SEYFARTH SHAW

2014

YEAR IN REVIEW

Trading Secrets

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

Trading Secrets

Dear Clients and Friends,

2014 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 at the end of 2013. 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 2014 Year in Review, which compiles our significant blog posts from 2014 and highlights our blog's authors. For a general overview of 2014, we again direct you to our Top 10 2014 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2014 Trade Secrets Webinar Series - Year in Review blog entry, which provide a summary of key cases and legislative developments in 2014, 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 2014, we offered video blog posts, audio podcasts, more special guest authors, and provided an additional enhanced Resources page on the blog. We also created a special feature tracking the proposed federal trade secret legislation. We will also offer in 2015 additional content on recent developments in privacy, social media, and cybersecurity in 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 2014, we hosted 10 webinars, which are listed in this Review. For those who missed any of the programs in the 2014 webinar series, the webinars are available on compact disc upon request.

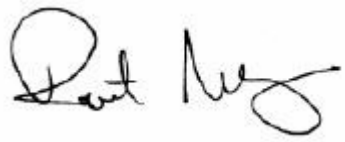
We are kicking-off the 2015 webinar series with a program entitled, "2014 National Year in Review: What You Need to Know About Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law." More information on our upcoming 2015 webinars is available in the program listing contained 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* leading firm.

Thank you for your continued support.

Michael Wexler

Practice Group Chair

Robert Milligan



Practice Group Co-Chair and Blog Editor

Trading Secrets

Table of Contents

Trading Secrets

2014 Trade Secrets Webinar Series

- 2013 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law
  March 6, 2014
- Employee Social Networking: Protecting Your Trade Secrets in Social Media
  April 24, 2014
- Barbarians at the Gate: Class Action Avoidance and Mitigation for Data Breach
  May 28, 2014
- Trade Secret and Non-Compete Legislative Update
  June 17, 2014
- International Trade Secrets and Non-Compete Law Update
  July 31, 2014
- Protecting Confidential Information and Client Relationships in the Financial Services Industry
  August 26, 2014
- Ins and Outs of Prosecuting and Defending Trade Secret Injunction Cases
  September 16, 2014
- Protecting Trade Secrets: The Current Landscape, Top Threats, Best Practices for Assessing and Protecting Trade Secrets, Proposed Legislation and Future Scenarios
  October 7, 2014
- How and Why California is Different When it Comes to Trade Secrets and Non-Competes
  October 28, 2014
- Protecting Trade Secrets and Intellectual Property in Business Transactions
  December 2, 2014

Trading Secrets

2015 Trade Secrets Webinar Line Up

- 2014 National Year in Review: What You Need to Know About the Recent Cases/ Developments in Trade Secrets, Non-Compete, and Computer Fraud
- Protecting Confidential Information and Client Relationships in the Financial Services Industry
- International Trade Secrets and Non-Compete Law Update
- Employee Social Networking: Protecting Your Trade Secrets in Social Media
- How and Why California is Different When it Comes to Trade Secrets and Non-Competes
- State Specific Non-Compete Oddities Employers Should be Aware Of
- So You Want An Injunction in A Non-Compete or Trade Secret Case

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.

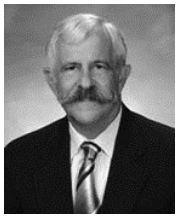
Robert Milligan is the Editor of the blog and Co-Chair of the national Trade Secrets, Computer Fraud, and Non-Competes Practice Group. His practice encompasses a wide variety of commercial litigation and employment matters, including general business disputes, unfair competition, trade secret misappropriation 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

Eric Barton is a counsel in the Litigation Department of Seyfarth Shaw LLP. For more than a decade, Mr. Barton has represented, advocated for, and advised clients in all forms of dispute resolution, including serving as lead trial counsel in numerous jury trials and arbitration proceedings throughout the Southeast. Recognizing that trial is typically not the ultimate goal for a client, Mr. Barton devotes a significant portion of his practice to advising and counseling clients on issues related to pre-trial resolution and avoidance of business disputes.

Razia Begum is an associate in the London office of Seyfarth Shaw (UK) LLP. Her focus is on all areas of employment law, both contentious and non-contentious. Ms. Begum advises clients on various contentious issues, including unfair dismissal, breach of contract and various discrimination claims. Ms. Begum's non-contentious work includes advising and assisting with the employment aspects of multi-jurisdictional corporate transactions, including share and asset sales, corporate restructurings and outsourcing. In particular, Ms. Begum has experience of advising on cross-border.



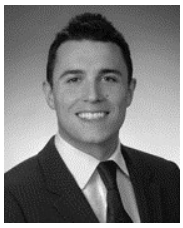
Jeffrey Berman is a partner in the Los Angeles office of Seyfarth Shaw LLP. A member of the Labor & Employment Department, he represents management in a variety of industries, including major medical centers, universities, religious organizations, manufacturers and restaurants.

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.

Jonathan Brophy is an associate in the Los Angeles office of Seyfarth Shaw LLP. A member of the Labor & Employment Department, he focuses his practice on discrimination, retaliation, harassment, and wrongful termination cases in state and federal court. Mr. Brophy also represents employers in wage and hour class actions in both state and federal court. Mr. Brophy has extensive experience in trial preparation, discovery, and law and motion.

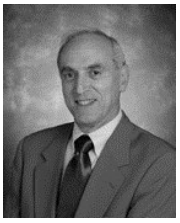
Trading Secrets

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.



Nicholas Clements is an associate in the San Francisco office of Seyfarth Shaw LLP, and is a member of the Labor & Employment practice group. Mr. Clements' practice focuses on all aspects of state and federal employment litigation. He has significant experience in wage and hour matters and has represented numerous employers in front of California's Division of Labor Standards Enforcement (DLSE) in settlement conferences and Berman hearings. Mr. Clements also defends employers in class action and single-plaintiff matters, and in a host of other California Labor Code matters. Additionally, his practice includes the defense of clients in employment discrimination claims under the California Employment and Housing Act, Title VII, and the Age Discrimination Act.

Ada Dolph is a partner in the Labor & Employment Department of Seyfarth Shaw LLP. She represents clients in a wide range of labor and employment matters, with an emphasis on employment discrimination, ERISA and whistleblower claims. She is a member of the Firm's ERISA & Employee Benefits Practice Group, as well as its Whistleblower and Health Care Fraud and Provider Billing Litigation Teams.



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

Matthew Hafter is a partner in the Chicago office of Seyfarth Shaw LLP and serves as vice co-chair of the firm's national Capital Markets practice. Mr. Hafter represents clients in diverse corporate and commercial matters, including venture capital transactions; mergers, acquisitions, and divestitures; public and private securities offerings; securities reporting and compliance matters; corporate governance matters, and commercial credit and secured lending transactions.

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.

Ming Henderson is a partner in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP's London office. She is qualified in both France and the UK. Before joining the firm, Ms. Henderson worked as an in-house employment counsel for a global software and hardware company covering Europe Middle-East and Africa (EMEA). She was also previously head of the EMEA Employment Law Practice for a global financial institution in the UK.

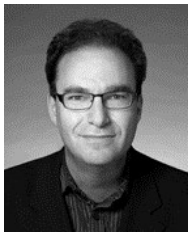
Cassie Howman-Giles is a senior associate in Seyfarth Shaw Australia's International Labour & Employment practice in Sydney. She has over 7 years of experience advising clients in respect of employment and workplace relations law in both Australia and the UK.

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.

Trading Secrets

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.

Adam Laughton is an associate in the Corporate department of Seyfarth Shaw LLP's Houston office. His practice focuses on the healthcare industry and sourcing matters. Mr. Laughton has served hospital and health system clients in mergers and acquisitions of other healthcare providers, False Claims Act litigation and Medicare/Medicaid reimbursement and regulatory issues.



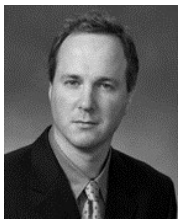
Bart Lazar is a partner in the Chicago office of Seyfarth Shaw LLP. He counsels clients in intellectual property, data privacy and security, advertising, promotion and related matters. Mr. Lazar helps clients structure and implement strategies to comply with domestic and international data privacy and security laws and respond to actual and potential security breach incidents. Mr. Lazar has handled numerous privacy matters before federal and state agencies, including defending the first Internet privacy case brought by the Federal Trade Commission and the first database security breach case brought by the New York Attorney General.

Wan Li is a partner in the Shanghai office of Seyfarth Shaw LLP. He has over 20 years of experience in China-related matters advising a diverse range of clients in employment, mergers and acquisitions (corporate and cross-border), private equity and corporate matters including restructuring. Wan Li has a broad practice focused on foreign direct investments into China and representing Chinese companies in relation to multinational transactions including acquisition of equity and assets of telecommunication, internet, high-tech, energy and resources, medicine and dairy products companies.

Andrew Masak is an associate in the Atlanta office of Seyfarth Shaw LLP and is a member of the firm's Labor & Employment department. Mr. Masak represents employers in all aspects of labor and employment issues, including the National Labor Relations Act, arbitration, collective bargaining, discrimination, workplace harassment and retaliation claims under Title VII of the Civil Rights Act of 1964, the Age Discrimination in Employment Act, the Americans with Disabilities Act, and other state and local statutes, as well as various other common law torts and employment contractual disputes.

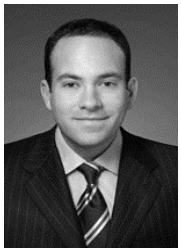
Trading Secrets

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.



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. He 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.

Dawn Mertineit is an associate in the Litigation Department of Seyfarth Shaw LLP. Ms. Mertineit specializes in non-compete and trade secrets litigation, representing both plaintiffs and defendants in state and federal courts, from pre-litigation counseling through to judgment or settlement, as well as advising her clients on their non-compete agreements and other restrictive covenants. Ms. Mertineit also has experience litigating a variety of employment actions, Computer Fraud and Abuse Act claims, partnership disputes, banking and finance matters, breach of contract suits, product and premises liability actions, real estate disputes, construction claims, and various tort actions.



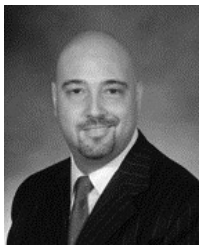
Marcus Mintz is a senior associate in the Chicago office of Seyfarth Shaw LLP. Mr. Mintz's practice focuses on complex commercial litigation, including cases involving post-merger disputes, misappropriation of trade secrets and intellectual property, equity rights, and business tort claims. Mr. Mintz 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.

Trading Secrets

Anthony Orler is senior counsel in the Los Angeles-Century City office of Seyfarth Shaw LLP. Mr. Orler practices in the Intellectual Property arena, where his focus is on foreign and domestic patent prosecution and client counseling. He has experience in patent litigation, and drafts non-infringement and validity opinions for clients in the electrical/mechanical arts.

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.

Christopher Robertson is Co-Chair of the National Whistleblower Team and a member of the Complex Litigation, Capital Markets and Investment Management practice areas in the Boston Office of Seyfarth Shaw LLP. His areas of focus include complex commercial and financial litigation, securities litigation, consumer fraud litigation, regulatory compliance, corporate governance, and internal investigations.



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.

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. Mr. Salinas' experience includes the prosecution and defense of trade secret misappropriation and unfair competition claims.

Trading Secrets

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.

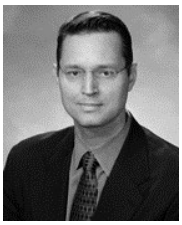
Jason Stiehl is a partner in the Litigation Department of Seyfarth Shaw LLP. Mr. Stiehl represents clients in complex commercial disputes involving trade secrets and restrictive covenants, unfair competition, corporate espionage, contract, and intellectual property claims in both state and federal court.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

Robert Szyba is an associate in the Labor & Employment department in the New York office of Seyfarth Shaw LLP. Mr. Szyba's practice focuses on litigating employment law matters before state and federal courts, both trial and appellate levels, as well as federal and state administrative agencies, including the Equal Employment Opportunity Commission, Department of Labor, New Jersey Division on Civil Rights, New Jersey Office of Administrative Law, and New York State Division of Human Rights. He has litigated claims involving restrictive covenants, such as non-compete agreements, non-solicitation agreements, confidentiality agreements, and misappropriation of trade secrets. In addition to his litigation practice, Mr. Szyba regularly advises clients about pre-litigation strategy and litigation avoidance, employment contracts, employment policies and procedures, privacy considerations, and minimizing exposure to liability.

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.

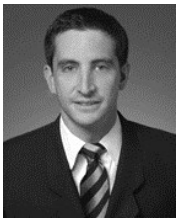
Justine Turnbull is a partner in the Sydney office of Seyfarth Shaw LLP. Mr. Wan has over 20 years of experience in China-related matters advising a diverse range of clients in employment, mergers and acquisitions (corporate and cross-border), private equity and corporate matters including restructuring. He has a broad practice focused on foreign direct investments into China and representing Chinese companies in relation to multinational transactions including acquisition of equity and assets of telecommunication, internet, high-tech, energy and resources, medicine and dairy products companies.

Trading Secrets



Erik von Zeipel is a partner in Seyfarth Shaw's Los Angeles office. A member of the firm's Litigation department, Erik maintains a broad litigation and counseling practice representing businesses in a variety of areas. Erik has significant experience in complex litigation, including class actions, trade secrets, breach of contract, unfair competition, construction, and real estate lawsuits.

Erik Weibust is a partner in the Litigation Department of Seyfarth Shaw LLP, and is a member of the Securities & Financial Litigation and Trade Secrets, Computer Fraud & Non-Competes practice groups, and an active member of the firm's national Whistleblower Team. Mr. Weibust regularly represents clients in disputes involving trade secrets and restrictive covenants, shareholder disputes, consumer class actions, and claims of unfair competition, fraud, and commercial disparagement, among other matters.



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

Candice Zee is a partner in the Los Angeles office of Seyfarth Shaw LLP. As a member of the Labor & Employment Department and Single Plaintiff Litigation and Wage and Hour Practice Groups, she has substantial experience in defending employers against class action and single-plaintiff claims for alleged wage and hour violations, discrimination, harassment, retaliation, and violation of public policy, as well as workplace torts, including defamation, emotional distress, and interference with contractual relations. Ms. Zee has taken and defended numerous depositions and conducted several factual investigations. She frequently appears and argues on behalf of clients at state and federal courts. She also has extensive trial experience and has litigated multiple trials.

Trading Secrets

2014 Summary Posts

- 2014 Trade Secrets Webinar Series – Year in Review
  By Robert Milligan and Michael Wexler (December 18, 2014)

- Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2014
  By Robert Milligan and Daniel Hart (January 6, 2015)

Trade Secrets Legislation

- Latest Updates on Federal Trade Secrets Legislation
  By Robert Milligan and Joshua Salinas (September 8, 2014)

Trade Secrets

- Texas Appellate Court Affirms Multi-Million Dollar Jury Verdict For Trade Secret Misappropriation in Gas Drilling Dispute
  By Paul Freehling (January 10, 2014)

- "But I'm a Whistleblower!": Is an Employee Who Takes Confidential Documents Invincible?
  By Christopher Robertson (February 4, 2014)

- Texas Trade Secrets Decision Helps Energy Companies
  By Randy Bruchmiller (February 6, 2014)

- Loose Lips Sink Ships! Can an Employer Ask a Whistleblower to Keep Her Complaints "Confidential"?
  By James Beyer (February 10, 2014)

- Massachusetts Court Confirms That When It Comes To Trade Secrets, Confidentiality Is Key
  By Dawn Mertineit (February 14, 2014)

- Tricks of the Trade Secrets – Can Casino Applications Be Kept Confidential?
  By Erik Weibust and Dawn Mertineit (February 28, 2014)

- Global Business 101: Hire Your Competitor as a "Consultant"
  By Anthony Orler (March 20, 2014)

- Trade Secrets: A New Framework
  By Guest Author, Pamela Passman of CREATe.org (March 24, 2014)

Trading Secrets

- The Two Billion Dollar Zhu Zhu Pet, Sold for $5k: Puffing in Trade Secret Misappropriation Pleadings May be Perilous
  By Anthony Orler (March 27, 2014)

- Tips for Ensuring Your Competitors Do Not Steal the Valuable Fruits of Your Research and Development
  By Kate Perrelli and Erik Weibust (March 28, 2014)

- Covert Cellular: Enough Protection for Trade Secrets?
  By Anthony Orler (April 8, 2014)

- Jury's $920 Million Trade Secret Misappropriation Verdict Vacated
  By Paul Freehling (April 9, 2014)

- Randy Bruchmiller Discussing the Finer Points of the Texas Uniform Trade Secrets Act
  By Randy Bruchmiller (April 14, 2014)

- Patent and Trade Secret Protection: Turning Nightmares into Sweet Dreams
  By Anthony Orler (April 24, 2014)

- Bad Practices for Interviewing Competitors' Employees and Dealing with Departing Employees
  By Robert Milligan and Joshua Salinas (May 5, 2014)

- Tips for Avoiding Liability for Trade Secret Misappropriation Concerning the Hiring and Departure of Employees
  By Robert Milligan and Joshua Salinas (May 9, 2014)

- Not Easy Being Green: Trade Secret Holders May Be Singing the Blues Over Green Chemistry
  By Anthony Orler (May 14, 2014)

- Employees Strike Back Against Former Employer For Alleged Bogus Claim of Trade Secret Misappropriation
  By Paul Freehling (June 3, 2014)

- Seyfarth Attorney to Present on Protecting Pharmaceutical Trade Secrets at the Chinese Biopharmaceutical Association's Annual Meeting
  By Justin Beyer (June 19, 2014)

- Josh Salinas Explains How Drones Could Pose a Threat to the Protection of Trade Secrets
  By Joshua Salinas (June 29, 2014)

- Legal 500 Names Seyfarth Shaw as a Finalist for Top Trade Secrets Litigation Department in the U.S.
  By Robert Milligan (July 1, 2014)

Trading Secrets

- Texas Federal Court Imposes Ongoing Royalty Rather Than Permanent Injunction Against Alleged Trade Secret Misappropriator
  By Shashank Upadhye (July 15, 2014)

- $16 Million Awarded By Arbitrator Against 50 Cent in Trade Secret Spat
  By Christina Jackson (July 16, 2014)

- Preliminary Injunction Entered After Texas Federal Court Concludes That Ex-Employee "Inevitably" Will Disclose His Former Employer's Trade Secrets
  By Paul Freehling (July 24, 2014)

- Eighth Circuit Affirms $31.1 Million Dollar Jury Verdict in Favor of Hallmark Cards over Private Equity Firm
  By Timothy Hsieh (July 25, 2014)

- There Are Many Ways to Milk a Cow and Not All Are Protected Trade Secrets
  By Sarah Izfar (July 29, 2014)

- Steps to Protect Trade Secrets in the Non-Profit Sector and Balance the Need for Transparency
  By Andrew Masak (August 19, 2014)

- Trade Secret Mediation: Advice from a Mediator's Perspective
  By Guest Author, Erica Bristol of EB Resolution Services (September 3, 2014)

- Today's Connected Employee: A License to Steal
  By Guest Author, Trent Livingston of iDiscovery Solutions (September 25, 2014)

- When "The End" Is Not "The End": Asserting Trade Secret Claims After The Execution of a Mutual Release
  By Eric Barton (October 3, 2014)

- High Times in Trade Secrets
  By Anthony Orler (October 7, 2014)

- Trade Secret Attorneys Discuss Latest Issues in Trade Secret Litigation in Corporate Disputes Magazine
  By Robert Milligan and Michael Wexler (October 13, 2014)

- Pythagoras and the Geometry of Intellectual Property: Where Do Trade Secrets Fit In?
  By Anthony Orler (October 16, 2014)

- "Bridgegate" Triggers Proposed Expansion of New Jersey Whistleblower Protections
  By Ada Dolph, Robert Syzba and Jade Wallace (October 20, 2014)

Trading Secrets

- Don't Come to a Trade Secret Fight with a Patent Law Defense
  By Michael Baniak (November 10, 2014)

- Seyfarth Attorneys to Present Paper on Trade Secrets and Lawyer Mobility at AIPLA Trade Secret Summit
  By Daniel Hart and Erik Weibust (November 17, 2014)

- Seyfarth Team Co-Edits and Co-Authors Prominent New Trade Secret Protection and Litigation in California Treatise
  By Robert Milligan (December 1, 2014)

