-11, (“SCA”) or New Jersey’s common law invasion of privacy tort, the District Court found that MONOC’s receipt of the communications from an authorized user satisfied an exception to the SCA.



Specifically, Ehling sought damages arising out of MONOC’s viewing and discipline of Ehling for a Facebook post she made in June 2009. The post in question related to a shooting at the National Holocaust Museum in June 2009. In that Facebook post, Ehling wrote:

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

Following that post, one of Ehling’s Facebook friends and another MONOC employee, Tim Ronco, provided a screenshot copy of the post to a MONOC manager, Andrew Caruso. Caruso, in turn, turned over this Facebook post (as well as others he received from Ronco) to Stacy Quagliana, one of the named defendants and MONOC’s Executive Director of Administration. After MONOC learned of the post, it temporarily suspended Ehling, with pay, and sent a memo that MONOC management was concerned that Ehling’s comment—made by a registered nurse and EMT—displayed a “deliberate disregard for patient safety.” Ehling unsuccessfully filed a complaint with the NLRB, who also found that no privacy violation occurred because MONOC was sent the post and did not acquire it on its own. Nearly three years later in February 2012, MONOC terminated Ehling, for cause, when she failed to return to work after her yearly FMLA leave time expired.

Ehling, however, argued that her termination and suspensions (other suspensions were discussed in the decision but not here) were pretext for MONOC retaliating against her for her role as president of



# Trading Secrets



the union within MONOC as well as her complaints to the State of New Jersey and OSHA for MONOC's use of a particular chemical at its facility.

Rejecting Ehling's argument that a SCA violation occurred, the Court [held](#) that, **while Ehling's non-public Facebook wall post was covered by the SCA**, one of the exceptions applied. Specifically, the District Court rejected Ehling's argument, finding that MONOC did not violate either the SCA or state law when it received **paper copies of Ehling's Facebook posts from one of Ehling's Facebook friends**.

Judge Martini's decision is important to employers for a number of reasons. First—like other recent Federal decisions—this decision continues to recognize that a distinction exists between public and private social media posts and that an employer cannot be liable for viewing public posts or receiving private posts from a third-party. See, e.g. "Nevada District Court Finds No Reasonable Expectation of Privacy in Private Twitter Posts", Erik B. von Zeipel, Sept. 10, 2013, <http://www.tradesecretslaw.com/2013/09/articles/social-media-2/nevada-district-court-finds-no-reasonable-expectation-of-privacy-in-public-twitter-posts/>, (commenting on *Rosario v. Clark County School District*, No. 2:13-cv-362, 2013 U.S. Dist. LEXIS 93963 (Nev. Jurisdictional. 3, 2013); see also *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (holding that Facebook posts disseminated to the public are not protected by the Fourth Amendment).

Second, the decision provides direction to employers that they may receive even private social media posts, but that they may not coerce or pressure their employees to provide such information. In offering such guidance, the court wrote: "Access is not authorized if the purported 'authorization' was coerced or provided under pressure." (Op. at p. 10.) In reaching that conclusion, the court relied on another New Jersey District Court decision, *Pietrylo v. Hillstone Rest. Grp.*, No. 06-5754, 2009 WU 3128420, at \* 3 (D.N.J., Sept. 25, 2009). While the court does not explain what might constitute coercion or pressure, employers should be mindful that its acts cannot be construed as either.

Finally, when coupling this decision with the various other social media decisions handed down over the last few years, a growing national trend is apparent. Essentially, courts are holding that employees lack a reasonable expectation of privacy in public social media posts and that even some private posts might become "public" if acts are taken by others to publish those posts to the public. A dividing line seems to be forming wherein employers cannot take covert actions to discover the content of employer social media posts, but, if those posts are disseminated publicly, the employer is likely not liable for disciplining an employee for violating its code of conduct through such social media posts.



# Trading Secrets



## Fourth Circuit Holds That Facebook “Like” Is Protected by the First Amendment

*By Jessica Mendelson (September 20th, 2013)*

Remember that Facebook photo of a friend’s vacation that you “liked” a couple of days ago? Well, congratulations, you’ve just exercised your constitutional right to free speech! This week, in an intensely followed case in the Fourth Circuit, the court [held](#) that “liking” something on Facebook is “a form of speech protected by the First Amendment.”