- Has the Patent Fee Shifting Analysis of Octane Fitness Influenced Fee Shifting in Trade Secret Cases?
  By Matthew Werber (December 2, 2014)

- California Court Extends Protections To "Silent Whistleblowers"
  By Jeffrey Berman and Jonathan Brophy (December 5, 2014)

- USPTO To Host Trade Secret Symposium
  By Joshua Salinas and Robert Milligan (December 17, 2014)

- Arizona Supreme Court Holds that UTSA Does Not Preempt Common Law Claims for Misuse of Confidential Information That Is Not a Trade Secret
  By Daniel Hart (December 17, 2014)

- Seyfarth Attorneys Present At 2014 American Intellectual Property Association Trade Secret Summit
  By Erik Weibust, Daniel Hart, and Andrew Masak (December 19, 2014)

Computer Fraud and Abuse Act

- Nosal Update: Nosal Sentenced to One Year in Federal Prison
  By Erik von Zeipel (January 9, 2014)

- Courts Disagree on Meaning of "Interruption of Service" When Determining Loss Under the Computer Fraud And Abuse Act
  By Paul Freehling (March 17, 2014)

- Computer Fraud and Abuse Act Claims in the First Circuit – Will the Narrow Approach Prevail?
  By Dawn Mertineit (March 25, 2014)

- Third Circuit Signals Pro-Defendant Interpretation of the Computer Fraud and Abuse Act's "Authorized Access" Provisions
  By Scott Schaefers (April 16, 2014)

- Louisiana District Court Extends Pro-Employer Interpretation of the Computer Fraud and Abuse Act's "Authorized Access" Provisions to Impose Civil Liability on Former Employee
  By James Beyer (May 2, 2014)

Non-Competes & Restrictive Covenants

- Federal Court in Alabama Rules That Non-Compete Signed Prior to Employment is Void
  By Bob Stevens and Daniel Hart (January 16, 2014)

- Illinois Federal Court Finds Only 15 Months' Employment Sufficient Consideration For Non-Compete Agreement
  By Paul Freehling (February 7, 2014)

- Texas And North Carolina Appellate Courts Repulse Efforts To Enforce Restrictive Covenants
  By Paul Freehling (February 26, 2014)

- Beware: Over-Inclusive Non-Compete Agreement May Be Unenforceable
  By Paul Freehling (March 21, 2014)

- Ohio Court Issues Significant Non-Compete Decision: Damages for a Breach are the Payor's Lost Profits, Not the Amount of Consideration
  By Paul Freehling (April 23, 2014)

- Massachusetts Moves to Ban Non-Competes – Dawn Mertineit Explains What Employers Should Do Now
  By Dawn Mertineit (April 28, 2014)

- Unemployment Compensation Awarded To Ex-Employee Refusing Employer's Order To Execute Non-Compete Covenant
  By Paul Freehling (May 1, 2014)

- Hiring Employees with Non-Compete Agreements: Tread Lightly
  By Sarah Izfar (May 6, 2014)

- Bob Stevens Reflecting On Georgia's Non-Compete Law at its Third Anniversary
  By Bob Stevens (May 15, 2014)

- Employee's Competition With Former Employer Restricted Despite Absence Of Signed Non-Compete
  By Paul Freehling (May 21, 2014)

- Divided Appellate Court Voids Employer's Non-Compete Covenants Because One Employee Did Not Sign
  By Paul Freehling (June 18, 2014)

Trading Secrets

- Enforcing Non-Compete Agreements in the Pharmaceutical Industry
  By Kate Perrelli and James McNairy (June 19, 2014)

- Florida Court Finds That Employer Without Knowledge That Employees It Just Hired Have Non-Competes Are Not Liable For Tortious Interference With Contract
  By Paul Freehling (July 9, 2014)

- Eleventh Circuit Affirms Alabama Federal Court Ruling that Non-Compete Signed Prior to Employment is Void
  By Daniel Hart (July 14, 2014)

- Seyfarth Offers 2014-2015 Edition of 50 State Desktop Reference: What Employers Need to Know About Non-Compete and Trade Secrets Law
  By Robert Milligan (July 17, 2014)

- Rebecca Woods on Recent Kentucky Supreme Court Decision Holding that Non-Compete Failed for Lack of Consideration
  By Rebecca Woods (July 22, 2014)

- Liquidated Damages, A Permanent Injunction, and Attorneys' Fees Awarded For Violating Non-Disclosure/Non-Compete Agreement And Preliminary Injunction
  By Paul Freehling (July 31, 2014)

- Seyfarth Attorneys Present on Latest Developments in Trade Secrets and Non-Compete Law At ABA Annual Meeting
  By Kate Perrelli and Robert Milligan (August 7, 2014)

- Appellate Court Orders Trial Judge To Rewrite Parties' Non-Compete Covenant To Make It Enforceable
  By Paul Freehling (August 27, 2014)

- Ten-Day Interruption In Employment Necessitates New Non-Compete
  By Paul Freehling (September 12, 2014)

- Non-Compete and Forum Selection Clauses in Franchise Agreement Binding on Franchisee Who Signed It and on His Wife Who Didn't
  By Paul Freehling (September 23, 2014)

- Competitor Avoids Injunction Because Competition Was Not Significantly Aided And Abetted By A Signatory To Non-Compete
  By Paul Freehling (September 26, 2014)

Trading Secrets

- Customer Non-Solicitation Covenant Runs From Date Employment With Asset Seller Terminated, Not From Later Date Employment With Asset Purchaser Ended
  By Paul Freehling (October 20, 2014)

- Non-Compete And Non-Solicitation Covenants Contained In Bovine Artificial Insemination Employment Agreements Held Unenforceable
  By Paul Freehling (October 28, 2014)

- Non-Compete And Confidentiality Clauses In A Beverage Maker's Contracts With A Bottler And A Consultant Held To Be Unenforceable
  By Paul Freehling (November 25, 2014)

- Court Thwarts Employer's Effort To Block Vested Profit-Sharing Plan Participant from Obtaining Employment with a Competitor
  By Paul Freehling (December 8, 2014)

- No Stick Without a Carrot: UK Court Refuses to Enforce Post-Employment Restrictive Covenants
  By Razia Begum (December 16, 2014)

- Court Refuses To Enforce Settlement Agreement Containing Non-Compete Covenant Citing Lack of Assent
  By Paul Freehling (December 23, 2014)

Legislation

- Breaking News: Massachusetts Governor Deval Patrick to Propose Legislation Eliminating Non-Compete Agreements in Certain Industries
  By Erik Weibust and Dawn Mertineit (April 10, 2014)

- Update: Massachusetts Governor Proposes Sweeping Legislation Banning Non-Compete Agreements
  By Kate Perrelli, Erik Weibust and Dawn Mertineit (April 17, 2014)

- Massachusetts Governor Proposes Sweeping Legislation Banning Non-Compete Agreements
  By Kate Perrelli, Erik Weibust and Dawn Mertineit (April 18, 2014)

- Big Changes May Be Ahead for the Nation's Trade Secret Laws
  By Robert Milligan and Joshua Salinas (May 13, 2014)

- Robert Milligan Explaining the Defend Trade Secrets Act of 2014
  By Robert Milligan (May 19, 2014)

Trading Secrets

- Inching Closer to California: An Update on Massachusetts Non-Compete Legislation
  By Erik Weibust and Dawn Mertineit (June 11, 2014)

- Another Public Hearing Scheduled for Massachusetts Non-Compete Bill: What's Next
  By Kate Perrelli and Erik Weibust (June 27, 2014)

- On the Eve of The Esplanade July 4th Fireworks Celebration – Massachusetts May Not Blow Up Non-Competes After All – A Compromise is in the Air
  By Kate Perrelli (July 2, 2014)

- No Massachusetts Non-Compete or Trade Secret Legislation This Year
  By Kate Perrelli, Erik Weibust and Dawn Mertineit (July 21, 2014)

- Push for Federal Trade Secret Legislation Gaining Momentum
  By Robert Milligan (August 13, 2014)

- Massachusetts Governor Makes Last Ditch Effort to Pass Non-Compete Legislation Before His Term Ends
  By Erik Weibust and Dawn Mertineit (August 25, 2014)

- House Judiciary Committee to Consider Federal Trade Secret Legislation
  By Robert Milligan and Joshua Salinas (September 9, 2014)

- House Judiciary Committee Considers Federal Trade Secret Legislation
  By Robert Milligan and Joshua Salinas (September 17, 2014)

International

- Chinese Espionage Latest Target: Correction Fluid
  By Anthony Orler (March 11, 2014)

- Recent Decision Affirms Significant Protections for Confidential Information in United Kingdom
  By Ming Henderson and Razia Begum (March 26, 2014)

- Australia Non-Compete Primer: Protecting Your Business Interests Post-Employment
  By Justine Turnbull and Cassie Howman-Giles (March 31, 2014)

- European Commission Proposes Directive for Trade Secrets Protection in EU
  By Daniel Hart, Razia Begum and Andrew Masak (May 7, 2014)

- Seyfarth Attorneys Lead Discussion of Proposed EU Trade Secrets Directive at ITech Law World Technology Conference
  By Daniel Hart (May 16, 2014)

Trading Secrets

- Once You've Made Your Restrictive Covenant Bed You Must Lie Upon It…
  By Ming Henderson and Razia Begum (July 30, 2014)

- When Is The Possession of International Trade Secrets A Mistake Or Economic Espionage: Contrasting U.S. v. Yeh with U.S. v. Liew
  By Timothy Hsieh (August 5, 2014)

- United Kingdom Update on Contractual Notice Periods and Restrictive Covenants
  By Ming Henderson and Georgina McAdam (August 7, 2014)

- Kansas Federal Court Denies Preliminary Injunction For Alleged Violation Of Confidentiality And Non-Compete Covenants under Canadian Law
  By Paul Freehling (August 11, 2014)

- The French Answer To Flexible Working: The Right To Privacy and To Limit Work After Business Hours
  By Ming Henderson (August 19, 2014)

- Shanghai Courts Provide Additional Relief to Employers for Breach of Non-Compete Agreements
  By Wan Li (August 20, 2014)

- What You Need to Know About Non-Compete Covenants in India
  By Guest Authors, Sajai Singh and Soumya Patnaik of J. Sagar Associates (August 22, 2014)

- What You Need to Know About Trade Secrets in India
  By Guest Authors, Sajai Singh and Soumya Patnaik of J. Sagar Associates (August 22, 2014)

- Seyfarth Attorneys Facilitate Discussion On Trade Secret Protections and Legislative Developments in US and EU at ITechLaw 2014 European Conference
  By Robert Milligan and Ming Henderson (October 17, 2014)

- French Court Rules That A Confidentiality Clause Does Not Require Any Financial Compensation to Be Lawful
  By Ming Henderson (November 20, 2014)

- Proposed New Rules on Trade Secrets in Europe – the European Commission Proposal on the Protection of Know-How
  By Guest Author, Bartosz Sujecki (December 1, 2014)

- First United Kingdom Decision on Tweeting in Workplace
  By Ming Henderson and Razia Begum (December 22, 2014)

Trading Secrets

Social Media and Privacy

- Tips For Protecting Trade Secrets In The Social Media Age
  By Erik Weibust (January 4, 2014)

- Big Data and IP Business Strategy
  By Guest Author, Joren De Wachter of Belisarius BVBA (March 19, 2014)

- California Attorney General Provides Some Guidance on Cybersecurity
  By John Tomaszewski (March 27, 2014)

- Scott Schaefers Discussing Employee Social Media Privacy – How Employers Can Strike the Necessary Balance
  By Scott Schaefers (April 18, 2014)

- Heartache from Heartbleed – The Security of Open Source
  By John Tomaszewski (April 25, 2014)

- Trading Secrets is on Twitter, Facebook, Google+, Tumblr, YouTube, and LinkedIn
  By Robert Milligan (April 29, 2014)

- Seyfarth Shaw's Social Media Privacy Legislation Desktop Reference
  By Robert Milligan (April 30, 2014)

- Talking About Big Data: A Framework
  By John Tomaszewski (May 7, 2014)

- Massachusetts Social Media Privacy Bill Hits A (Small) Bump In The Road
  By Erik Weibust (July 1, 2014)

- John Tomaszewski Explains the Supreme Court's Riley v. California Decision and What It Means for Consumer Privacy Going Forward
  By John Tomaszewski (July 7, 2014)

- Time to Party Like It's 1999… Again: Information Technology Returns to Center Stage
  By Matthew Hafter (July 8, 2014)

- NLRB Rules That "Liking" A Facebook Comment Is Protected Activity
  By Jeffrey Berman and Candice Zee (August 27, 2014)

- Security Breach Liability – Its Complicated
  By John Tomaszewski (October 6, 2014)

- Cybersecurity: Coming to an Office Near You
  By Anthony Orler (October 20, 2014)

Trading Secrets

- Seyfarth Attorneys Facilitate Discussion On Cybersecurity and Protecting Valuable Trade Secrets at the 39th Annual Intellectual Property Institute Conference
  By Robert Milligan (November 4, 2014)

- Connecticut Supreme Court Grants Private Action for HIPAA Breach
  By Adam Laughton (November 11, 2014)

- Union Files NLRB Complaint Regarding the USPS' Handling of Security Breach Involving Employee Personal Information
  By Bart Lazar (November 19, 2014)

- NLRB "Deletes" Employer Email Rule
  By Jeffrey Berman and Nick Clements (December 15, 2014)

2014 Summary Posts

2014 Trade Secrets Webinar Series Year in Review

By Robert Milligan and Michael Wexler (December 18, 2014)

Throughout 2014, Seyfarth Shaw LLP's dedicated Trade Secrets, Computer Fraud & Non-Competes Practice Group hosted a series of CLE webinars that addressed significant issues facing clients today in this important and ever changing area of law. The series consisted of 10 webinars:

1. 2013 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law
2. Employee Social Networking: Protecting Your Trade Secrets in Social Media
3. Barbarians at the Gate: Class Action Avoidance and Mitigation for Data Breach
4. Trade Secret and Non-Compete Legislative Update
5. International Trade Secrets and Non-Compete Law Update
6. Protecting Confidential Information and Client Relationships in the Financial Services Industry
7. Ins and Outs of Prosecuting and Defending Trade Secret Injunction Cases
8. Protecting Trade Secrets: The Current Landscape, Top Threats, Best Practices for Assessing and Protecting Trade Secrets, Proposed Legislation and Future Scenarios
9. How and Why California is Different When it Comes to Trade Secrets and Non-Competes
10. Protecting Trade Secrets and Intellectual Property in Business Transactions

As a conclusion to this well-received 2014 webinar series, we compiled a list of key takeaway points for each webinar, 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 below of each webinar for the online recording. We are pleased to announce that Seyfarth will continue its trade secrets webinar programming in 2015 and has several exciting topics lined up. We will release the 2015 trade secrets webinar series in the coming weeks.

Trading Secrets

2013 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, James McNairy and Joshua Salinas, reviewed noteworthy cases and other legal developments from across the nation in the areas of trade secret and data theft, non-compete enforceability, computer fraud, and the interplay between restrictive covenant agreements and social media activity. They also provided predictions for what to watch for in 2014.

- While courts continue to struggle with what is the proper scope of trade secret preemption and at what stage in the case it should be applied (e.g., at the motion to dismiss/demurrer vs. summary judgment stage), courts increasingly hold that trade secret claims preempt or "supersede" concurrently pled common law tort claims based on the theft of information.
- The U.S. Supreme Court's decision in *Atlantic Marine Const. Co., Inc. v. U.S. Dist. Court for W. Dist. of Texas*, 134 S. Ct. 568 (2013), appears to strengthen the enforceability of forum selection clauses as it held that, where the other requirements for transferring an action exist, courts ordinarily should, except in exceptional circumstances, transfer cases where valid, enforceable forum selection clauses exist. However, because this case did not involve a forum selection clause in an employment agreement, it remains to be seen whether lower courts faced with transfer motions in employment disputes will interpret forum selection clauses in the same manner as the *Atlantic Marine* court.
- During 2013, courts in Massachusetts, Minnesota, and New York joined the Ninth Circuit's narrow reading of the Computer Fraud and Abuse Act, limiting its applicability to scenarios where the defendant(s) hacked into or otherwise took affirmative steps to circumvent computer security, finding that violating employer computer usage or access policies alone do not violate the CFAA.

Employee Social Networking: Protecting Your Trade Secrets in Social Media

In our second webinar of the series, Scott Schaefers, Justin Beyer and Joshua Salinas addressed the interplay between trade secrets and social media.

- ***Social Media Privacy Laws are on the Rise.*** At least 14 states now have laws prohibiting employers from requiring or even asking for access to employees' or job applicants' personal social media accounts. Penalties for violations range from nominal administrative fines to much larger damages, including punitive damages and attorneys' fees. Many of the laws, however, have broad exceptions and loopholes, including required employer access of "non-personal" accounts and on suspected data theft or workplace misconduct. To learn more, please see our *Social Media Privacy Legislation Desktop Reference*.
- ***Watch Out for Your Trade Secrets.*** The new legislation may throw wrenches into employer-employee trade secret theft cases. For example, a disloyal employee secretly copies a confidential employer customer list onto his personal LinkedIn account. The employee works in a state that has adopted the new privacy legislation, which has an exemption for suspected data theft. The employer hears unsubstantiated gossip about that list copying, but does not investigate based on the flimsy evidence and for fear of violating the privacy law. The employee later resigns, and uses that list for a competitor. Did the former employer waive a trade secrets claim against the employee because it decided not to investigate, even though it could have? Did that decision amount to an unreasonably insufficient effort to protect its trade secrets?

- ***Have a Social Media Policy.*** Employers should have compliant social media usage policies. The policy should describe, among other things, what constitutes a "personal" social media account, what types of information belong to the employer, what types of social media activity is permissible, the instances in which the employer may seek to require or request access, and the potential consequences for non-compliance.

Barbarians at the Gate: Class Action Avoidance and Mitigation for Data Breach

The third installment of the series was presented by Robert Milligan, Bart Lazar and John Tomaszewski as they discussed avoidance and mitigation techniques for data breaches, including where the class action bar is going and what potential defenses and strategies companies can employ in such lawsuits.

- A strong data security program requires layers. You can't rely just on technical safeguards and the IT group. You also need people and processes to help catch the threats which get through the cracks that technology cannot plug. As part of that layering, it isn't just about the prevention of threats, it is also about detection and early warning of threats. This will allow for the isolation of a threat which has made it through the "front door" before it gets into the safe in the bedroom.
- A company gets a greater return on investment by being prepared for a security breach. Training employees on handling personal information engages them in the process, and raises awareness to reduce the risk of an incident or that an incident will go unnoticed. Developing an incident response protocol and team with defined responsibilities allows a company to be more nimble and efficient when a potential incident occurs. And, as the study we referenced demonstrates, companies that already have an incident response plan in place spend 1/3 less on security incidents than those that do not have an incident response protocol.
- Increasingly courts are becoming more receptive to putative class claims alleging unlawful data breach in violation of statute or under the common law. Article III standing and lack of actual damages continue to be key defenses to such claims but courts are more receptive to creative claims based upon statutory language or contract interpretation. Companies should consider using arbitration agreements with class action waivers, as well as early dispositive motions to attempt to manage the risk of these dangerous and expensive suits.

Trade Secret and Non-Compete Legislative Update

The fourth webinar in the series, presented by Katherine Perrelli, Daniel Hart and Dawn Mertineit discussed the significant statutory changes to several jurisdictions' laws regarding trade secrets and restrictive covenants and pending legislation proposed in additional jurisdictions over the past year.

- Employers should employ a holistic approach to the protection of their trade secrets and confidential information, whether or not Massachusetts bans non-compete restrictions altogether or adopts the Uniform Trade Secrets Act. Utilize non-solicit, non-disclosure and invention assignment agreements; implement entrance and exit interview protocols to educate employees on non-disclosure obligations; create a culture of confidentiality with regular training programs, and various levels of security access to confidential business information; regularly evaluate your trade secret protection policies/protocols; and forensically review computer usage of departing employees with access to confidential information.
- As non-compete and trade secrets law continues to evolve, expect a greater trend toward uniformity in trade secrets law and a continued attempt to regulate trade secrets at the federal

level. Review your company's policies and practices on a regular basis to ensure that they are consistent with the latest developments and continue to take proactive, practical measures to ensure that your trade secrets are subject to reasonable methods to maintain their secrecy.