In [Bland v. Roberts](#), No. 12-1671 (4th Cir. Sept. 18, 2013), the former deputy sheriff of Hampton Virginia alleged he was fired because he had “liked” the Facebook page of a man opposing his boss in the race for sheriff of the city. Last year, a federal district court held that this was “insufficient speech to merit constitutional protection.” The district court found that, although First Amendment protection might apply to Facebook posts, such posts are actual statements in a way a “like” is not.



However, the Fourth Circuit disagreed, holding that liking the campaign page was the “Internet equivalent of displaying a political sign in one’s front yard, which the Supreme Court has held is substantive speech.” According to Judge William B. Traxler Jr, who wrote for the unanimous Court, “On the most basic level, clicking on the ‘like’ button literally causes to be published the statement that the User ‘likes’ something, which is itself a substantive statement.” Representatives for the ACLU expressed support for the ruling, stating, ““The Constitution doesn’t distinguish between ‘liking’ a candidate on Facebook and supporting him in a town meeting or public rally.”

The Fourth Circuit also revived claims of the former deputy sheriff, but noted, however, that even if the Sheriff were to lose the lawsuit, he would not be required to pay monetary damages, as he was entitled to qualified immunity under the 11th amendment.

Employers ought to take note of the court’s ruling, as it could signal a trend toward increased First Amendment protection of social media actions. Although at first glance the case [may not appear](#) to mean much to private employers, some legal commentators are predicting that the Court’s ruling “may foreshadow a decision by the National Labor Relations Board that workers’ ‘likes’ can be protected under federal labor law.” While the NLRB has not issued a ruling yet, such a ruling may not be a surprise considering its rulings regarding social media policies, which we have [previously blogged about](#). Furthermore, in certain states, such as Connecticut, where a [statute](#) prohibits employers from disciplining an employee based on his or her exercise of First Amendment rights, the court’s ruling suggests that even private employees (at least in the Fourth Circuit) cannot be fired for “liking” a page that an employer does not agree with.

We will continue to keep you posted on this emerging issue.



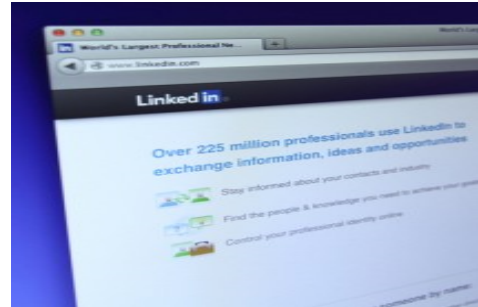
# Trading Secrets



## When does LinkedIn Activity Violate Non-Solicitation Agreements?

*By Erik von Zeipel (November 4th, 2013)*

LinkedIn is the biggest professional networking site in the world. It has more than 225 million users in more than 200 countries and territories. Approximately 75 million users are in the United States. Many of those users have signed non-solicitation agreements with their employers prohibiting them from soliciting the employers' customers and workers. Unfortunately, many of those non-solicitation agreements are not well-suited to address somewhat unique solicitation issues related to LinkedIn usage.



This article is intended to highlight some inherent problems associated with attempting to govern post-employment LinkedIn activity through traditional non-solicitation agreements, and to encourage employers to review and revise such agreements to better address issues posed by LinkedIn usage. While this article focuses on LinkedIn, similar issues arise from employees' use of other social networks.

### **The potential problem with traditional non-solicitation provisions and LinkedIn activity:**

Many employers require their employees to sign agreements containing non-solicitation provisions prohibiting employees from soliciting the employers' workers and customers after termination of their employment. By way of example, a basic provision may look something like this:

Employee agrees that during his/her employment with the company and for one (1) year after any termination of his/her employment, Employee will not directly or indirectly solicit or attempt to solicit, divert or hire away any person employed by the Company or any customer of the Company.

While this type of non-solicitation provision may do a reasonably good job of addressing the traditional solicitation scenario (setting aside potential enforceability issues), LinkedIn poses a number of challenges for which traditional provisions are not necessarily a good fit.