- Even if your company has operations in a state that does not prohibit employers from requiring employees and applicants to provide social media login information or access, your best bet is to avoid asking employees and applicants for this sort of information (unless account access is necessary to investigate workplace misconduct). More and more states are considering laws prohibiting such actions, and it's best to be ahead of the curve.

To learn more, please see our *50 State Desktop Reference: What Employers Need to Know About Non-Compete and Trade Secrets Law*

International Trade Secrets and Non-Compete Law Update

The fifth webinar in the 2014 series, presented by Wan Li, Ming Henderson, Justine Turnbull and Daniel Hart, 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 Europe, Australia, and China compared to the United States. This 90-minute webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these countries and ensure protection of their trade secrets and confidential information, including the effective use of non-compete and non-disclosure agreements.

International

One size does not fit all. Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. Bearing in mind non-compete covenants may be unlawful in certain countries or heavily restricted, employers should carefully tailor agreements to satisfy local legal requirements and appropriately apply local drafting nuances to aid enforceability of any restrictive covenants. In addition, employers should take advantage of other contractual and/or tactical mechanisms as a "belt-and braces" approach, such as, clawbacks and forfeiture of deferred compensation (where permitted), use of garden leave provisions, and strategic use of forum selection and choice-of-law provisions.

Employers should also take practical measures to protect their confidential information and trade secrets, including limiting access to sensitive information, using exit interviews, and (provided that applicable privacy laws are followed) monitoring use of company IT resources and conducting forensic investigations of departing employees' computer devices.

France

Drafting a non-compete clause under French labor law requires specific care as courts are particularly critical of the following: duration, the geographical and activities scope, the conditions in which the employer releases the employee from such obligation, the employee's role, the interests of the company and the financial compensation provided by the clause.

During employment an employee is subject to a general obligation of confidentiality and breach may be subject to civil and criminal sanctions. Only "trade secrets", however, are protected post-termination under certain circumstances. Employers should therefore enter into a confidentiality agreement to strengthen the protection of the company's data post-termination. Unlike non-compete covenants, a confidentiality clause does not require any financial compensation and can be unlimited in time and scope, if justified by the nature of the confidential information to protect.

United Kingdom

Restrictive covenants are potentially void as an unlawful restraint of trade and are therefore only enforceable if they go no further than is necessary to protect legitimate business interests. In practical terms, this means that such covenants are only likely to be enforceable where they are fairly short in duration, the restriction is narrowly focused on the employee's own personal activities (e.g. geographical scope) and is specific to the commercial environment. Careful drafting is key especially given the unforgiving nature of the English Courts when it comes to poor drafting even if the intention of the parties is obvious, an unclear clause could be struck out, rather than redacted. Employers should also consider other creative and acceptable ways to aid enforceability, such as, deferring remuneration and varying and reaffirming covenants.

Absent any agreement, only "trade secrets" will be protected after employment. Employers should therefore ensure that employment contracts and/or other free-standing binding agreements provide full coverage for the protection of confidential and other valuable business information post-termination. In addition, employers should also physically protect their confidential information (e.g. encrypting data, installing passwords, secure storage, etc.) and seek to retain control of it to reduce and limit unwanted disclosure and misuse. Physical security can be a more effective and less costly approach in the long-term.

Australia

It is possible to protect an organization's confidential information, customer or client connections, trade secrets and other proprietary interests from inappropriate use by former employees in Australia. To do this detailed consideration is required of the employee's role and responsibilities and we as their personal situation. Further, protection must not only be included in the written terms of employment but also employed at a very practical level in the business, for example, by password protecting documents, limiting access to confidential information to those who 'need to know' and by expressly reminding employees in different forms about the importance of certain information and relationships to the business and their related obligations.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

The sixth webinar of the year, led by Scott Humphrey, Jason Stiehl and Rebecca Woods, 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 confidentially 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.

- Use of cloud-based services is increasing, including in the financial services industry. This creates different risks for protecting trade secrets with potential theft, exposure, or loss from cloud providers, hackers, and rogue or sloppy employees. A comprehensive and preventative slate of measures should be considered in order to ensure protection from each of these threats and to manage and mitigate the consequences of a compromise of protected information. "Analog" protections, such as confidentiality agreements, employee training, and basic security safeguards remain relevant. "Cloud" protections should be added, however, and include maximizing technology-based security features, negotiating savvy and strong vendor agreements, and obtaining properly-scaled cyber-insurance coverage. The compromise of proprietary information that includes personal information may trigger federal and/or state breach notification obligations.

Ins and Outs of Prosecuting and Defending Trade Secret Injunction Cases

In the seventh installment, Justin Beyer, Dawn Mertineit, and James Yu discussed practical steps employers can take to protect trade secrets during an employee's employment and after, best practices employers should take upon discovering or suspecting that an employee has misappropriated its data, best practices employers should take in onboarding a competitor's former employee to minimize the likelihood of being sued, and strategic considerations when faced with defending a trade secret misappropriation case.

- Employers can best protect their trade secrets by instituting robust training, policies and procedures aimed at educating its work force as to what constitutes confidential information and that this information belongs to the employer, not the employee. By utilizing confidentiality, invention assignment, and reasonable restrictive covenants, as well as implementing onboarding and off-boarding protocols, educating employees on non-disclosure obligations, educating employees on that data which the employer considers confidential, clearly marking the most sensitive data, and restricting access to confidential information, both systemically and through hardware and software blocks, employers can both educate and prevent misappropriation.
- If an employee voluntarily resigns his or her employment with the company, the employer should already have in place a specific protocol to ensure that the employee does not misappropriate company trade secrets. Such steps include questioning the employee on where he intends to go, evaluating whether to shut off access to emails and company systems prior to the expiration of the notice period, requesting a return of company property, including if the company utilizes a BYOD policy, and reminding the employee of his or her continuing obligations to the company. Likewise, companies should have robust onboarding policies in place to help avoid suit, such as attorney review of restrictive covenants, offer letters that specifically disclaim any desire to receive confidential information from competitors, and monitoring of the employee after hire to ensure that they are not breaching any confidentiality or non-solicitation obligations to the former employer.
- If a company finds itself embroiled in litigation based on either theft of its trade secrets or allegations that it either stole or received stolen trade secrets, it is important to take swift action, including interviewing the players, preserving the evidence, and utilizing forensic resources to ascertain the actual theft or infection (if you are on the defense side). Companies defending against trade secret litigation also need to analyze and consider whether an agreed injunction is in its best interests, while it investigates the allegations. These types of cases tend to be fast and furious and the internal business must be made aware of the impact this could have on its customer base and internal resources.

Trading Secrets

Protecting Trade Secrets: The Current Landscape, Top Threats, Best Practices for Assessing and Protecting Trade Secrets, Proposed Legislation and Future Scenarios

In our eighth installment, Robert B. Milligan, Daniel Hart, along with the CREATe.org's CEO Pamela Passman and Marissa Michel, the Director in PricewaterhouseCoopers' Forensic Services Group, took a rigorous look at the issue or trade secret theft and discussed insights from a recent PwC – CREATe.org report: *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate potential threats*.

- Theft of trade secrets poses a substantial threat to companies throughout the world and will likely remain a significant challenge in the next 10-15 years as companies face increasing threats from competitors, malicious insiders, nation states, transnational organized crime, and hacktivists.
- Companies should carefully assess their existing trade secrets portfolio and the steps needed to protect their trade secrets by following a detailed and comprehensive 5-step framework: (1) identifying their trade secrets, (2) assessing the threats to their trade secrets portfolio and possible exposures, (3) analyzing the relative priorities of their trade secrets to assess which trade secrets require the highest level of protection, (4) assessing the likely economic impact that would be caused by a theft of trade secrets, and (5) secure the trade secrets portfolio by implementing a management system (including policies, protocols, training, and other measures across the organization).
- Effective protection of trade secrets requires a coordinated and deliberative effort across all business units in a company, including IT, HR, legal, and other business leaders. The only way to effectively protect a company's trade secrets portfolio is to carefully analyze the threats to the company's trade secrets and thoughtfully develop a comprehensive and customized strategy with buy-in from all stakeholders across the organization.

How and Why California is Different When it Comes to Trade Secrets and Non-Competes

The ninth webinar this year, presented by Robert Milligan, James McNairy and Joshua Salinas, focused on recent legal developments in California trade secret and non-compete law and how it is similar to and diverse from other jurisdictions, which included: a discussion of the California Uniform Trade Secrets Act, trade secret identification requirements, remedies, and the interplay between trade secret law and Business and Professions Code Section 16600, which codifies California's general prohibition of employee non-compete agreements. The panel discussed how these latest developments impact litigation and deals involving California companies.

- While California has rejected the inevitable disclosure doctrine, threatened misappropriation can be a viable theory for relief when there is evidence of data theft and intent to use company data.
- California's recent appellate decision in *Altavion, Inc. v. Konica Minolta Sys. Laboratory, Inc.*, 226 Cal. App. 4th 26 (2014) has broadened the scope of trade secret protectable information to include ideas.
- Federal district courts in California have increasingly elected to enforce forum selection clauses in non-compete agreements of California employees and found that enforcement of such clauses does not violate California's strong public policy of employee mobility. See, e.g., *Hegwer v. American Hearing and Associates*, 2012 WL 629145 (N.D. Cal., Feb. 27, 2012)

(granting motion to dismiss California action based upon Pennsylvania forum selection law clause – alleged illegality of non-compete irrelevant to enforcement of forum selection clause); *Hartstein v. Rembrandt IP Solutions*, 2012 WL 3075084 (N.D. Cal., July 30, 2012) (court agrees to enforce Pennsylvania forum selection clause, disregarding ultimate affect that Pennsylvania court will enforce improper non-compete clause against California citizen).

- The recent decision in *Cellular Accessories For Less, Inc. v. Trinitas LLC*, No. CV 12–06736 D, DP (SHx), 2014 WL 4627090 (C.D. Cal. Sept. 16, 2014) illustrates that LinkedIn contacts and other social media connections could be protectable as trade secrets if the methods used to compile the contact information are "sophisticated," "difficult," or "particularly time consuming." Nonetheless, the purported trade secret holder will also have to establish that the contacts were not made public.

Protecting Trade Secrets and Intellectual Property in Business Transactions

In the final installment of our 2014 Trade Secrets Webinar Series, Seyfarth attorneys Michael Baniak and Randy Bruchmiller focused on considerations involving protecting trade secrets and intellectual property in business transactions, including, mergers and acquisitions, joint ventures and other collaborative arrangements.

- The protection of intellectual property is critical in joint venture and other agreements in order to protect what, many times, is some of the most important assets of the company. These protections may include protecting the confidentiality of the information and addressing what rights each party will have in the intellectual property after the transaction or venture.
- Companies should protect their trade secrets at every level of the employee hierarchy. Executives and high-level employees usually have employment agreements that address confidentiality and the handling of trade secret information. Mid-level managers and lower level employees are often over-looked. It is important to have all employees enter into confidentiality agreements and, in many cases, intellectual property assignment agreements.
- Regardless of what protections are put in place, it is very important to be aware of law changes in the states where the company has employees and to revise agreements to address any changes in the law.

2015 Trade Secret Webinar Series

Beginning in January 2015, we will begin another series of trade secret webinars. The first webinar of the year will be "2014 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.

Seyfarth Trade Secrets, Computer Fraud & Non-Compete attorneys are happy to discuss presenting similar presentations to your groups for CLE credit.

Michael Wexler is Chair and Robert Milligan is Co-Chair of the Trade Secrets, Computer Fraud & Non-Compete Practice Group. If you have any questions, please contact Michael Wexler at mwexler@seyfarth.com /(312) 460-5559, Robert Milligan at rmilligan@seyfarth.com /(310) 201-1579, the Seyfarth Shaw attorney with whom you work or any Trade Secrets, Computer Fraud & Non-Compete attorney on our website (www.seyfarth.com/tradesecrets).

Trading Secrets

Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2014

By Robert Milligan and Daniel Hart (January 6, 2015)

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 2014. Please join us for our complimentary webinar on January 27, 2015, at 1:00 p.m. e.s.t., where we will discuss them in greater detail. As with all of our other webinars (including the 10 installments in our 2014 Trade Secrets webinar series), this webinar will be recorded and later uploaded to our Trading Secrets blog to view at your convenience.

Here is our listing of top developments/headlines in trade secret, computer fraud, and non-compete law for 2014, as well as our predictions for 2015, in no particular order:

1. Increased Threat to Trade Secrets by Hackers. As demonstrated by the suspected North Korean-linked cyber-attacks, hackers represent a significant and growing threat to the intellectual property of U.S. and multinational companies. ICANN recently reported its own data breach and indicated that the email credentials of some ICANN staff members were compromised. Security company Mandiant published a report finding that the government of the People's Republic of China ("PRC") is sponsoring cyber-espionage to attack top U.S. companies. Moreover, CREATe.org released a whitepaper that highlighted how far-reaching and deeply challenging trade secret theft is for companies operating on a global scale and identified "hacktivists," some foreign governments, and organized crime (as well as competitors and rogue employees) as major threats to trade secrets. While much of the attention on foreign threats to trade secrets has focused on the PRC, recent decisions from courts in Shanghai suggest that some courts in the PRC may be adopting an enforcement approach in trade secrets and non-compete cases that is closer to the approach of U.S. courts. Notwithstanding this potentially significant development in the PRC, hackers, especially those tied to foreign governments, will likely continue to pose a major threat to U.S. and multinational companies in the near future. Please see our recent webinar on addressing data security breaches.

2. More High-Profile Prosecutions under the Computer Fraud and Abuse Act and Economic Espionage Act. In response to the growing threat to the trade secrets of U.S. companies, the Obama Administration released a 150-page report that unveiled a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies. Consistent with this strategy, in 2014 the U.S. Department of Justice continued to pursue high-profile prosecutions under the CFAA and Economic Espionage Act, particularly against defendants tied to the Chinese government. As we previously reported, earlier this year the DOJ obtained the first-ever federal jury conviction under the Economic Espionage Act in the *U.S. v. Liew* case. Following the jury's conviction of two individuals and one company in that case, a federal court sentenced defendant Walter Liew to 15 years in prison for theft of trade secrets from chemical giant DuPont and selling them to an overseas company controlled by the government of the PRC. In another high-profile criminal case, a federal grand jury indicted five high-ranking officials of the PRC's People's Liberation Army for computer hacking, economic espionage and other offenses directed at American companies in the nuclear power, metals

and solar products industries. More high-profile prosecutions will likely continue in the next year as the federal government further cracks down on trade secret theft.

3. Continued Attempt to Create Civil Cause of Action for Trade Secrets Theft in Federal Court. As we previously reported, the past several years have seen increased attempts to create a civil cause of action for trade secrets misappropriation at the federal level. 2014 was no exception. Earlier this year, Sens. Christopher Coons (D-Del.) and Orrin Hatch (R-Utah) introduced the Defend Trade Secrets Act of 2014 in the U.S. Senate. The bill amends the Economic Espionage Act to provide a civil cause of action to private litigants for violations of 18 U.S.C. § 1831(a) and 1832(a) of the EEA and for "misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce." The bill also would allow a plaintiff to obtain a seizure order, though some have questioned whether this remedy may be subject to abuse and have concerns about implementation. A few months later, a bi-partisan group led by Reps. George Holding (R-N.C.) and Jerrold Nadler (D-N.Y.) introduced a similar bill in the House of Representatives, the Trade Secrets Protection Act of 2014. The House bill largely tracks the Senate bill but refines the seizure provisions and contains other notable refinements that we discussed here. The House Judiciary Committee has reported favorably on the bill and recommended its passage. Although the House did not pass the bill before adjourning, expect to see the same or similar legislation introduced early next year. With the recent high profile hacking incidents, we believe that there is momentum for the passage of a bill this year.

4. Attempt to Harmonize Trade Secrets Protection in EU. Across the pond, European lawmakers are considering a similar proposal to harmonize trade secrets protection throughout the EU's 28 members states. As we discussed here, currently there is no uniform protection of trade secrets across the EU. Instead, a patchwork of uneven levels of protection and remedies exist among EU Member States. After a study prepared for the European Commission identified substantial perceived weaknesses in the trade secrets protections afforded by the laws of many Member States, the European Commission announced a proposal for a Directive on trade secrets that, if enacted, will substantially alter the legal landscape in Europe regarding trade secret protection and will enhance cross-border certainty within the EU. The draft directive is currently being reviewed by the EU Parliament's Legal Affairs, Internal Market, and Industry Committees and their decisions have not been released yet. While the European Parliament has not yet voted on the proposal, it is expected that the matter will be scheduled for a first reading in the Parliament during the first half of 2015.

5. Massachusetts Fails to Enact Proposed Non-Compete / Trade Secrets Legislation. In what has become an annual tradition over the past several years, lawmakers in Massachusetts once again debated, but failed to pass, legislation that would overhaul the Bay State's existing law on non-competes and trade secrets, which are currently governed by state common law. Along with New York, Massachusetts is one of only two states that has not yet adopted a version of the Uniform Trade Secrets Act ("UTSA"). This past legislative session, the Massachusetts legislature considered a proposed bill that would have adopted the UTSA and that (more controversially) would have virtually eliminated employee non-compete agreements in Massachusetts. Although the state Senate overwhelmingly approved a compromise bill that, if enacted, would have imposed certain notice requirements and established presumptions of reasonableness for employee non-competes (among other provisions), ultimately the legislature did not pass either the compromise bill or any of the various alternative non-compete or trade secrets bills proposed this year. But if recent history is any guide, expect to see attempts to overhaul Massachusetts non-compete law once again introduced in 2015. In fact, after this year's legislative session ended, outgoing Governor Duval Patrick introduced another compromise bill that legislators may debate when the new legislative session begins in January.

6. Courts Continue to Grapple with UTSA's Preemptive Impact. Among the 48 states that have adopted some version of the UTSA, courts continue to grapple with the impact of the UTSA on common law remedies for misappropriation of confidential information (such as claims for unfair competition, conversion, tortious interference, or unjust enrichment). The UTSA contains a provision stating that the Act "displaces conflicting tort, restitutionary, and other laws of this State providing civil remedies for misappropriation of a trade secret" but "does not affect (1) contractual remedies, whether or not based on misappropriation of a trade secret; (2) other civil remedies that are not based on misappropriation of a trade secret; or (3) criminal remedies, whether or not based on misappropriation of a trade secret." As we discussed here, courts in several states have held that the UTSA should be read broadly to preempt all claims related to the misappropriation of information, regardless of whether or not the information falls within the definition of a trade secret. In contrast, courts in other states have concluded that the UTSA preempts only claims for misappropriation of "trade secrets," as defined by the UTSA, and leaves available all other remedies for the protection of confidential information that is not a trade secret. With its recent decision in *Orca Communications Unlimited, LLC v. Noder*, 337 P.3d 545 (Az. 2014), the Arizona Supreme Court joined this latter group and held as a matter of first impression that the AUTSA does not displace common law remedies for misappropriation of confidential information that does not qualify as a trade secret. Expect to see states continue to line up on either side of this divide.

7. Continued Significance of Choice of Law and Forum Selection Provisions In Non-Compete Disputes. Following the U.S. Supreme Court's decision in *Atlantic Marine v. U.S.D.C. for the W.D. of Texas*, choice of law and forum selection clauses are increasingly significant in non-compete litigation. In *Atlantic Marine*, the Supreme Court 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, the decision appears to strengthen the enforceability of forum selection clauses generally. For example, in *AAMCO Transmissions, Inc. v. Romano*, — F. Supp. 2d –, 2014 WL 4105986 (E.D. Pa. Aug. 21, 2014), a federal district court in Pennsylvania enforced a forum-selection clause in a non-compete agreement against both a franchisee who signed the agreement and the franchisee's wife who, though not a signatory the agreement, was also deemed to be bound by the forum selection clause because of her close connection to the signatory. In addition, as we reported here, federal district courts in California are increasingly enforcing forum selection clauses in non-compete agreements of California employees and finding that enforcement of such clauses does not violate California's strong public policy of employee mobility. In light of *Atlantic Marine*, expect companies to make greater use of choice of law and forum selection clauses (and the resulting "race to the courthouse") in suits to enforce their restrictive covenants.

8. Social Media Continues to Generate Disputes. Continuing a trend that we discussed last year, social media continues to generate disputes in trade secret, computer fraud, and non-compete law, as well as in privacy law. Wisconsin, Louisiana, Oklahoma, New Hampshire, and Rhode Island joined several other states in enacting legislation to protect "personal" use of social media by employees. Expect other states to get on the social media bandwagon in the next year. The ownership of content stored in LinkedIn and other social medial accounts is also a continuing source of disputes. Like courts in the UK and elsewhere, US courts continue to grapple with whether there can be trade secret protection for such information. For example, a few months ago, a federal district court in California issued a well-publicized decision in *Cellular Accessories For Less, Inc. v. Trinitas LLC*, No. CV 12–06736 D, 2014 WL 4627090 (C.D. Cal. Sept. 16, 2014), in which it denied a motion for summary judgment on a trade secrets misappropriation claim against a former employee who retained the contacts in a LinkedIn account that he created while employed by the plaintiff. That case illustrates that LinkedIn and other social media contacts can be protectable as trade secrets if the methods used to compile the contact information are "sophisticated," "difficult," or "particularly time consuming,"

though the purported trade secret holder will also have to establish that the contacts were not made public in order to be entitled to trade secret protection. Although the *Cellular Accessories* court did not rely on decisions from other jurisdictions, the court's decision is consistent with a handful of recent decisions in which English courts have suggested that an employee's competitive use of LinkedIn contacts that the employee developed during his or her employment might, in some circumstances, constitute a breach of the duty of good faith. (*See, e.g., Whitmar Publications Limited v Gamage* [2013] EWHC 1881 (Ch.) and *Hays Specialist Recruitment (Holdings) v. Ions* [2008] EWHC 745 (Ch.).) As use of social media continues to proliferate, more courts are likely to weigh-in on this issue.

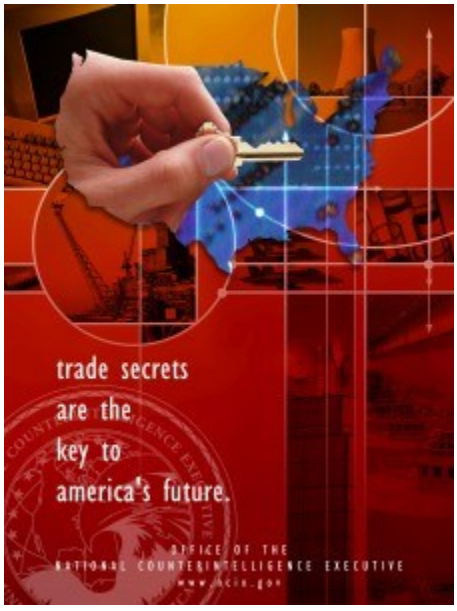
9. NLRB Challenges Employer Policies on Employee Use of Social Media and IT Resources. Speaking of social media, the National Labor Relations Board ("NLRB") issued significant decisions this year that have left many employers scrambling to revise their policies on employee use of social media and IT resources. As we reported here, in *Triple Play Sports Bar & Grille*, 361 NLRB No. 31 (2014) , the NLRB ruled that a Facebook discussion regarding an employer's tax withholding calculations and an employee's "like" of the discussion constituted concerted activities protected by Section 7 of the National Labor Relations Act ("NLRA"), which protects employees' rights to engage in concerted activities regarding the terms and conditions of their employment. The Board also held that the employer's internet and blogging policy (which provided that "engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment") was overly broad and, therefore, violated the NLRA. Additionally, as we reported here, the NLRB recently ruled that employees who have access to an employer's email system as part of their job generally may, during non-working time, use the email system to communicate about wages, hours, working conditions and union issues. The NLRB's ruling (*Purple Communications*, 361 NLRB No. 126 (2014)) poses a major headache for employers who seek to control use of their IT assets. As the new Republican-led Congress seeks to reign-in the NLRB, expect these rulings to be hotly debated in the coming year.

10. Courts, Lawmakers, and Regulators Continue to Scrutinize Non-Competes and Consideration Remains a Hot Button Issue. Finally, as in past years, many employers are once again reviewing and tweaking their non-competes and onboarding procedures in light of continued scrutiny of non-competes by courts, legislatures, and regulators. On the enforcement side, the Texas Supreme Court found that the enforcement of a forfeiture provision for competitive activity in an employee incentive compensation plan was not contrary to Texas public policy. Courts have, however, continued to issue significant decisions invalidating some non-competes. For example, in *Dawson v. Ameritox, Ltd.,* 571 Fed. App'x. 875 (11th Cir. 2014), the Eleventh Circuit affirmed an Alabama federal court's ruling that a non-compete executed prior to employment was unenforceable. In *Nott Co. v. Eberhardt*, Nos. A13–1061, A13–1390, 2014 WL 2441118 (Minn. Ct. App. June 2, 2014), the Minnesota Court of Appeals held that a non-compete was unenforceable against an employee who signed the non-compete and received benefits purportedly as consideration for the agreement because another employee did not sign a non-compete but nevertheless received the same benefits. Following an Illinois Court of Appeals' decision in *Fifield v. Premier Dealer Servs., Inc.*, 993 N.E.2d 938 (Ill. App. Ct. 2013), courts in Illinois are continuing to consider whether less than two years employment is adequate consideration to enforce a non-compete against an at-will employee where no other consideration is given for the non-compete. Courts in Pennsylvania and Wisconsin are also grappling with what constitutes sufficient consideration for the enforcement of non-competes. We also expect that government agencies and employees will continue to mount challenges to the use and enforcement of some non-compete and other restrictive covenants (including "no poaching" provisions) with certain employees and industries this year. In light of these decisions and other continuing developments in non-compete law, employers should periodically review their existing agreements and on-boarding procedures to maximize the likelihood that their agreements will be upheld.

Trade Secrets Litigation

Latest Updates on Federal Trade Secrets Legislation

By Robert Milligan and Joshua Salinas (September 8, 2014)



With increased activity regarding proposed federal trade secrets legislation expected this month and for the remainder of the fall Congressional session, Seyfarth Shaw's dedicated Trade Secrets group has created a resource which summarizes the proposed legislation, outlines the arguments in favor of and against the legislation, and provides additional legislation resources for our readers' convenience. This page will be continuously updated as we monitor and keep you apprised of the most recent developments, debate, and news regarding the legislation.

Below we provide an overview of trade secret law and the proposed legislation, the arguments on both sides of the debate, and our most current resource links.

How Are Trade Secrets Currently Protected?

Trade secrets consist of information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, it must be used in business, and give an opportunity to obtain an economic advantage over competitors who do not know or use it. Trade secrets are generally protected by statute under the Uniform Trade Secrets Act (UTSA). The UTSA, published by the Uniform Law Commission (ULC) in 1979 and amended in 1985, was an act promulgated in an effort to provide a unified legal framework to protect trade secrets.

Texas recently became the 48th state to enact some version of the UTSA. New York and Massachusetts are the remaining states not to have enacted the UTSA. Trade secrets are protected in those jurisdictions under the common law.

Trade secrets are also protected under federal criminal laws, i.e. the Economic Espionage Act of 1996, as well as state criminal laws.

Unlike patent, trademark, or copyright protection, there is no set time period for trade secret protection. A trade secret is protected as long as it is kept secret. However, once a trade secret is lost, it is lost forever. As we have seen in a post-Wikileaks world, once confidential information is disclosed, it can be instantly distributed online for hundreds of millions to see, access, and download, and thereby lose its trade secret status.

What Is the Proposed Legislation?

The proposed legislation would authorize a private civil action in federal court for the misappropriation of trade secrets when certain circumstances are present and certain specified requirements are met. Two bills have been recently introduced into Congressional committee:

A. Senate Bill: Defend Trade Secrets Act

On April 29, 2014, Sens. Christopher Coons (D-Del.) and Orrin Hatch (R-Utah) introduced the Defend Trade Secrets Act of 2014. The bill amends the Economic Espionage Act to provide a civil cause of action to private litigants for violations of 18 U.S.C. § 1831(a) and 1832(a) of the EEA and for "misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce." According to the Senate sponsors, the bill will provide uniform trade secrets protection and federal remedies across the United States.

The bill marked the latest attempt in the past four years to create a private civil cause of action for trade secret misappropriation at the federal level. The following bills previously failed: Amendment to Currency Exchange Rate Oversight Reform Act of 2011, Protecting Trade Secrets and Innovation Act of 2012 ("PATSIA"), and the Private Right of Action Against Theft of Trade Secrets Act of 2013 ("PRATSA").

The bill uses the statutory language for "improper means" and "misappropriation" from the UTSA. The bill also provides for a five year statute of limitations and provides uniform remedies for misappropriation of trade secrets. It provides for injunctive relief to prevent any actual or threatened misappropriation of trade secrets. It also allows for affirmative actions to be taken to protect trade secrets, such as protective orders. With respect to damages, it provides damages for actual loss, unjust enrichment, and a reasonable royalty in certain scenarios. Additionally, in exceptional circumstances, royalties can be awarded for the use of trade secrets in lieu of a permanent injunction. In cases of willful or malicious misappropriation, the bill provides for exemplary damages of not more than three times the actual damages. It also provides for attorneys fees' and costs for willful and malicious misappropriation or for the pursuit of a trade secret cause of action in bad faith.

It also provides for *ex parte* orders for preservation of evidence and seizure of any property used, in any manner or part, to commit or facilitate a violation of the statute, using the procedure contained in the Lanham Act.

Lastly, the bill provides that nothing in the statute "shall be construed . . . to preempt any other provisions of law." Accordingly, the intent of the bill is not to preempt state UTSA claims.

B. House Bill: Trade Secrets Protection Act

On July 29, 2014, a similar bill, entitled the Trade Secrets Protection Act of 2014, was introduced into the House, by a bi-partisan group led by George Holding (R-N.C) and Jerrold Nadler (D-NY).

"American businesses face relentless cybersecurity threats every day, costing our economy billions of dollars and tens of thousands of jobs each year," said Rep. George Holding in his press release in support of the bill.

"As a way to help create jobs, grow our economy and protect our businesses, I have introduced the Trade Secrets Protection Act of 2014. This bill will help supply American businesses, both large and small, with the tools needed to combat these destructive threats," he added.

"American businesses are global leaders in innovation and job creation, yet they are faced with increasing threats to valuable information. The current patchwork within state and federal statutes is not enough to keep pace with organized trade secret theft, resulting in a loss of nearly $100 billion which could mean 200,000 jobs, a recent report stated," he remarked.

"By helping American businesses defend against these threats, we are not only protecting American interests, but helping recover the millions of dollars and thousands of jobs lost each year," Holding concluded.

The bill was originally co-sponsored by Holding, Howard Coble, R-N.C., Hakeem Jeffries, D-N.Y., Steve Chabot, R-Ohio and John Conyers, D-Mich. Additional House members have subsequently joined these members in co-sponsoring the bill.

What Are The Differences Between The Two Bills?

The House bill largely tracks the Senate's Defend Trade Secrets Act but has three notable and significant modifications:

1. It only permits a civil claim for "misappropriation of a trade secrets that is related to a product or service use in, or intended for use in, interstate or foreign commerce." It does not permit a claim for a violation of 18 U.S.C. § 1831(a) and 1832(a).

2. It permits a seizure order on an *ex parte* basis to preserve evidence or to prevent the propagation or dissemination of the trade secret that is the subject of the action but it has certain precautions and limitations not found in the Senate bill.

3. It clarifies that it only covers misappropriation actions that occur on or after it is enacted.

With respect to the seizure order language, in order to obtain an *ex parte* order, the plaintiff must show, that (1) a temporary restraining order under Federal Rule of Civil Procedure 65(b) would be inadequate because the defendant would evade, avoid, or otherwise not comply with such order; (2) an immediate and irreparable injury will occur if seizure is not ordered; (3) the harm to the plaintiff of denying the order outweighs the legitimate interests of defendant and substantially outweighs any harm to third parties; (4) the plaintiff is likely to succeed against the defendant in showing that the defendant misappropriated the trade secret and is in possession of the trade secret; (5) the plaintiff described with particularity the matter to be seized and the location where the matter is to be seized; (6) the defendant would destroy or make the property inaccessible to the court if the applicant were to proceed on notice; and (7) the plaintiff has not publicized the request.

Additionally, the court's order must (1) minimize any interruption of the business operations of third parties and the defendant that is unrelated to the trade secret that has allegedly been misappropriated; (2) protect the property from disclosure to plaintiff; (3) set a hearing date no later than seven days after the order is issued; and (4) require a security adequate to cover damages from a wrongful or excessive seizure. The court is required to take appropriate action to protect the defendant from publicity. The court is also required to take custody of the material ordered seized. Lastly, any person who suffers damage by reason of a wrongful or excessive seizure has a cause of action against the plaintiff.

Accordingly, the House bill provides even more restrictions and safeguards on the ability to obtain an *ex parte* seizure order. In sum, the most significant difference between the bills is the clarification and refinement of the seizure order and the exclusion of section 1831 and 1832 civil claims.

Do We Need Federal Trade Secrets Legislation?

Many business, professional, political, and academic leaders have called for the creation of federal civil cause of action for trade secret misappropriation. There has been some vocal opposition to the legislation.

Trading Secrets

Recent scholarly articles in the Gonzaga Law Review and Fordham Law Review indicate that federal courts may be more equipped to devote resources to trade secret claims so as to establish a uniform body of case law, like other intellectual property. *See A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 Gonzaga Law Review 57 (February 2011); *Four Reasons to Enact a Federal Trade Secrets Act*, 19 Fordham Intellectual Property, Media & Entertainment Law Journal 769 (April 2009).

Additionally, published reports indicate that there is a growing rise in trade secret theft from foreign hackers and rogue employees interested in obtaining U.S. businesses' trade secrets. Foreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security. In response, the Obama Administration released a 150-page report that unveiled a government-wide strategy designed to reduce trade secret theft by hackers, employees, and companies. In its published strategy plan, the Obama Administration recognized the accelerating pace of economic espionage and trade secret theft against U.S. corporations and suggested looking into creating additional legislative protections.

Additionally, security company Mandiant published a report finding that the Chinese government is sponsoring cyber-espionage to attack top U.S. companies. Moreover, CREATe.org released a whitepaper that highlighted how far-reaching and deeply challenging trade secret theft is for companies operating on a global scale. Further, a report commissioned by IT security company Symantec revealed that half of the survey respondents, employees from various countries, including the United States, revealed that they have taken their former employer's trade secret information, and 40 percent say they will use it in their new jobs. Lastly, estimates of trade secret theft range from one to three percent of the Gross Domestic Product of the United States and other advanced industrial economies, according to a new report by PwC US and CREATe.org.

Indeed, the recent expansion of penalties and expanded definition of trade secrets under the EEA reflects a recognition by the government that the EEA is a valuable tool to protect secret, valuable commercial information from theft and that Congress can work in a bi-partisan effort to address such theft.

The significant harm caused by economic espionage for the benefit of foreign actors is illustrated by a recent case where a project engineer for the Ford Motor Company copied 4,000 Ford Motor Company documents onto an external hard drive and delivered them to a Ford competitor in China. The documents contained trade secret design specifications for engines and electric power supply systems estimated to be worth between $50 million and $100 million. Similarly, a former employee of a North American automotive company and the employee's spouse were found guilty of stealing trade secrets related to hybrid vehicle technology worth $40 million. The couple intended to sell the information to a Chinese competitor.

There is also significant harm caused by economic espionage committed by insiders. An employee of a large U.S. futures exchange company pleaded guilty to stealing more than 10,000 files containing source code for a proprietary electronic trading platform. Prosecutors estimated the value of these trade secrets between $50 and $100 million. The employee said he and two business partners had planned to use this source code to develop their own company.

The United States currently has an un-harmonized patchwork of trade secret protection laws that are ill-equipped to provide an effective civil remedy for companies whose trade secrets are stolen. Not all states have adopted the Uniform Trade Secrets Act, and many differ in the interpretation and implementation of certain trade secret laws. For instance, states have differences in their definition of a trade secret (e.g. Idaho expressly includes computer programs) and what is required to maintain a claim for trade secret misappropriation. Some states have found a novelty requirement for information to be considered a trade secret and some are more protective of customer lists. There are also several

states that have different statute of limitations for trade secret claims and there are also significant differences on the availability of a royalty injunction. Many states also did not pass Section 8 of the UTSA which provides, "[t]his [Act] shall be applied and construed to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among states enacting it." Moreover, victims of trade secret theft can face lengthy and costly procedural obstacles in obtaining evidence when the misappropriators flee to other states or countries or transfer the evidence to other states or countries.

Proponents and Sponsors of the Bills

The two pending trade secret bills have bi-partisan support in both houses by high ranking legislators. Additionally, the Heritage Foundation recently wrote an article in support of a private right of action. Congresswoman Zoe Lofgren, D-Cal., previously proposed creating a civil cause of action in federal court last year with the PRATSA bill. Also, a diverse set of companies and organizations have come out in favor of legislation or the concept of a federal civil cause of action, including Adobe, Boeing, Microsoft, IBM, Honda, DuPont, Eli Lilly, Broadcom, Caterpillar, NIKE, Qualcomm, General Electric, Michelin, 3M, United Technologies Corporation, AIPLA, IPO, National Association of Manufacturers, and the National Chamber of Commerce.

As indicated NAM supports the bill, noting that it marked "a critical step toward ensuring manufacturers can effectively and efficiently enforce their trade secrets at home and abroad." "[Trade secret] theft costs businesses in this country some $250 billion a year," the group said. "The Trade Secrets Protection Act would help to address this challenge by providing access to federal civil enforcement for trade secrets theft. Right now, businesses must go state by state to defend their rights."

Proponents of the bills have cited the advantages of a federal cause of action, as among other things, a unified and harmonized body of law that addresses discrepancies under the existing law and provides companies a uniform standard for protecting its proprietary information. Federal legislation will treat trade secrets on the same level as other IP and establish them as a national priority, address national security concerns, and create a demonstrative effect on major foreign jurisdictions. The bill may also provide a complimentary measure to combat trade secret misappropriation by private industry in light of strained government resources. A federal cause action may also provide service of process advantages, the ease of conducting nationwide discovery, and additional remedies to aid victims, such as seizure.

Additionally, the former head of the Patent Office, David Kappos recently came out in favor of the bill on behalf of the Partnership of American Innovation stating, "Trade secrets are an increasingly important form of intellectual property, yet they are the only form of IP rights for which the protection of a federal private right of action is not available. The Trade Secrets Protection Act will address this void, and the PAI supports its swift enactment."

Erik Telford of the Franklin Center for Government and Public Integrity added, "[t]he weakness of these laws is that there is no overarching legal framework at the federal level to account for both the sophistication and international nature of new threats. As Mr. Kappos noted, even the government is bound by finite resources in its efforts to protect companies, evidenced by the fact that under the Economic Espionage Act, the Department of Justice initiated only 25 cases of trade secret theft last year."

Opposition To The Bills

A group of 31 professors from throughout the United States who teach and write about intellectual property law, trade secret law, invocation and/or information have submitted an Opposition Letter to the

two bills. The professors cite five primary reasons for their opposition: (1) effective and uniform state law already exists; (2) the proposed Acts will damage trade secret law and jurisprudence by weakening uniformity while simultaneously creating parallel, redundant, and/or damaging law; (3) the Acts are imbalanced and could be used for anti-competitive purposes; (4) the Acts increase the risk of accidental disclosure of trade secrets; and (5) the Acts have potential ancillary negative impacts on access to information, collaboration among businesses, and mobility of labor. A forthcoming article by Washington and Lee University School of Law professor Christopher Seaman critiques the federalization of trade secrets law. See also Mr. Seaman's related guest post at the Patently-O blog.

Current Status Of Proposed Legislation

Both bills have been introduced into their corresponding judiciary committee.

The Senate Judiciary Committee held a closed-door briefing on September 4, 2014 to review the proposed legislation.

The bill was reported favorably to the full House after a House Judiciary Committee markup hearing on September 17, 2014.