Consider, for example, what may happen when an employee leaves company X to go to work for company Y, a direct competitor to company X, and updates his LinkedIn profile to reflect his new position with company Y. In simplified terms, a number of things are likely to occur. First, the departed employee's contacts will automatically get an "update" on their LinkedIn home page indicating that the departed employee has a new job and suggesting that they "congratulate" the employee. Second, when the departed employee posts any messages, including messages about company Y, those messages will be automatically delivered to the employee's contacts on their LinkedIn home pages. Third, similar information may also be included in e-mails LinkedIn automatically sends to its users on a regular basis about their contacts. Fourth, the departed employee may send messages through LinkedIn to individual recipients just like regular e-mail. Finally, the departed employee may seek to "connect" with the former employer's employees and customers through LinkedIn.



# Trading Secrets



The above examples illustrate some of the special problems associated with LinkedIn in the non-solicitation context. By a simple profile update, the departing employee's entire network of contacts is immediately and automatically informed that the employee has left company X and is now working at company Y. Similarly, the departing employee may effortlessly push information about company Y to his contact network, including, potentially the former employer's employees and customers. While in this largely automated process, a departing employee may not have any intent to solicit anyone, it is easy to see how an employer may have various degrees of discomfort with some or all of the above things depending on the type of activity, the message, the target audience and the employer's overall sensitivity to solicitation issues. The question is what activity a court will find to be in violation of a non-solicitation provision.

## **Case law provides little guidance for when LinkedIn activity violates non-solicitation provisions:**

A few years ago, our firm represented an employer in an employee and customer "raiding" case. Departing employees were alleged to have violated non-solicitation provisions by soliciting former co-workers to work for their new employer and to take the former employer's customers with them. In addition to more traditional violations of the non-solicitation provisions, there were potential violations where some of the departing employees' former co-workers and customers received information through LinkedIn from some departing employees attempting to hype their new employer. While annoying to the former employer, it was not clear whether the contents of the messages actually constituted "solicitations" as prohibited by the non-solicitation provisions. It was also unclear whether the messages were specifically targeted at former co-workers or customers, or if all the departing employees' LinkedIn contacts received the same messages. At the time, it seemed like an interesting issue of first impression. Unfortunately, the case settled before the court addressed whether the former employees' LinkedIn activity violated their non-solicitation agreements.

A few more recent cases have also involved allegations of impermissible LinkedIn solicitations. For example, in *TEKSystems v. Hammernick*, a 2010 case filed in U.S. District Court for the District of Minnesota, TEKSystems filed suit against its former employee Hammernick for violating an agreement not to solicit TEKSystem's employees and customers to go to its competitors. Hammernick allegedly violated the agreement by communicating with TEKSystems employees via LinkedIn. Unfortunately, this case also settled without resolving the issue of when LinkedIn activity constitutes an impermissible solicitation.

Similarly, in *Graziano v. NESCO Service Company*, No. 1:09CV2661, 2011 U.S. Dist. LEXIS 33497 (N.D. Ohio Mar. 4, 2011), NESCO alleged that its former employee, Graziano, violated a severance agreement and non-solicitation provision which prohibited him from soliciting NESCO's employees. After Graziano was terminated, he set up a LinkedIn account and contacted some NESCO employees. NESCO sent a cease and desist letter to Graziano, alleging that his conduct violated the non-solicitation provision. When Graziano refused to stop his conduct, NESCO stopped paying severance benefits and Graziano filed suit against NESCO. This case also settled without addressing whether the LinkedIn activity violated the non-solicitation agreement.

Presumably, there have been other disputes involving LinkedIn and non-solicitation agreements. However, research has not uncovered any published court decisions specifically addressing when LinkedIn activity may violate a non-solicitation agreement.



# Trading Secrets



## **Considering LinkedIn activity in drafting non-solicitation agreements:**

Given the special challenges posed by LinkedIn activity in the non-solicitation context and the dearth of cases addressing the issue, employers are wise to carefully consider how they want to handle their employees' use of LinkedIn.

In addition to customary and traditional non-solicitation provisions, employers would be wise to work with attorneys to consider specific provisions addressing how they want departing employees to conduct themselves with respect to LinkedIn accounts and post-employment activity. Such provisions may include a combination of: (1) specifying the employer's ownership of LinkedIn accounts and contacts; (2) requiring departing employees to delete LinkedIn accounts, or to relinquish control over accounts to their former employers; (3) imposing limits on employees' contacts with co-workers and customers through LinkedIn; (4) requiring departing employees to delete LinkedIn contacts with co-workers and customers; and (5) requiring departing employees not to establish or re-establish such contacts through LinkedIn.