Additional News and Resources

Our Recent Blog Articles:

Push for Federal Trade Secret Legislation Gaining Momentum — Aug. 13, 2014

Webinar Recap! Trade Secret and Non-Compete Legislative Update — June 23, 2014

Big Changes May Be Ahead for the Nation's Trade Secret Laws — May 13, 2014

U.S. Senators Propose Legislation To Strengthen Federal Criminal Trade Secret Laws— Aug. 13, 2013

Representative Zoe Lofgren Introduces Bill to Create Private Civil Claim for Trade Secrets Theft Under the Economic Espionage Act — June 26, 2013

Obama Administration's Request for Public Comment on Trade Secrets Law Underscores Importance for Companies to Protect Their Proprietary Assets Now — April 16, 2013

New Federal Trade Secrets Legislation Proposed — July 19, 2012

Other Recent News and Informative Articles:

House Panel OKs Trade Secret Bill, Disputed Seizure Rules — *Law360*, Sept. 17, 2014

Congress Is Considering A New Federal Trade Secret Law. Why? — *Forbes*, Sept. 17, 2014

Profs Ask Congress to Reject Trade Secret Lawsuit Bills — *Corporate Counsel*, Sept. 12, 2014

U.S. Trade Secrets Law, Intellectual Property — *Bloomberg*, Sept. 9, 2014

Trading Secrets

Trade secrets: even more exposed! — *IP Kat*, Sept. 8, 2014

Protecting Trade Secrets to Stimulate Knowledge Flows — *Ideas Lab*, Sept. 4, 2014

US trade secret law: Time for an upgrade — *Tech Policy Daily*, Sept. 3, 2014

Ready to Nationalize Trade Secret Law? — *Patently-O*, Aug. 27, 2014

Law Professors Oppose Federal Trade Secrets Acts, Ignore Their Benefits — *Protecting Trade Secrets*, Aug. 26, 2014

Why Protecting Our Trade Secrets Is Essential To Saving the Economy — *Business Insider*, Aug. 18, 2014

Congressman Holding Introduces Bipartisan "Trade Secrets Protection Act of 2014" — Press Release, July 29, 2014

BSA Applauds Introduction of Trade Secrets Legislation in the House — *The Software Alliance*, July 28, 2014

Proposed U.S. and EU trade secret laws could create more tools to protect your valuable information — *InsideCounsel*, July 22, 2014

Business leaders endorse Senator Coons' bipartisan bill to strengthen protection of trade secrets — Press Release, May 14, 2014

Senator Coons' bipartisan intellectual property legislation to be focus of Tuesday hearing — Press Release, May 12, 2014

Request for Public Comments on "Trade Secret Theft Strategy Legislative Review" — IP Enforcement Coordinator Hon. Victoria Espinel, April 22, 2013

Create.org and PwC: Economic Impact of Trade Secret Theft

Chamber of Commerce: The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement

Trade Secrets

Texas Appellate Court Affirms Multi-Million Dollar Jury Verdict For Trade Secret Misappropriation in Gas Drilling Dispute

By Paul Freehling (January 10, 2014)

Under Texas law, disclosure of a trade secret to potential investors to enable them to decide whether to invest *does not* destroy secrecy. Those who learn of the confidential information under those circumstances are not authorized to destroy its protection and may not use the information in a manner harmful to the interests of the one making the disclosure.

Summary of the Case

An oil and gas developer owned a working interest in and non-exclusive drilling rights for a natural gas reservoir. The developer had an alleged trade secret, a seismic map of the area. Lamont, a co-owner, director and officer of the developer, learned of the map as he was negotiating — in conjunction with his resignation from the company — acquisition of a portion of the developer's working interest. He allegedly never was asked to sign a confidentiality agreement. The developer allegedly disclosed the map to other potential investors as well. After he resigned, Lamont and his investment partner allegedly used the map and secretly obtained the drilling rights that the developer did not own. Lamont and his partner then allegedly removed all of the gas from the reservoir. They were sued for trade secret misappropriation and other torts. As part of their defense, Lamont and his partner asserted that the map's secrecy was forfeited by disclosure of it to Lamont and other potential investors. The Texas Appellate Court recently rejected that defense and affirmed a trial court's entry of judgment for the plaintiffs based on a $4.9 million jury award. *Lamont v. Vaquillas Energy Lopeno Ltd.*, No. 04-12-00219-CV (Dec. 11, 2013).

Formation of Ricochet

Hamblin and Lamont formed Ricochet, a Texas oil and gas development company. Each owned 50% of the company. They were its only directors and its two most senior officers.

The Alleged Trade Secret

Vaquillas Energy and JOB Energy entered into a Prospect Generation Agreement with Ricochet. Pursuant to that agreement, they paid monthly fees in exchange for which they were given confidential information concerning promising projects and were given a right of first refusal to explore and develop prospects.

Ricochet had a working interest in the promising Lopeno natural gas prospect. A key to developing Lopeno was the acquisition of drilling rights on one or both of the primary surface properties over the gas reservoir. Ricochet acquired drilling rights with respect to one of the two properties. In her capacity as a director and officer of the company, Hamblin had a copy of a seismic map relating to Lopeno. The

map allegedly was a trade secret belonging to Ricochet. She showed the map to potential investors including Vaquillas and JOB who agreed to buy a portion of Ricochet's working interest.

Lamont's resignation from Ricochet and alleged misappropriation. In conjunction with negotiations regarding Lamont's separation from Ricochet, Hamblin gave Lamont a copy of the seismic map and offered him a portion of the company's working interest in the Lopeno prospect. Lamont accepted the offer, withdrew from Ricochet, and then showed the map to an experienced oil and gas investor who proceeded to buy 10% of Lamont's working interest. Lamont and his investment partner secretly formed a new company which outbid Ricochet for drilling rights on the contiguous property Ricochet did not own. The new company immediately began drilling and depleted the reservoir, thereby preventing Vaquillas and JOB from withdrawing gas there.

The Lawsuit

Vaquillas and JOB sued Lamont and his partner in a Texas state court, alleging that the seismic map was a trade secret which the defendants misappropriated (the plaintiffs also alleged tortious interference with prospective economic advantage). A jury trial resulted in a verdict for Vaquillas and JOB and the multi-million dollar award for lost profits. Lamont and his partner appealed. They argued that even if the map qualified as a trade secret, it ceased to be one because the developer showed it to Lamont and other prospective investors, and Lamont had a right to disclose it to his investment partner. The appellate court rejected those arguments and affirmed.

The Appellate Court's Reasons for Affirming

1. According to the appellate court, Texas law holds that "[t]rade secret status is not destroyed simply by showing the protected item to buyers, customers, and licensees," and so "Ricochet's limited disclosure to Lamont and other potential investors did not destroy the secrecy of the" seismic map. Citations omitted.

2. Lamont claimed that he was free to disclose and use the seismic map after he left Ricochet's employ. The court concluded that Lamont was entitled to review the map for purposes of deciding whether to invest in the wells. However, with regard to using the map in order to drill in competition with Ricochet, "It was not unreasonable for the jury to determine [that the defendants] misused the map to locate the [gas] and in doing so, their actions fell 'below the generally accepted standards of commercial morality and reasonable conduct'" (quoting precedent). Ricochet's failure to obtain a confidentiality agreement with Ricochet was not dispositive. The court quoted precedent holding that employees are forbidden "from using trade secret information acquired during the employment relationship in a manner adverse to [their] employer, and this obligation survives the termination of employment." According to the court in Lamont, he "did not have authority to destroy the trade secret status of the [seismic map], even after his resignation became effective."

Takeaways

Texas law is quite favorable to owners of trade secrets, more so than the law of some other states. In part, that may account for this decision. However, Lamont's use of the map for purposes in addition to simply making a passive investment also seems to have influenced the appellate ruling.

"But I'm a Whistleblower!": Is an Employee Who Takes Confidential Documents Invincible?

By Guest Author Christopher Robertson (February 4, 2014)

Hypothetical, based upon a real fact pattern:

Employee believes she has witnessed improper activities at her employer and begins preparing a *qui tam* whistleblower complaint alleging False Claims Act violations to file under seal. During the course of preparing the complaint, employee removes highly confidential electronic and original documents from her workplace, copying entire folders of sensitive corporate and personal information and downloading substantial electronic files from the company's secure network. After the complaint is unsealed, the employer learns of the significant theft of information in violation of multiple agreements signed by the employee at the time of hiring. Those agreements prohibit the removal of confidential information and require its return when the employee leaves the company. The employee claims that the removal of this information is protected because it was in furtherance of her whistleblowing activity.

What should the Company do?

The company has a number of options in this situation. First, it may seek to obtain an injunction from the court prohibiting the disclosure of the confidential information and requiring the return of the documents that had been previously removed. For example, in *Zahodnick v. IBM Corp.*, 135 F.3d 911, 915 (4th Cir. 1997), the United States Court of Appeals for the Fourth Circuit upheld an injunction issued by the district court prohibiting the disclosure of confidential information and requiring the plaintiff to return that information.

As to Lockheed's counterclaim for breach of confidentiality, the record discloses that Zahodnick signed two nondisclosure agreements. In these agreements, Zahodnick agreed not to disclose confidential information to anyone outside of IBM and to return all IBM property to IBM when he left IBM's employment. Zahodnick retained confidential materials belonging to IBM after termination of his employment and forwarded those documents to his counsel without IBM's consent. Under such circumstances, the district court did not err either in enjoining Zahodnick from disclosing Lockheed's confidential materials to third parties or in ordering Zahodnick to return all confidential materials to Lockheed. Accordingly, we affirm the district court's order.

The company can also file a counterclaim for independent damages, as long as such claims are not in the nature of indemnification or contribution. That is, they should not be styled as a set-off of the whistleblower claims, but rather an independent claim for damages based on the violation of the employee agreements not tied to the qui tam claims. This was the case in *United States ex rel. Madden v. General Dynamics Corp.*, 4 F.3d 827 (9th Cir. 1993), where the United States Court of Appeals for the Ninth Circuit reversed the district court's dismissal of General Dynamics' counterclaim for

damages holding that "[c]ounterclaims for independent damages are distinguishable, however, because they are not dependent on a qui tam defendant's liability." Although monetizing "independent" damages may be a challenge, the claim is viable.

Likewise, the United States Court of Appeals for the Ninth Circuit has rejected the concept of "blanket" protection for whistleblowers for violation of confidentiality agreements and misappropriation of confidential documents. In *Cafasso v. General Dynamics C4 Systems, Inc.*, 637 F.3d 1047 (9th Cir. 2011), the employee removed vast amounts of confidential information from the company, including attorney-client privileged communications, trade secrets, internal research and development information, sensitive government information and documents under a secrecy order. The employee claimed that "public policy" should allow for the removal of this information by a whistleblower. The Ninth Circuit disagreed, holding that "[t]he need to facilitate valid claims does not justify the wholesale stripping of a company's confidential documents." In so holding, the court affirmed the district court's grant of summary judgment to General Dynamics on its counterclaim against the employee.

Because an injunction is often the first and best option, a company that learns of the removal of information in violation of its confidentiality agreements with employee should not sit on its rights. It should demand that no information be disclosed to third parties and all confidential documents returned. If the demand is rejected, it should take action to protect itself. Waiting after knowledge could negatively impact the ability to obtain an injunction. If quantifiable, the company can also seek independent damages.

What are the risks to the employee?

Until recently, an employee removing confidential information likely correctly believed that the worst that could happen is she would be enjoined from using or disclosing the information or required to return it. A recent decision in New Jersey, however, has potentially increased the stakes for employees. In *State v. Saavedra*, 2013 WL 6763248 (N.J. App. Dec. 24, 2013), a public sector employee took highly confidential original documents from the North Bergen Board of Education. These documents included sensitive personal information, such as individual financial and medical information regarding individual students. The employee asserted that the criminal indictment against her for the removal of this information was required to be dismissed because the information was taken in furtherance of her claims under the New Jersey whistleblower law. The appellate court disagreed and upheld the indictment, refusing to "categorically insulate" employees from criminal theft and official misconduct statutes if they take documents, even as a whistleblower.

Although a company often feels helpless to stop the removal of information by whistleblowers either cooperating with the government or building their own claims, and the trend has been to not punish employees cooperating with the government, a company is not without recourse. Judicial avenues are available, and in the most egregious cases, possibly even criminal prosecution. Having clear confidentiality policies signed by the employee, however, is critical.

Christopher Robertson is a partner and co-chair of Seyfarth's Whistleblower Team. If you would like further information or to submit a question regarding this post please contact the Whistleblower Team at *ask-whistleblower@seyfarth.com*.

Texas Trade Secrets Decision Helps Energy Companies

By Randy Bruchmiller (February 6, 2014)

Seismic information about potential oil and gas reservoirs and other sensitive data are regularly used by energy companies to make business decisions and compete in the market. Energy companies must take reasonable precautions to protect such trade secrets. For example, trade secret status may be destroyed if the trade secret is disclosed to a party that has not signed a confidentiality and nondisclosure agreement. This area of Texas law continues to develop, as illustrated by an important new case, *Lamont v. Vaquillas Energy Lopeno Ltd.*, No. 04-12-00219-CV (Tex. App. — San Antonio, Dec. 11, 2013). This post is a follow up to our prior discussion of *Lamont*.

Background

Hamblin and Lamont owned Ricochet, which entered into a prospect generation agreement with Vaquillas and JOB. Pursuant to the agreement, Ricochet agreed to generate oil and gas prospects and give Vaquillas and JOB a right of first refusal for exploration and development. The agreement also vested Vaquillas and JOB with a proprietary interest in all acquired or generated data and interpretations of any accepted prospects.

In September 2004, Ricochet's geologist identified the Lopeno Prospect gas reservoir, which covered 161 acres in South Texas and contained an estimated $40 million to $60 million in natural gas. The Lopeno Prospect overlapped two contiguous tracts of property, Worley property and El Milagro property. A seismic map of the Lopeno Prospect was created.

In September of 2005, Hamblin and Lamont met with Vaquillas and JOB to discuss the Lopeno Prospect. Vaquillas agreed to participate as a 20 percent working-interest owner and JOB agreed to participate as a 15 percent working-interest owner. Ricochet retained the remaining percentage of the working-interest in the Lopeno Prospect. Ricochet then obtained a lease on only the Worley property because the El Milagro property was in litigation at the time over a previous lease.

Ricochet only showed the seismic map of the Lopeno Prospect to working-interest investors. There was no evidence it was ever made public.

In August 2006, Lamont notified Hamblin that he wanted to separate from Ricochet. In February 2007, agreements were signed dividing Ricochet's oil and gas prospects between Lamont and Hamblin (and made them retroactive to Dec. 31, 2006) and Lamont tendered his resignation, which he also said was retroactive to Dec. 31, 2006. At the same time, Lamont signed a joint operation agreement with Ricochet for the Lopeno Prospect as a 29 percent working-interest owner.

In February 2007, Lamont met with Carranco, a CPA and oil and gas investor, to offer him 10 percent of Lamont's 29 percent working-interest. Ricochet's geologist, at the direction of Hamblin, emailed

Lamont the seismic map of the Lopeno Prospect. The purpose of sending the map was so that Lamont could entice Carranco to invest in the Lopeno Prospect. Carranco then purchased the 10 percent of Lamont's 29 percent working-interest in the Lopeno Prospect. Lamont and Carranco were not required to sign a confidentiality agreement before receiving the seismic map.

Lamont and Carranco then formed a new entity and secretly leased the adjoining El Milagro property, paying an up-front cash bonus of $1 million. Ricochet was attempting to secure a lease on the El Milagro property at the same time. During the next six months, a company owned by Lamont depleted the Lopeno Prospect gas reservoir, thereby preventing Ricochet from withdrawing the same.

Trial

Vaquillas and JOB then sued Lamont and Carranco for trade secret misappropriation and other torts. At trial, the jury awarded Vaquillas and JOB $4.9 million in damages.

On appeal, Lamont argued that the map was not a trade secret because its secrecy was forfeited when it was disclosed to him and other potential investors who did not sign confidentiality/nondisclosure agreements. One key issue is whether, at the time the seismic was emailed, Lamont was in a confidential relationship with Ricochet. Lamont argued that he was not because he made his resignation letter (which was given after the email) retroactive to a date before the email with the secret map was sent.

The court pointed out that Lamont, as a former employee/officer of Ricochet, had a common law duty to protect and not disclose the confidential information learned during his employment, a duty which continues after the employment ends. The court found that Lamont was, at the very least, a prospective investor when Ricochet's geologist emailed him the map. Carranco was also a prospective investor when he was shown the map.

The court of appeals rejected Lamont's argument and held that "[t]rade secret status is not destroyed simply by showing the protected item to prospective buyers, customers, or licensees." In other words, the disclosure of a trade secret to potential investors to enable them to decide whether to invest does not destroy secrecy. Those who learn of the confidential information under such circumstances are not authorized to destroy its protection and may not use the information in a manner harmful to the interests of the one making the disclosure, even if they were not required to sign confidentiality/non-disclosure agreements.

Lamont and Carranco were also unsuccessful in trying to argue they obtained information that lead them to lease the El Milagro property by means independent of Ricochet's information. Information taken from the seismic data and other information from Ricochet was used by Lamont and Carranco in documents to obtain a bank loan necessary to pay for the working-interest in the El Milagro wells. The evidence also indicated that Lamont and Carranco did not conduct any independent research of the gas reservoir before leasing the El Milagro property.

Lessons Learned

The most significant development from this case is further clarification that companies may be protected by common law if they disclose trade secret information to an investor without a confidentiality and nondisclosure agreement in place.

When consulted by energy companies regarding their internal practices, it is important to consider the use of confidentiality agreements. Despite the holding in Lamont, it is important for energy companies

to require confidentiality and non-disclosure agreements with their employees, potential investors, contractors, vendors and others who may come in contact with their confidential and trade secret information. While common law and other protections do provide some protection in some circumstances, such as those described in Lamont, the best practice is to also have agreements in place to provide an extra layer of protection.

If a confidentiality and nondisclosure agreement is in place and there is a breach of the agreement, companies have a much better chance of being awarded attorneys' fees in the course of any subsequent litigation. Attorneys' fees have traditionally not been available when suing the disclosing party for a breach of their common law duty (as opposed to a contractual duty due to a confidentiality agreement), although the ability to recover attorneys' fees has improved with the recent adoption of the Texas Uniform Trade Secrets Act.

Confidentiality and nondisclosure agreements also allow companies to broadly define what information is confidential so that it is difficult to argue otherwise in litigation. Confidentiality and nondisclosure agreements also help combat a defense commonly raised in this type of litigation — that the holder of the confidential or trade secret information did not take steps to protect the confidentiality of the information. The bottom line is that companies have significantly more protection when they have confidentiality and non-disclosure agreements in place.

Loose Lips Sink Ships! Can an Employer Ask a Whistleblower to Keep Her Complaints "Confidential"?

By James Beyer (February 10, 2014)

Hypothetical, based upon a real fact pattern:

Sally works for a chair manufacturer and believes the chairs are made with unsafe and illegal toxins. Sally reports her concerns to the head of HR. Sally also says that she thinks her supervisor is "harassing" her for raising this with him because he gave her a bad performance rating. The HR Head thanks Sally for raising her concerns and makes it clear that he appreciates Sally bringing this to his attention and tells Sally that the Company takes such issues extremely seriously. He also states that the Company policy forbids retaliation in any form against any employee for reporting such actions. He also then says that the Company will investigate the allegations and that as part of that investigation it will need to determine what other employees it may need to speak with. In order not to "tip off" other employees in advance and also to protect confidentiality to the extent possible, the HR Head asks Sally not to discuss the investigation with other employees and to keep the investigation confidential. Not more than 10 minutes after Sally leaves his office, the HR Head gets a call that Sally is out on the shop floor loudly telling other employees that she thinks the chairs are made with unsafe and illegal toxins and that she has reported it to HR and may also inform the government of her concerns. Can the employer discipline Sally for violating its instructions to maintain confidentiality?

What should the Company do?

Even though the employer certainly had a valid reason to ask Sally to keep the investigation confidential and not to discuss it with others, disciplining Sally for violating these instructions is quite risky.

There do not appear to be decisions directly addressing this issue in the context of whistleblower claims. In one case that we reported on as one of the top 10 whistleblower decisions of 2012, an employee was terminated as part of a large reduction in force. Prior to her termination, Plaintiff alleged that she discovered what she believed to be reporting discrepancies and reported them to her supervisor, who forbade her from discussing her findings with co-workers or anyone outside of her department. The court held that the alleged instruction not to discuss the matter with her co-workers or anyone outside her department was one of the factors that showed that there were material issues of fact as to whether the Plaintiff engaged in protected activity which meant that the case would not be dismissed before a trial on the merits.

Outside of the realm of whistleblower cases, there has been a virtual cornucopia of National Labor Relations Board activity finding that any instruction to keep investigations confidential are unlawful under the NLRA because they have a tendency to chill employees from exercising their statutory rights under Section 7 of the Act to engage in concerted activity. Even policies that "recommend" employees

maintain the confidentiality of investigations have been struck down because there was nothing assuring employees that they were "free" to disregard the Company's recommendation/request. See here.

In addition, It may be only a matter of time before the EEOC joins the fray. See here.

An August 2012 pre-determination letter issued out of the EEOC's Buffalo, New York district office cautioned an employer that its policy of warning employees not to discuss harassment investigations with co-workers could be a violation of Title VII's anti-retaliation policies. The letter seems to run afoul of the EEOC's longstanding enforcement guidance that directs employers conducting investigations of workplace harassment to "protect the confidentiality of harassment complaints to the extent possible." This may signal an emerging trend within the agency as a whole.

In light of this uncertainty, employers may want to:

- Limit confidentiality instructions to investigations of complaints and issues that implicate or are likely to implicate EEO or other legal issues or when investigation integrity is a particular concern;
- Consider and document why confidentiality is necessary to a particular investigation;
- Tailor the confidentiality requirement to the specific subject matter of the investigation and matters discussed in investigatory interviews while the investigation is ongoing;
- Limit the confidentiality instruction to employees who will or are likely to be interviewed during the investigation because they have personal knowledge of events or other directly relevant information;
- Clarify that the confidentiality restriction is not intended to prevent employees from addressing concerns with one another or with the employer; and
- Explain to witnesses that the purpose of the confidentiality restriction is to:
- Preserve the integrity of the investigation process;
- Encourage employees to speak up when they have a problem and give them confidence that they may speak the truth;
- Uphold an anti-retaliation policy; and
- Allow the company to conduct thorough and objective investigations, which, in turn, allows the employer to effectively address employee complaints and concerns and resolve workplace conflict.

It also may be appropriate to forgo the threat of discipline for individuals who breach confidentiality or at the very least make clear that the confidentiality instructions are not intended to interfere with employees' Section 7 rights, including the right to discuss wages, hours and working conditions with their co-workers.

Massachusetts Court Confirms That When It Comes To Trade Secrets, Confidentiality Is Key

By Dawn Mertineit (February 14, 2014)

A recent case in Massachusetts confirms that taking affirmative steps to protect the confidentiality of trade secrets is absolutely critical to litigating a claim for misappropriation. In *C.R.T.R. v. Lao*, Plymouth Superior Court Docket No. 2011-962 (Dec. 30, 2013), the plaintiff sued a former independent contractor for, among other things, misappropriation of the company's trade secrets. The defendant moved for summary judgment on the grounds that the information allegedly misappropriated was not a trade secret, and that even if the information were a trade secret, the company had not taken adequate steps to protect the information. The court agreed with the company that there was a genuine dispute of fact over whether the information allegedly taken by the defendant constituted a trade secret, in light of the company's identification of several trade secrets — including prices paid by the company and its customers, amounts sold and purchased, billing procedures, customer lists, business processes and work flow patterns, and processes for obtaining customers, among other things. The court also determined that the company had put forth sufficient evidence to suggest that the information provided the company with a competitive advantage, and that it was not generally known to those outside the business, both hallmarks of a trade secret.

But the court's inquiry didn't end there. Instead, the court determined that in order to support a misappropriation claim against the independent contractor, the company would have to demonstrate that it took adequate steps to protect its trade secrets. The court noted that the company had not required the defendant to sign a confidentiality agreement, and that the company did not even have a policy regarding the protection of confidential information. Additionally, the company's customer lists were available on the company's computer systems and certain contracts were advertised on the company's website. In light of these facts, the court held that there was no evidence that the company had taken appropriate measures to protect its trade secrets, and accordingly granted summary judgment on the misappropriation claim.

This ruling should serve as a warning to employers — even if you are able to demonstrate that information obtained or accessed by a former employee, independent contractor, or other individual or entity is indeed a trade secret, a failure to "exercise eternal vigilance" in protecting those trade secrets will doom a misappropriation claim. Employers should not only implement and distribute policies regarding the protection of confidential information, but it should also require its employees, independent contractors, or other individuals who are granted access to such information to sign a confidentiality agreement. Failure to do so could be catastrophic to your business.

Tricks of the Trade Secrets – Can Casino Applications Be Kept Confidential?

By Erik Weibust and Dawn Mertineit (February 28, 2014)

With the recent slew of casino application filings being submitted to the Massachusetts Gaming Commission, following the passage of the Massachusetts Expanded Gaming Act in 2011, a new question has many on Boston's Beacon Hill scratching their heads – can the contents of such filings be considered trade secrets?

The Gaming Commission's standard casino application form includes a list of 47 filings that the Commission presumes applicants will want to keep confidential, but applicants can request that additional filings also be kept confidential. Recently, Wynn Resorts submitted an application to the Gaming Commission for a proposed casino in the Boston suburb of Everett, and requested that an additional 38 filings (constituting 77 pages total) be considered trade secrets protected from public disclosure. These filings include Wynn's plans for how the proposed casino will fit the "Massachusetts brand," its plans for staff training to identify gambling addicts, and the company's plans to work with minority- and female-owned businesses.

That drew the disapproval of newly-inaugurated Boston Mayor Marty Walsh, who expressed skepticism that the sealed portions of the application should be kept confidential. Walsh told the *Boston Herald* that Wynn's lack of full disclosure was "alarming." Nonetheless, Wynn spokesman Michael Weaver insisted that the filings include "sensitive financial and strategic company information," thus requiring their protection as trade secrets.

Meanwhile, Mohegan Sun's rival proposal to build a $1.3 billion "gambling resort" in neighboring Revere, which just this week won the approval of the city's voters, only requested that two additional filings beyond the standard 47 be kept confidential. Mohegan Sun issued a public statement that it "believes openness is important in the licensing process, and our application allows not only the Gaming Commission but our host community, surrounding communities and the public to examine and understand our proposal."

As the two companies square off for the sole casino license in eastern Massachusetts, Wynn's broad invocation of its trade secrets protection may ultimately be its downfall.

Stay tuned for the resolution of this high stakes game.

Global Business 101: Hire Your Competitor as a "Consultant"

By Anthony Orler (March 20, 2014)

Why spend millions of dollars employing a bunch of bright, talented employees to develop your business when you can just hire a worker from your rival to steal all their research? As on every test you took in school, isn't getting the right answer more important than figuring out how to solve the problem?

Competition for business is fierce. Small price differences or lower development costs can win your company any number of contracts. How can one effectively compete in today's marketplace?

Some companies, in a word, cheat.

Korea-based KCC Silicones hired chemist Michael Agodoa of Michigan-based rival Wacker Chemical Corp. as a consultant in 2010. Rather than taking years to determine the proper formulas and millions in experimentation costs on plastics used in extrusion, silicone mold making materials, and elastomers, KCC employed Mr. Agodoa to steal over 100 of Wacker's trade secrets.

Isn't this what business people call a "win-win" situation? Mr. Agodoa probably made enough extra cash to have a nice vacation or two. KCC didn't have to waste any time testing and certainly received a large "ROI" (return on investment). Business, after all, is business.

Wacker Chemical spent two *decades* developing and refining their manufacturing methods. Mr. Agodoa's defense was that he shared Wacker's knowledge and experience "in the spirit of scientific cooperation" over a period of two *years*. In other words, KCC bought eighteen years' worth of intelligence for the price of one consultant.

Facing up to forty-six months behind bars, Mr. Agodoa plea-bargained his way to a two-year federal prison sentence and a $7,500.00 fine. Wacker Chemical's losses were estimated at more than $15 million.

Trade secrets are valuable weapons in today's global marketplace. Trade secrets are often very costly to develop, and may provide the competitive edge for your company. Although Mr. Agodoa only faced federal trade secret charges, the addition of even harsher criminal penalties under the Economic Espionage Act will hopefully make employees think twice about taking that moonlighting "consulting" job.

Federal prosecution for trade secret theft is a "closing the door after the horse has left the barn" approach. Yes, it is nice to know that your trade secrets are protectable and additional statutes are increasing that protection. As employers, however, it may be prudent to make your employees aware of the potential penalties before they decide to sell your proprietary information. The Office of the National Counterintelligence Executive is a good place to look for materials that may be useful in your workplace.

Trading Secrets

As with students of every age, the temptation is to take the path of least resistance. Just as with students, the reward is potentially great; your company could win that lucrative contract or catch up to the competition in a short amount of time. Just find a way to "borrow" your competitor's know-how.

With trade secret theft, and the Economic Espionage Act, the penalty is not a few days of vacation from school and a meeting with some toothless academic honor board.

You, like Mr. Agodoa, get to head straight to a federal penitentiary.

For more details on *U.S. v. Agodoa*, 13-cr-20525, (E. D. Mich. 2014), see the Rubber News article and the Bloomberg News article.

Trade Secrets: A New Framework

By Guest Author Pamela Passman (March 24, 2014)

As a special feature of our blog – special guest postings by experts, clients, and other professionals – please enjoy this blog entry by Pamela Passman, President and CEO for the Center for Responsible Enterprise and Trade (CREATe.org)

-Robert Milligan, Editor of Trading Secrets

Around the globe, dozens of countries are considering or enacting legal reforms to grapple with the growing misappropriation of trade secrets. As these changes lumber forward, it remains to be seen how new laws will be enforced, and whether legal remedies will offset the losses from theft.

In this uncertain landscape, companies must invest in practical, preventive measures to address the risk to their valuable intellectual assets, according to a new report, "Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats."

The report by the Center for Responsible Enterprise and Trade (CREATe.org) and PriceWaterhouseCoopers provides a fresh look at the problem of trade secret theft — including an estimate of the magnitude of the problem and analysis of the main types of perpetrators, their motivations and means. It also develops several scenarios suggesting how the effectiveness of regulation, the openness of the internet, and cyber threats could play out and impact the environment for the protection of trade secrets in the coming 10-15 years.

Practical Measures in an Uncertain World

For companies, this analysis provides a backdrop for addressing the immediate and pressing challenge: How to protect trade secrets in a rapidly changing and risky global marketplace?

The report offers companies an original framework for protecting valuable competitive information that has been developed through experience, investment and research.

A series of practical measures, the report argues, should be adopted throughout the company's operations — and shared or required of contractors and business partners throughout the global supply chain, to the greatest extent practical.

The five-part framework — illustrated with the help of a fictional company, ABC Widget— starts with making an inventory of trade secrets.

ABC is billed as a large, global, publicly traded, U.S.-based alternative energy company with a widely dispersed global supply chain.

Get a Handle on the Goods

The inventory process starts with "a cross-functional team of senior executives, business unit leaders and corporate functional leaders" who are asked to make lists of key company information in five categories: product information, research and development, critical and unique business processes, sensitive business information, IT systems and information.

"Participants arrive at the working session with their lists, which they present, discuss, and compile into a master list that aligns with ABC's views about what constitutes a trade secret. The meeting results in a categorized list of valuable trade secrets reflecting critical elements of ABC's business model."

With that, a team of security professionals moves into action:

"Using tools that search based on keywords and other identifiers, trade secrets from the master list are found on various servers, in files with non-relevant file names, and on shared-file sites created for reasons unrelated to the trade secret itself. The results for the location of each trade secret found are noted on the master list, to be incorporated later into the vulnerability assessment."

The security team also works with the other business leaders to find trade secrets that are not digitized — things like hand written notes and prototypes — in an effort to make the inventory as comprehensive as possible.

Pick Your Poison

The second step is to assess the "threat actors" that present the greatest risk to the company's assets, given its specific industry and areas of operation—and how company security systems measure up.

Various perpetrators — competing companies, transnational criminal organizations, "hacktivists," nation-states and "malicious insiders" in the company have various means of stealing trade secrets and a variety of motivations, including pure profit, nationalistic advantage and political or social goals.

Companies involved in military technologies or dual-use technologies that have civilian and military applications, for instance, will need to factor in the threat from governments that have been known to steal information through cyber attacks or by dealing with "malicious insiders" who work for the company.

Where to Put the Money

From there, the report walks through level three of the framework — ranking trade secrets according to the impact that their theft would have on the business.

Step four is to assign a dollar cost to those hypothetical losses. This includes direct impact on performance, including lost sales revenue and market share. It also includes indirect losses, where there is damage to investor confidence, customer trust or other secondary impacts.

So, in the case of the fictional ABC alternative energy company, the report explores the indirect dollar impact from stolen source code:

ABC… investors may assert that the company lacks appropriate controls and protection processes to support sustainable growth, deciding to sell shares despite the absence of direct financial consequences of the theft. Also, if discussion of the theft trends on social media blogs or is covered by

traditional media, it can influence long-term customers' buying decisions. Similarly, the theft may erode the trust of the company's key business partners.

After assigning costs to the damage, the company is in a position to make decisions and investments — step five — to invest its resources to mitigate the most significant potential threats to trade secrets.

This, of course, is the bottom line: Companies need to understand, assess and embrace their trade secrets, and develop security around them. In the global economy, this security is an investment, rather than a cost.

###

Pamela Passman is President and CEO of the Center for Responsible Enterprise and Trade, a non-profit organization working with companies to protect intellectual property and prevent corruption in global supply chains. Previously, Pamela was the Corporate VP and Deputy General Counsel, Global Corporate and Regulatory Affairs at Microsoft Corp and has practiced law with Covington & Burling (Washington, DC) and Nagashima & Ohno (Tokyo).

Trading Secrets

The Two Billion Dollar Zhu Zhu Pet, Sold for $5k: Puffing in Trade Secret Misappropriation Pleadings May be Perilous

By Anthony Orler (March 27, 2014)

Zealous advocacy, copious use of Latin, and literary devices advantageously applied to attack our adversaries' arguments. These are the cornerstones of American legal representation.

These tools are part of the *modus operandi* of every lawyer. This article may use dead language and assonance as running themes, but some lawyers take zealous advocacy *ad infinitum*. Such attorneys are rarely even admonished by the courts, much less sanctioned. That said, theNinth Circuit has approved sanctions against an attorney for "misrepresentations" made in the complaint of a trade secret lawsuit.

Wait a minute…the COMPLAINT? The boiler-plate statement "upon information and belief" was somehow omitted? After the trial is over and the bad, bad defendant is found to be not so bad after all, is not all that bluster and bravado in the complaint long forgotten?

N.B.: Perhaps not.

Although they are called "pleadings" for a reason, statements in the pleadings must be at least "grounded in fact" to pass muster as fact, even in the complaint. Synonyms used to impress clients might better be left to other writing exercises, *e.g.*, fantasy novels and fairy tales.

In *Heller v. Cepia LLC et al.*, 11-cv-1146 (N.D. Cal. 2011), Jason Heller claimed that Cepia, the makers of "Zhu Zhu Pets" robot toy hamsters, used the same features and accessories he had disclosed to toy manufacturers in his prototype designs. Mr. Heller asserted, *inter alia*, that the manufacturers forwarded his trade secrets to Cepia, who then used his ideas in the Zhu Zhu Pets products.

In the 2011 complaint, Mr. Heller's attorney alleged that visitor logs at one of the manufacturers "appeared to confirm" that Cepia had visited the manufacturer. Mr. Heller then "confronted" the manufacturing company who "refused" to provide information about any relationship with Cepia.

Sort of benign, isn't it? Some visitor logs and a request for additional information that was denied. *Prima facie* this does not seem to be sanctionable writing or behavior. Yet the use of "appeared to confirm" and "confronted" are why Mr. Heller's attorney was sanctioned.

This puffing seems rather tame in comparison to the damages Mr. Heller sought: over **$2,000,000,000.** Yes, two **Billion**. For a toy hamster? Such a damage request, seemingly made rather boldly across several pages in the complaint, appears somewhat less *bona fide* than something couched with "appeared," and, remarkably, did not even rate a *de minimis* or *dicta*mention by the court as raising any cause for concern.

No wonder there are so many cries for tort reform.

Fast forward to a year later, where, on joint stipulation, the complaint was dismissed against Cepia with prejudice. *Per se*no sanctions, right?

Wrong.

In part of the *quid pro quo* for the dismissal stipulation, Cepia received Mr. Heller's acknowledgement that "he did not find any evidence that Cepia had any access to any of Mr. Heller's hamster toy ideas or information" in the documents and evidence produced during discovery.

First mistake: saying, "There is nothing in any of the evidence showing the defendant was bad." Because then the complaint looks like, oh, a big lie.

Second mistake: letting a client say, "There is nothing in any of the evidence showing the defendant was bad." Because then it looks like the attorney fabricated the complaint *ab initio*. And yes, now sanctions may be apropos, in this case to the tune of $5,000.00 from the Northern District of California.

Mr. Heller's attorney appealed, arguing in his appellate brief that "in hindsight, my wording could have been better." Admitting the wording was misleading is likely a third mistake.

Mr. Heller's attorney then tried to save the day, *ibid*, by arguing that his letter to one of the manufacturers constituted a "method of confronting them on the issues."

Fourth mistake: unless you are a Court of Appeals for the Federal Circuit judge, you are not allowed to construe the meaning of words *de novo*.

Confront means "to oppose or challenge (someone) especially in a direct and forceful way" or "to directly question the action or authority of (someone)." (Merriam-Webster).

The complaint implied that someone went to the defendant's place of business and spoke to them face-to-face, or challenged them to prove they were innocent. Nope. His attorney dashed off a quick note saying, in essence, "Hey, thanks for the visitor logs, can you tell us a little more about your relationship with Cepia?" The defendants did not answer. There was no confrontation, and the visitor logs didn't confirm any visits by Cepia.

In reality, the only mistake here was somebody thinking it was a good idea to make the defendants appear uncooperative and/or hiding the truth. Had the complaint contained the facts, instead of something that sounded a little more ominous, the lawsuit would have still gone forward exactly as it did.

Everything except for the sanctions.

For more on *Heller v. Cepia*, see the Law360 Article.

Trading Secrets

Tips for Ensuring Your Competitors Do Not Steal the Valuable Fruits of Your Research and Development

By Katherine Perrelli and Erik Weibust (March 28, 2014)

Every employer in the pharmaceutical industry is keenly aware of the need to ensure that a departing employee, a potential investor, or a business partner does not misappropriate the company's valuable trade secrets. If such valuable information falls into a competitor's hands, they may use it to gain a significant market advantage. Companies in the pharmaceutical industry face unique challenges because, while the fruits of their research and development are often protectable as trade secrets, companies are often required to communicate this valuable information to potential investors, partners, and governmental agencies, such as the U.S. Food and Drug Administration (FDA). Because pharmaceutical companies spend an extraordinary amount of money on research to develop new products, understanding how much of this valuable information is protectable as a trade secret, and how best to protect such information, is key to the company's success, regardless of whether its products are in early stage development or are well-established in the industry. This article is the first in a series about protecting trade secrets and enforcing non-competition agreements in the pharmaceutical industry.

I. Trade Secrets Specific to the Pharmaceutical Industry

First we will address what kind of information you can protect and then we will explain how to protect it.

Companies cannot protect information contained in patent applications and patents as trade secrets, because they must disclose that information publicly to the U.S. Patent and Trademark Office (PTO) and ultimately to the public at large. However, there are many types of information at all stages of drug development, from the discovery phase through the commercial launch, that a company can protect as trade secrets. Indeed, the most sensitive information is often developed early in the process, before the company can even request a patent.

Early Research & Development. In the discovery or pre-clinical phase, a company generates a great deal of useful information that it can protect as trade secrets. Most of this information is intangible data, formulations, or processes, as opposed to tangible products. This includes, for instance, a "vision plan" (i.e., brainstorming of possible drug candidates, plans of attack, etc.), data regarding which candidates are viable and which pathway to follow, and early manufacturing techniques that the company has considered.

Product Development. During the development phase, a company generally produces more tangible products, processes, and data. For instance, during the clinical trials, a company can protect all of the following as trade secrets: lead candidate information, optimization data, bench trials, synthesis (organic or recombinant), formulations, safety and efficacy information, and clinical trial sites and data.