At the same time, employers must be mindful of the risk of violating employees' rights, including under the National Labor Relations Act and applicable state laws. Provisions that restrict employees' mobility may not be enforceable, and courts may impose liability for requiring employees to enter into invalid agreements as a condition of employment. For these reasons, and given the uncertainty of the law, employers would be wise to include severance clauses in their agreements in the event any particular provision is held to be invalid.

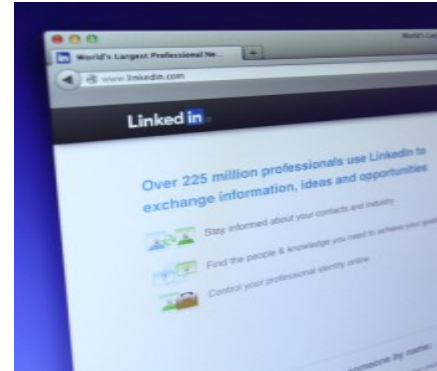
# Trading Secrets



## Massachusetts Judge Rules That Updating LinkedIn Does Not Constitute Solicitation

*By Erik Weibust (November 20th, 2013)*

Judge Thomas P. Billings, of the Massachusetts Superior Court's Business Litigation Session, recently [declined](#) to issue a preliminary injunction in a non-compete case brought by KNF&T Staffing, Inc. against its former employee, Charlotte Muller, who had left to join a competitor. Among other things, KNF&T alleged that Muller had updated her profile on LinkedIn to reflect her new position, "resulting in notification to all of Muller's 500+ LinkedIn contacts, including the numerous contacts she established during, and which were related to, her employment at KNF&T." Judge Billings rejected the argument, however, noting that her new firm does not compete with KNF&T in certain industries:



Quite simply, Muller was not and is not prohibited from soliciting or accepting any potential client – whether or not it is a present client of KNF&T – for recruitment of IT professionals, or anyone else in a field in which KNF&T does not recruit.

Judge Billings also noted that the same reasoning would apply to Muller's LinkedIn activities, where she listed only generic skills and responsibilities including "internet recruiting," "temporary staffing," "staffing services" and "recruiting":

There is no more specific mention of any of KNF&T's "Fields of Placement" than this. So long as Muller has not and does not . . . solicit or accept business in the Fields of Placement for herself or others . . . she will not have violated the covenant not to compete.

The decision is rather narrow, however, and the Court did not address whether a social media post could ever violate a restrictive covenant. As we have previously noted – in a blog [posting](#) from which Massachusetts Lawyers Weekly quoted extensively in an [article](#) about this case – the issue remains unresolved and decisions like the one issued by Judge Billings are at the forefront of this burgeoning area of law.

On a separate issue, whether a material change in Muller's employment voided her non-compete agreement, the Court assumed, but did not rule, "that Muller's promotions, and the corresponding increases in responsibility and compensation, did not constitute an abandonment of the covenant" under *F.A. Bartlett Tree Expert Co. v. Barrington*, 353 Mass. 585, 587-88 (1968). We have previously [blogged](#) about this issue as well, which also remains unresolved (as Judge Billings points out in a footnote).



# Trading Secrets



## **Acknowledgments:**

Special thanks to Lauren Leibovitch, Nicole Lumley and Bridget Rabb for their work in putting together this year in review.



Atlanta

Boston

Chicago

Houston

London

Los Angeles

Melbourne

New York

Sacramento

San Francisco

Shanghai

Sydney

Washington, D.C.

[www.seyfarth.com](http://www.seyfarth.com)

"Seyfarth Shaw" refers to Seyfarth Shaw LLP. Our London office operates as Seyfarth Shaw (UK) LLP, an affiliate of Seyfarth Shaw LLP. Seyfarth Shaw (UK) LLP is a limited liability partnership established under the laws of the State of Delaware, USA and is authorised and regulated by the Solicitors Regulation Authority with registered number 55692. Our Australian practice operates as Seyfarth Shaw Australia, an Australian multidisciplinary partnership affiliated with Seyfarth Shaw LLP, a limited liability partnership established in Illinois, USA. Legal services provided by Seyfarth Shaw Australia are provided only by the Australian legal practitioner partners and employees of Seyfarth Shaw Australia.