Approval. At the approval stage, a company can protect the following as trade secrets: FDA interactions, risk evaluation and management systems (REMS) data, current good manufacturing

practices (cGMP), quality assurance and quality control (QA/QC), and ICH compliance. While the Company will have to share much of this information with the FDA to obtain approval, as discussed below, it can nevertheless maintain its trade secret status.

Post-Approval. Following the approval of a new drug, the most sensitive information is generally commercial in nature, such as sales data, marketing plans, customer lists, general marketing feedback, cost of goods sold (COGS), supply chain information and integrity, sales forecasts, adverse drug events, new indications, life cycle management, and new plans for related development.

II. Protecting Trade Secrets

Information and data from the early stages of new drug research and development is arguably the most sensitive, because its misappropriation can lead to the most severe consequences. Specifically, a competitor could use misappropriated information to develop the same product and obtain patent protections before the original company even discovers that the information is missing. This is particularly problematic if the company utilizing the misappropriated information has greater resources and can develop the drug more quickly. Indeed, there are generally three motivations for misappropriating trade secret information during this early stage: (1) to directly compete by racing to develop the drug first; (2) to indirectly compete by creating another drug candidate in the same therapeutic class or by creating a combination therapy; and (3) to apply for patent protection under the new "race to file" system and thereby block out the original developer from doing so. Of course, information from the later stages is also highly important and must be protected, but that type of information—which is generally more commercial in nature—is less unique to the pharmaceutical industry, and there is not much commercial damage if the original company has patents in place.

We recommend the following processes to our pharmaceutical clients in order to ensure that you protect your valuable trade secrets: Implement and enforce strict post-employment restrictive covenants (i.e., non-compete and non-solicitation agreements) and non-disclosure or collaboration agreements with third parties (i.e., potential investors and partners) (stay tuned for part 2 of this series). In addition, you should create and disseminate internal and external policies and procedures (see part 3 of this series), including:

- Onboarding checklist and exit interview policies and procedures;
- Confidentiality policies and procedures (including annual training programs and disciplining or termination of employees who improperly disclose or use confidential information);
- Work from home policies and procedures;
- Internal notebooks that are marked confidential and kept in secure spaces, password protected computers, or clean rooms;
- USB usage policies and procedures;
- Social media and internet usage policies and procedures; and
- Cell phone usage policies.

Similarly, you should consider hiring an outside professional to conduct annual or semi-annual trade secret audits to determine how easy or difficult it is to exfiltrate sensitive information. You can even install mobile device management software that can protect sensitive information from being exfiltrated

through mobile devices such as iPhones, and also permit the company to access and/or wipe company information if a mobile device is stolen or lost, or an employee leaves the company.

Finally, you may still maintain trade secret status for information that you provide to the FDA despite your limited disclosure for regulatory purposes. Federal regulations governing the FDA specifically exempt trade secret and confidential commercial or financial information from public disclosure by the FDA. Likewise, the federal Freedom of Information Act provides that a federal agency, such as the FDA, may withhold information if it constitutes or contains trade secrets, and certain patent, trademark, and copyright regulations permit companies to redact trade secrets from public filings, subject to certain limitations.

Of course, the best way to ensure that trade secrets are not disclosed, intentionally or otherwise, is to define clearly what information constitutes trade secrets and what your expectations are as to how your employees and investors/partners will treat such information. Moreover, you should only provide such information to those employees or potential investors/partners who need to know it, can be trusted, and are subject to strict post-employment restrictive covenants and/or non-disclosure agreements. The Company should also have a commitment to, and culture of, enforcing these agreements and company policies, and ensuring that anyone giving access to trade secrets understands the serious consequences of disclosure. This is not an easy task, but particularly in the pharmaceutical industry, where so much of a company's fortunes can be tied up in its ideas and development plans, it is imperative that the company take pains to do this correctly.

Covert Cellular: Enough Protection for Trade Secrets?

By Anthony Orler (April 8, 2014)

With the ever-increasing need to maintain communications with customers and your employees, mobile phones have become a requirement for business people. Spanish telecommunications company Geeksphone is targeting the business market with Blackphone, the first mobile phone that encrypts data transmissions. No one would argue against the value of increased wireless data security, but do CIA-style cellular phones really provide enough extra protection to justify the cost?

All cell phone transmissions are encoded in some way, which may be why we feel some level of comfort sending some of our most intimate personal information through mobile devices. We text our friends from Antarctica using satellite phone links, Instagram selfies from the beach, play games with people from all over the world while waiting for a flight (thank you, Alec Baldwin, fordelaying a flight departure because of a "Words with Friends" obsession), purchase goods online (with our credit card numbers sailing through cyberspace) and catch up on email while driving (which may be against the law in some jurisdictions). If these modern conveniences are not continuously available from almost anywhere on the globe, some may consider that cellular service providers have somehow usurped our constitutionally guaranteed freedom of expression.

Business discussions also involve confidential data. If trade secrets are involved, reasonable measures, such as limiting dissemination and providing adequate safeguards on the restricted material, must be taken to maintain legally enforceable protection.

Thanks to Edward Snowden, though, we are aware that Big Brother is essentially recording every transmission from mobile phones. Senator Dianne Feinstein, German Chancellor Angela Merkel, and many Americans consider such data collection "spying." More First Amendment violations.

In light of Mr. Snowden's revelations, the use of cellular communications in business, especially when confidential information is involved, may fall short of the required security threshold.

And thus, a niche market for encrypted cellular communication has been born. With a Blackphone, whomever attempts to record your encrypted calls and texts will record unintelligible data bits instead of a verbatim transcript.

This extra level of protection may be worth the $629 per unit for your company. Indeed, an entire fleet of spy-thwarting cellular phones may be a wise investment if your executives routinely travel to parts of the world where someone in addition to the National Security Agency (NSA) may be listening—and this may be especially true if your company uses wireless networks to send confidential data or trade secrets.

But are Blackphone's hyper-secrecy and extra cost really necessary for confidential data transfer? Possibly not. As another post on this blog reports, 2.5 Exabytes (computer jargon for "a whole bunch") of information are created daily. That means the "c u @ movies @ 7" text you just sent is akin to a single needle in a billion billion haystacks on any given day, so your data is already pretty difficult to locate even without Blackphone's extra level of encryption.

Still, all communications sent over wireless networks, even from a Blackphone, are broadcast in the open, and therefore subject to interception by unwanted prying eyes (and ears). Yes, Blackphone transmissions will be harder to interpret without the special secret decoder ring. And for additional privacy, the Blackphone automatically deletes the transmitted text or call details after the transmission is completed. Therein lies the problem.

Whether Blackphones are company-provided or the personal property of employees, the legal standard courts may use could be, "Does encrypted, public dissemination of a company's proprietary data represent 'reasonable protection'?" Is additional encoding of a public broadcast considered enough of an access limitation?

Further, although the extra layer of encryption may be deemed a limited access, is providing *untraceable* back doors to your private data an adequate safety measure?

Data-encrypting cell phones such as the Blackphone may appear to be the perfect fit for your company's needs, but do not be deluded into a false sense of security; Edward Snowden, after all, used the NSA's own technology to disseminate the agency's secrets. Remember that although Blackphone transmissions are difficult to trace, the data are sent *somewhere*. That means that *somebody* has the key to decode the data—and that might be your competition.

Indeed, the best course of action for your company might be to adopt a policy that prohibits confidential communications via cell phone, and restricts them to an environment that is secure.

If you absolutely must communicate verbally, or with drawings or formulae, you can always forego the phone and communicate *face-to-face* with your clients.

Because even with a Blackphone, the airwaves might just be your competitor's (and a spy's) best friend.

Jury's $920 Million Trade Secret Misappropriation Verdict Vacated

By Paul Freehling (April 9, 2014)

In a stunning *per curiam* ruling, the Fourth Circuit Court of Appeals last week vacated a judgment of nearly $1 billion, and a 20-year non-compete injunction, entered by an Eastern District of Virginia judge in favor of the DuPont Company. The appellate tribunal held that the lower court committed prejudicial error by granting DuPont's pre-trial motion in limine to bar defendant Kolon Industries from offering any evidence relating to an earlier lawsuit involving DuPont. The case was remanded for a new trial before a different judge. *E.I. DuPont De Nemours & Co. v. Kolon Industries, Inc.*, No. 12-1260 (4th Cir., Apr. 3, 2014).

Summary of the Case

DuPont maintained that one or more former employees, working as consultants to Kolon, misappropriated DuPont's trade secrets relating to the manufacture and marketing of "Kevlar," a strong, synthetic fiber used, for example, in bullet-resistant armor. Kolon contended that what the consultants disclosed was not confidential because it was part of the public record in prior trade secret misappropriation litigation DuPont filed against a company — not Kolon — that was, at the time, DuPont's primary competitor with respect to "Kevlar."

Granting DuPont's in limine motion in the Kolon case, the trial court ruled that any reference to that prior lawsuit would be confusing and prejudicial. The Court of Appeals reversed, holding that the trial judge's "wholesale preclusion of any mention" of the earlier litigation was arbitrary, irrational, and an abuse of discretion.

Kolon also contended that the trial judge should have recused himself because he formerly had practiced law at the firm representing DuPont in both the earlier and this litigation. That contention was rejected on appeal — 2-1 — as untimely but, in the exercise of its "supervisory powers," the panel unanimously directed the Chief Judge of the district court to whom the case was remanded to assign a different jurist to conduct further proceedings.

Origin of the Lawsuit

Former DuPont employee Mitchell, who had extensive knowledge concerning the manufacturing and marketing of "Kevlar," allegedly communicated repeatedly with Kolon about the product. In the course of an FBI investigation of Mitchell's conduct, he agreed to cooperate. As a result, Kolon and several of its officers were indicted for theft of trade secrets, conspiracy, and obstruction of justice. DuPont then sued Kolon.

The Erroneous Pre-Trial Evidentiary Decision

Kolon contended, in its defense to DuPont's misappropriation claims, that at least some of the trade secrets at issue in this case were "strikingly similar" to details of the production process described in

exhibits in the court's public files relating to DuPont's earlier lawsuit against the different competitor. Moreover, one of Kolon's witnesses was an expert witness for DuPont in the previous litigation. Mention of the prior case seemingly was inevitable at the Kolon trial. The trial judge granted DuPont's motion in limine to bar any reference to the earlier lawsuit on the ground that no showing had been made that a trade secret at issue in the Kolon case actually was disclosed in the earlier trial. The appeals court held, however, that the lower court applied "too stringent a standard for admissibility. Under the circumstances [here], a 'strikingly similar' standard of relevance is enough" to allow the jury to decide whether the information retained the requisite confidentiality.

Takeaways

Although the Fourth Circuit's opinion is designated "Unpublished" and, therefore, "not binding precedent," it seems to include carefully drafted guidelines regarding pretrial motions. The appeals court recognized that streamlining a trial and "fostering the orderliness of evidentiary presentations of complicated issues cannot be doubted" but cautioned that "a court is often wise to await the unfolding of evidence before the jury before undertaking to make definitive rulings on the likely probative value of disputed evidence." By the same token, a party who succeeds in obtaining an in limine instruction and who prevails at the subsequent trial may find that it was an exercise in futility. Lengthy trials — the one between DuPont and Kolon lasted seven weeks — are costly, and a retrial adds expense. So, litigants should think carefully before seeking to exclude a large volume of evidence.

Another lesson learned in this litigation is that confidential information disclosed in the course of a misappropriation trial thereafter may cease to qualify as confidential.

Finally, the Fourth Circuit's plurality and partially dissenting opinions relating to Kolon's effort to disqualify the trial judge also may be instructive in a future case. The plurality of the *per curiam* court denied disqualification, but all three judges voted nevertheless to remand for further proceedings before a different judge. So, consideration might be given to requesting, as an alternative in a federal appellate court motion seeking a recusal on remand, the exercise of "supervisory powers" with respect to assignment of another trial judge. Both requests seek substantially the same relief.

Randy Bruchmiller Discussing the Finer Points of the Texas Uniform Trade Secrets Act

By Randy Bruchmiller (April 14, 2014)

https://www.youtube.com/watch?v=ArOLwZbc2L4

The Texas Uniform Trade Secrets Act was signed into law in 2013 and applies to any misappropriation of trade secrets occurring on or after September 1, 2013. Texas trial and appellate courts will be interpreting these new provisions of Texas law as new trade secrets cases work their way through the legal system. Randy Bruchmiller weighs in on a couple of the new provisions that have already received considerable discussion in the legal community.

Trading Secrets

Patent and Trade Secret Protection: Turning Nightmares into Sweet Dreams

By Anthony Orler (April 24, 2014)

You arrive home from another long day at the office, have some dinner, start to catch up on the day's news on the couch, and slowly doze off…

…you are back in the office, and one of your employees comes to you with an idea that will make your company boatloads of money. You call your attorney and tell him you want this idea protected, immediately, if not sooner.

"What's the idea?"

"I can't tell just anyone."

"Well, if you want a patent, you are going to have to tell the whole world. Okay, let's go about this another way: How hard would it be for your competitors to figure out your approach once you start using it to make your products?"

"Pretty easy. If they cut open one of our devices, they could figure out what we're doing."

"So, what do you want to do?"

"AHHH!"

You awaken in a cold sweat, realizing that protecting your company's Intellectual Property (IP) really does keep you from sleeping well at night. Your "dreamy" attorney, however, asked at least some of the right questions regarding the protection of your company's IP.

The first question is one of disclosure. If you want a patent, trademark, or copyright, then you are required to disclose the idea to governmental agencies, in statutorily gory detail. But if you are reluctant to even tell your *attorney* about it, getting a patent may not be the best way to protect that blockbuster idea.

And assuming that you *are* willing to divulge the inner workings of your concept, remember that not everything can be patented. Patents can protect only four basic categories: methods; devices; articles produced by giving raw materials new forms, qualities, properties, or combinations; and compositions of matter. You cannot obtain patent protection on an equation (Albert Einstein could not patent E = mc2). Similarly, you can't patent something that occurs in nature.

Further, patent infringement is solely a question of federal law, and an infringement action can only be undertaken on an issued patent. That means it may be a couple years before you can really stop someone else from using your idea.

If disclosure is not something you are comfortable with, keeping the idea as a trade secret may be a better option. Frankly, although patents are a perfectly good mechanism to protect your IP assets in some situations, there are just some things better left unsaid.

Trade secrets have the ability to last longer than patents. Not to mention, trade secrets are essentially free of charge. Coca-Cola's secret formula (and their secret ingredient, "Merchandise 7X") has been a highly guarded secret for over 125 years (although Coke's formula may have been recently revealed). If Coca-Cola had obtained a patent on the specific composition of ingredients when it was first developed, that patent would have expired in the early 1900's.

Seems like an easy solution, right? Keep everything as trade secrets. No attorney costs, no time wasted with patent offices, just take the idea, mark it "company proprietary" and only let certain people access it.

The problem with that tactic goes back to your visionary counsel's second question: Can someone figure out the idea *from* your product? If so, it really isn't much of a secret. And it is almost impossible to protect.

Although neither is perfect, a well-rounded IP protection program includes both patents and trade secrets More importantly, developing this program should keep someone ELSE up at night.

Seyfarth's patent and trade secret attorneys are here to help your company determine effective ways to manage and protect your IP asset portfolio, so you can have pleasant dreams instead of recurring nightmares.

Bad Practices for Interviewing Competitors' Employees and Dealing with Departing Employees

By Robert Milligan and Joshua Salinas (May 5, 2014)

California is a unique jurisdiction because of its public policy against certain employee noncompetition agreements and post-termination restrictions on employee mobility. This general prohibition against noncompetes with employees leaves trade secret laws as the primary mechanism for employers with California based employees to protect against the unlawful use or disclosure of valuable company information and related competitive issues when key employees join competitors.

Yet many employers fall short in protecting trade secrets through the inadequate handling of employee departures. Moreover, many companies fail to understand the potential liability that may arise with the unlawful acquisition of a competitor's trade secrets when interviewing and onboarding a competitor's employees.

In this first video of a two-part series, we illustrate some bad practices when interviewing a competitor's employees, as well as handling your own employees' departures, regarding the protection of trade secrets and other confidential information. During the video, a prospective candidate offers to share during his employment interview his current employer's trade secrets regarding sensitive business and customer information for the Southern California market.

When watching the video below, consider the following:

- What concerns do you have about anything the interviewer did?
- What concerns about what the prospective employee did?
- How about the current employer?
- What type of policies and procedures could both the current employer and prospective employer put in place to better protect themselves?

Trading Secrets

https://www.youtube.com/watch?v=97vrZ2N7wCY

The Interviewer

- Fails to steer the interview away from customer specifics and potential trade secrets toward the employee's general skills and knowledge
- Encourages the employee to start in a mere 4 days
- Tells the employee to "give a shout out to his customers"
- Does not press the employee for copies of his previous agreements
- Encourages the employee to solicit fellow employees

The Applicant

- Offers to announce his move to customers before leaving his old job
- Shares specific confidential information about customers
- Plans to leave his old job with little to no notice
- Announces that he will bring his old employer's materials along with him in order to "hit the ground running"
- Hopes to bring the "OC franchisor team" with him to his new job

- Takes company property, including hard copy, electronic files, and USB devices
- Encourages other employees to join him at competitor despite non-solicitation covenant
- Uses social media and cloud storage to transfer company data

The Applicant's Current Employer

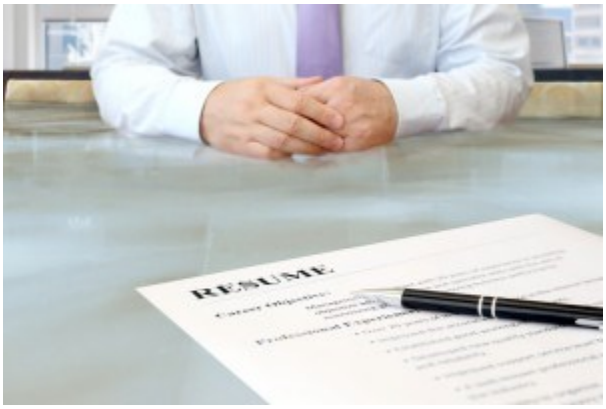
- Failed to create "culture of confidentiality"
- Allows employee to clean out office without HR present and take material without reviewing content
- Fails to conduct an exit interview
- Authorizes wiping of employee's computer which may destroy evidence that the employee forwarded files and customer contacts to his personal e-mail account
- Generally appears unconcerned about the abrupt and unexpected departure of an employee who had access to confidential and trade secret information

Stay tuned for part two of this series where we illustrate the best practices to protect company trade secrets when employees depart, and best practices for avoiding liability when interviewing and onboarding a competitor's employees.

Trading Secrets

Tips for Avoiding Liability for Trade Secret Misappropriation Concerning the Hiring and Departure of Employees

By Robert Milligan and Josh Salinas (May 9, 2014)



As companies face increasing competitive and financial pressures, management is understandably consumed with running the day-to-day operations of the business and working to achieve business objectives and maximize the bottom line. As a result, it is not uncommon for companies to find themselves in situations where important assets are overlooked or taken for granted. Yet, those same assets can be lost or compromised in a moment through what is often benign neglect.

Authoritative sources estimate that companies lose hundreds of millions of dollars (if not billions) as a result of trade secret theft. At the same time, companies sometimes find themselves, through poor controls, exposed when they inadvertently obtain others' trade secrets.

In the rush to deliver results, some companies take shortcuts in the hiring and departure process that often leave them exposed to claims for trade secret misappropriation, aiding and abetting breaches of loyalty, and intentional interference with contractual relationships or business expectancies with customers or employees.

California's strong public policy against certain employee noncompetition agreements and post-termination restrictions on employee mobility means strong trade secret protections are essential for California employers to protect against the unlawful use or disclosure of valuable company information and related competitive issues when key employees join competitors. Accordingly, while non-competes may be void in California, prudent companies conducting business in California will ensure that their trade secret protection practices are state of the art, including their onboarding and offboarding process.

In this second video of a two-part series (see part one here), we illustrate some best practices when interviewing a competitor's employees, as well as handling your own employees' departures, regarding the protection of trade secrets and other confidential information in California. During the video, a prospective candidate offers to share during his employment interview his current employer's trade secrets regarding sensitive business and customer information for the Southern California market. You will also see how the employer handles the exit interview of that employee.

When watching the video below, consider the following:

- How does the interviewer avoid the applicant's disclosure of trade secret and other confidential information and focus the candidate on general skills and knowledge?

- How does the prospective employer condition its offer of employment?
- How does the current employer try to protect its trade secret and other confidential information with departing employees?
- What type of policies and procedures do the current employer and prospective employer put in place to better protect themselves?

Click below to discover some of the best practices illustrated in the video and in general to protect trade secrets.

https://www.youtube.com/watch?v=_OZ4Z1h5n-Q

The Interviewer

- Discuss general skills and talents, not employer's customers or trade secrets
- Tells candidate to be careful not to reveal his employer's trade secrets or confidential information
- Controls the interview and puts the applicant at ease
- Encourages the applicant to give two weeks' notice to assist his employer with the transition
- Asks the applicant for all copies of his previous employment agreements, and indicates that the offer is contingent on a review of those agreements

- Consider putting in a position if hired where the employee will not reveal confidential or trade secret information
- Make clear that the applicant should not, under any circumstances, use or bring any of his former employer's property, including trade secret or confidential information, or solicit any former co-workers

The Applicant's Current Employer

- Conducts an exit interview
- Uses a checklist to ensure the employee returns all company property, including computer devices, hard copy documents, and online account passwords
- Disables employee's access to computer systems and networks
- Investigates prior to exit interview whether employee has taken, forwarded, or retains possession of any company documents or files and asks for the return of such information
- Reviews projects employee worked on to determine that all corresponding property has been returned
- Asks employee whether he worked at home and to make arrangements to coordinate the return of company property located on his personal computer devices
- Utilizes a written agreement with the employee to clarify the ownership and use of the company's social media accounts

Other Generalized Tips to Protect Trade Secrets in the Hiring, During Employment and the Departure Process

- Conduct new hire training on the importance of protecting your company's assets. Be sure to cover obvious topics, such as following computer access policies and your company's data encryption system, and less obvious topics, such as the possibility of accidental trade secret disclosure from holding business discussions in public places. Engrain a culture of protection of company assets through respect for confidentiality.
- Separate out trade secret agreements and training from the piles of paperwork and training that new employees receive so that they are not glossed over or disregarded as "just another piece of paper to sign."
- If the new employee's position at your company is going to be substantially similar to his or her previous position, consider initially assigning the employee to different projects. Also consider temporarily modifying the new employee's job responsibilities.
- Periodically review the new employee's work to confirm that he or she is not utilizing confidential and proprietary information belonging to previous employers. Monitor the employee's computer to ensure that confidential and proprietary information belonging to previous employers is not uploaded to company computers.

- Periodically follow up with all employees to ensure continued compliance with policies and agreements put in place to protect confidential information. Always emphasize the importance of protecting company trade secrets. Training employees solely at the new hire stage is not sufficient in the long run.

- Make sure you have an exit interview.

- Question the departing employee in detail about his or her new job, including identifying the new employer, position, duties, and responsibilities. Ask the employee why he or she is leaving. Question the employee on his or her access to company trade secrets during his or her employment. Question the employee on his or her possession of company property and his or her return of such property.

- Question the employee concerning any suspicious activities related to company property and computer access/ usage.

- Consider using an exit interview certification in which the departing employee acknowledges or certifies his or her understanding of his or her obligations. At the very least, provide the departing employee with a copy of his or her employment agreement. Inform the employee that the company expects departing employees to conform their conduct accordingly and instruct the employee to provide a copy of the agreement to his or her new employer.

Please check out this helpful practice guide for additional best practices to protect trade secrets during the onboarding and departure of employees.

Not Easy Being Green: Trade Secret Holders May Be Singing the Blues Over Green Chemistry

By Anthony Orler (May 14, 2014)

It isn't easy to change the mindset of a capitalistic society. Although the science of ecology dates back more than 150 years and has its roots in ancient Greece, society as a whole has only become more environmentally aware in the last 40 some years. It remains a struggle to make people aware that, really, we are not the only organisms on the planet. So let's start by making sure that we aren't using any secrets, including trade secrets, to contaminate our little place in the universe.

One of the latest efforts to minimize the effects of man on the world's diverse, delicate ecosystems is "Green Chemistry," which encourages products and processes that reduce use and generation of hazardous substances. To further the goals of Green Chemistry, the California "Safer Consumer Product (SCP) Regulations" became law October 1, 2013.

Sounds great, doesn't it? If a hydro-fluorocarbon (HFC) and a chlorofluorocarbon (CFC) can do the same job (*e.g.*, the air conditioning in your car), and HFCs do not destroy the ozone layer like CFCs do, why shouldn't the government force you to use HFCs? Unfortunately, implementing such change isn't as easy as a mere change in an acronym letter, and there are a few additional items in the rules that make full compliance, uh, uncomfortable.

One of the rules under the SCP is that there can be *no secrets* from the government. That means you must disclose your**trade secrets** in detail to the State of California. Don't worry, though, the government won't tell anyone your trade secrets. And there won't be any computer hacking or leaks either.

True, the SCP regulations have a process to protect trade secrets from public disclosure. It seems to be a "tell us your secret and hope for the best" approach, however.

If you have a trade secret that falls within the SCP regulations, you must first make a written claim to the Department of Toxic Substance Control (DTSC) that you have a trade secret. You tell the DTSC in writing exactly what your trade secret is and provide the DTSC evidence why it should remain a trade secret. The DTSC reviews your application and evidence and makes a ruling on your request.

If the DTSC decides — for whatever reason — that the information does not rise to the level of trade secret protection . . . they deny your request. If you disagree, you have to sue the State of California within 30 days of the denial to maintain the confidentiality of the information. If you don't file, the DTSC makes your trade secret information public.

If you do file a preliminary injunction or for declaratory relief to protect your information from disclosure, you have to disclose all of your trade secret information in court, but you are allowed to request

redaction of certain information. Redaction, schmedaction . . . there are *no rules* stating that the **court** must keep your information confidential.

Worse yet, at least 30 other states are considering similar regulations.

Disclosing your trade secrets may be necessary under California's SCP and similar laws around the country. The path to keeping your trade secrets confidential while becoming more ecologically sound just became a lot more difficult.

As a famous amphibian puppet says, "It's not easy being green."

Employees Strike Back Against Former Employer For Alleged Bogus Claim of Trade Secret Misappropriation

By Paul E. Freehling (June 3, 2014)

A state court issued a preliminary injunction for alleged trade secret misappropriation, but the enjoined parties successfully used post-injunction discovery to convince the court that the complaint was baseless. Those parties then filed a federal court lawsuit for abuse of process and other torts. In *Peek v. Whittaker*, Case No. 2:13-cv-01188 (W.D. Pa., May 22, 2014), the court held that most of the counts stated causes of action.

Summary of the Case

R.E. Whittaker Co. filed a complaint in a Pennsylvania state court against two ex-employees and their business partner, alleging that they were about to use misappropriated trade secrets to launch a business in competition with Whittaker. The court entered a preliminary injunction against the defendants. However, the court ultimately concluded that no evidence supported Whittaker's complaint and entered summary judgment for the defendants. Two of them then sued Whittaker in a Pennsylvania federal court. The majority of Whittaker's motion to dismiss the complaint was denied.

State Court Injunction

Whittaker sells commercial carpet cleaning machines and fluids. In 2008, it filed a 10-count complaint in a Pennsylvania Court of Common Pleas against ex-employee Offutt, another ex-employee, and their business partner Peek. Whittaker charged them with conspiracy to breach the ex-employees' covenants with the company and to misappropriate the company's trade secrets. The defendants' intent, according to Whittaker, was to use the purloined confidential information in competition with the company. Following a multi-day evidentiary hearing, the court preliminarily enjoined the defendants from engaging in any activity competitive with Whittaker. The injunction order was affirmed on appeal. Whittaker sent copies of the order to the defendants' potential customers and suppliers.

Post-Injunction Discovery

Discovery taken after the injunction order was entered disclosed that, contrary to Whittaker's witnesses' testimony at the injunction hearing, the defendants had misappropriated no Whittaker trade secrets. Stating that the record was "much different" from the one on the basis of which the preliminary injunction had been issued, and that Whittaker had failed to show trade secret misappropriation, breach of contract, or damages caused by the defendants, the injunction was vacated and Whittaker's complaint was tossed. Whittaker did not appeal.

Federal Court Litigation

Peek and Offutt sued Whittaker in federal court for abuse of process, unfair competition, false advertising, and other torts. The complaint alleged that Whittaker's state court complaint and preliminary injunction motion were filed for an improper purpose. Further, Peek and Offutt averred that false evidence was used to obtain the injunction. Whittaker's motion to dismiss the complaint was denied in most respects.

Takeaways

The federal court opinion teaches that suing and obtaining an injunction against ex-employees for trade secret misappropriation, without persuasive supporting evidence of their wrongdoing, can backfire. After more than five years of litigation, Whittaker has little to show for its efforts and expenditures, and it now is on the defensive in federal court. Before filing spurious litigation against ex-employees intended to head off their post-termination competition with the former employer, that company should consider the potential adverse consequences if the defendants have the will and financial resources to stay the course. In *Whittaker*, the ex-employees were knocked down, but they weren't knocked out.

Seyfarth Attorney to Present on Protecting Pharmaceutical Trade Secrets at the Chinese Biopharmaceutical Association's Annual Meeting

By Justin Beyer (June 19, 2014)

This Saturday, June 21, 2014, Seyfarth attorney Justin K. Beyer, will present at the 19th Annual Chinese Biopharmaceutical Association Conference on Legal Challenges in Trade Secret Protection, at the University of Maryland's Shady Grove Conference Center. Through this panel discussion, Mr. Beyer will offer insights into what constitutes a trade secret, trade secrets unique to the pharmaceutical industry, and best practices for protecting those trade secrets.

If you are attending the Chinese Biopharmaceutical Association's Annual Meeting, please be sure to stop by our table in the exhibition room.

Josh Salinas Explains How Drones Could Pose a Threat to the Protection of Trade Secrets

By Joshua Salinas (June 29, 2014)

https://www.youtube.com/watch?v=7TtQxKJ4Kps

The commercial and personal use of drones are becoming increasingly more prevalent. Indeed, there were allegations during the ongoing World Cup that a drone was purportedly used to spy on a team's practices by an opponent who was looking to gain a competitive advantage. Josh Salinas weighs in on the potential threat drones may pose to the protection of trade secrets.

Legal 500 Names Seyfarth Shaw as a Finalist for Top Trade Secrets Litigation Department in the U.S.

By Robert Milligan (July 1, 2014)

The 2014 edition of *The Legal 500 United States* recommends Seyfarth Shaw's Trade Secrets group as one of the best in the country.

Nationally, our Trade Secrets practice moved up one position from the 2013 rankings to Tier 2. In addition, *Legal 500* has launched its first-ever shortlist for U.S. awards, and we are very pleased to report that Seyfarth is one of five firms shortlisted for **2014 Law Firm Award for Trade Secrets Litigation**. We expect the award winner to be announced on Wednesday, July 2nd.

Based on feedback from corporate counsel, three Seyfarth partners were recommended in the editorial, and they include Michael D. Wexler, Robert B. Milligan, and Jason P. Stiehl.

The Legal 500 United States is an independent guide providing comprehensive coverage on legal services and is widely referenced for its definitive judgment of law firm capabilities. *The Legal 500 United States Awards 2014* is a new concept in recognizing and rewarding the best in-house and private practice teams and individuals over the past 12 months. The awards are given to the elite legal practitioners, based on comprehensive research into the U.S. legal market.

Texas Federal Court Imposes Ongoing Royalty Rather Than Permanent Injunction Against Alleged Trade Secret Misappropriator

By Shashank Upadhye (July 15, 2014)

A Texas federal trial court, finding the absence of any legal precedence to award an ongoing royalty in a trade secret misappropriation case, looked to the patent laws to impose an ongoing royalty. As a result, rather than permanently enjoining the misappropriator from continuing, the trial court imposed a royalty, thereby allowing the victim some compensation but allowing the other party to continue its activities. *Sabatino Bianco MD v. Globus Medical Inc.*, 2014 WL 2980740 (ED Tx. 02 July 2014)(docket no.: 2:12-cv-00147)

Summary of the Case

Dr. Bianco designed certain spinal implants. The jury ruled that Globus misappropriated Dr. Bianco's trade secrets and awarded damages. Dr. Bianco wanted disgorgement of Globus' profits, but the jury instead awarded Dr. Bianco a 5% royalty as back-payment for the taken secrets. Dr. Bianco asked for, but was denied, a permanent injunction. Instead, the district court asked the parties to come up with some figure for the ongoing royalty percentage, which the judge determined to be 5% also. The judge said that the payment period would extend for 15 years.

Dr. Bianco asked for more than 5% (he asked for 6%) and Globus said it wasn't going to pay anything in the future because the secrets were no longer secret and that the prior 5% back-payment was full compensation. Dr. Bianco said that the previous 5% was a floor and any new rate should necessarily be higher. Globus said that once the misappropriation was publicized and embodied in the actual spinal devices, nothing was a secret. Certainly there was no call for paying royalties over 15 years. Dr. Bianco asked for a higher rate to send warnings to other misappropriators that such behavior is not tolerated. The trial judge rejected both sides' proposals.

The Court's Rationales

First the court noted that in Texas, there is no state-based trade secret law covering the ongoing royalty situation. So the court unsurprisingly adopted patent law as the trial judge was in fact Judge William Bryson of the US Federal Circuit Court of Appeals, sitting in designation in Texas.

The court then noted that in Texas, injunctions can continue longer than the period after which a secret becomes public. The court also noted that any increase in the rate cannot be for punitive or willful theft purposes because Texas law does not allow for punitive forward looking remedies and that any punitives were included in the back-payment royalty rate.

Furthermore, the court reasoned that in Texas, trade secret theft is a one-time event, hence the proper calculation would be on what the parties would hypothetically negotiate on the one-time event. In patent law, though, each infringement is a continuing tort.

Finally, the court rejected Dr. Bianco's deterrent effect argument. The court noted that any deterrent effect is satisfied by the possibility that the court will not award any base damages or ongoing royalties but instead will order a full disgorgement.

Takeaways

This case teaches several aspects: (1) One should not assume that every trade secret theft can be remedied by automatic permanent injunction relief. Rather a court may allow the defendant to continue activities so long as it pays some royalty; (2) In your particular state, as here, there might be no case law precedent that sets the contours of the remedy, and hence, a court may borrow from another legal subject matter; (3) While we do not recommend any such action, this is an instance in which the misappropriation is allowed to continue, with a royalty payment. One could presume that there is still a significant financial benefit to the misappropriator in that it still makes money from its initial misappropriation; and (4) In the initial disclosure, though in confidence, of Dr. Bianco's information to Globus, would the result have been different if the disclosure documents included Globus Medical's agreement that it would be subject to permanent injunctive relief and disgorgement? Perhaps the disclosure documents could have included those statements.

$16 Million Awarded By Arbitrator Against 50 Cent in Trade Secret Spat

By Christina Jackson (July 16, 2014)

In a case out of Florida involving the rapper known as "50 Cent" an arbitrator found the rapper liable for trade secret misappropriation, among other claims, in the creation of his own line of headphones. The arbitrator awarded, the plaintiff in the case, Sleek Audio, LLC, a little over $11.5 million in damages. Attorney's fees were also awarded to Sleek and two other individual plaintiffs in the amount of nearly $4.5 million.

Summary of the Case

Curtis J. Jackson, III, (aka "50 Cent") had originally invested in a company known as Sleek Audio, LLC, to design a line of headphones. Jackson also became a member of Sleek's board. Sleek began creating a design for over-the-ear headphones known as "Sleek by 50." However, eventually Sleek and Jackson parted ways in 2011. Thereafter, Jackson collaborated with another company, of which he was a majority owner, SMS Audio, to create the headphones known as "Street by 50" and "Synch by 50." Jackson hired individuals to work on the SMS Audio headphones that had already had access to the design of Sleek's headphones.

Sleek then sued Jackson for misappropriation of trade secrets in relation to the headphone design of SMS Audio. Jackson brought claims against Sleek or fraud in the inducement to enter into a securities purchase agreement and operating agreement. The claims went to arbitration.

Comparing The Headphones

Ultimately the arbitrator found Jackson liable for misappropriation of trade secret claims, as well as other claims. As for the misappropriation claim, the arbitrator relied upon Sleek's expert testimony in comparing Sleek's headphones to SMS' headphones. The expert opined that the three sets of headphones "shared a multitude of mechanical design details" unlike those of other headphones. Moreover, since Sleek had not yet marketed its headphones to the public, the mechanical design was not "generally known" or "readily ascertainable" by others. The arbitrator thus found that these similarities as well as Sleek's internal company procedures for attempting to safeguard this information evidenced trade secret misappropriation.

Additionally, the arbitrator found that an employee of one of Jackson's company's had misappropriated trade secrets consisting of potential customer data on Sleek's webpage that had been password protected.

Inevitable Disclosure

Furthermore, the arbitrator, in relying upon Sleek's expert opinion, found that SMS' headphone design could not have been started in such a short period of time and be of such quality without having used Sleek's trade secrets. This finding was based upon Jackson hiring the individuals who, prior to working for SMS, had access to the design of Sleek's headphones.

Liability of Jackson

The arbitrator found Jackson was liable for the misappropriation of Sleek's trade secrets because of Jackson's role as a corporate officer of SMS. Under applicable case law, a corporate officer that "was aware of or ratified" use of "improperly obtained trade secrets" along with knowing (or should have known) they were "acquired by improper means" can be held personally liable. Here, the arbitrator found that the misappropriation of trade secrets by SMS employees combined with Jackson's awareness of the misappropriation was a sufficient basis for Jackson's liability.

Takeaways

This case highlights the need for entrepreneurs or businesses to be careful about who they hire and for what purpose. If a new hire or potential new hire has worked on a similar product for a competitor, caution should be applied in development of similar products. Perhaps the outcome in this case would have been different had Jackson hired individuals to design SMS' headphones who had not previously had access to Sleek's design information. Additionally, an officer of a company may be liable for an employee's misappropriation of trade secrets. This case serves as a reminder of the burdens an officer bears. Finally, in regard to litigation, as has been demonstrated time and again, a key expert can play a major and decisive role in the outcome of a case.

Preliminary Injunction Entered After Texas Federal Court Concludes That Ex-Employee "Inevitably" Will Disclose His Former Employer's Trade Secrets

By Paul Freehling (July 24, 2014)

An employee entered into non-compete and confidentiality agreements with his employer. Following his resignation from that company, he went to work for a competitor. His job functions and territory with both employers were similar. In a suit for violation of the non-compete and confidentiality agreements, a Texas federal court held recently that — absent an injunction — disclosure to his new employer of his former employer's confidential information was inevitable. The court concluded that all of the prerequisites were met for a preliminary injunction. *Brink's Inc. v. Patrick*, Case No. 3:14-cv-775-B (N.D. Tex., 6/26/14).

Summary of the Case

Greco was employed by Brink's, a provider of secure money transport services. Shortly before resigning from Brink's to go to work a competitor, he allegedly transferred confidential files from his Brink's office computer to his personal thumb drive and then deleted the files from the computer. Brink's sued him in a Texas state court, and he removed to the federal court. Brink's claimed that disclosure of its trade secrets was inevitable unless Greco was enjoined from competing with Brink's for the entire two-year term of the non-compete. The court granted the motion in part, limiting the scope of the covenant and enjoining Greco only while the litigation is pending.

Inevitable Disclosure

Injunctions based on the inevitable disclosure doctrine typically involve specialized and particularized information developed in the course of the former employer's R&D and used in that company's highly technical or complex workplace. Often, the new employer is a start-up, or a company planning a significant expansion, which would benefit — by not having to expend significant sums and effort on development — from the former employer's closely guarded, valuable trade secrets. In that situation, some judges will prohibit the newly hired employee from using or even inadvertently disclosing the secrets.

Other judges, however, express reluctance to invoke the inevitable disclosure doctrine, except in "the rarest of cases." For one thing, the more experienced the employee, and the more general the information disclosure of which is foreclosed, the harder it is for the parties and a court to differentiate between (a) knowledge gleaned simply from that experience, which the employee should be free to use, and (b) confidential information proprietary to the former employer. For another, an inevitable disclosure injunction might prevent the employee from providing meaningful services to a new employer in the industry in which the employee knows best. Those jurists maintain further that the inevitable disclosure doctrine adds little of substance to a non-compete if the employee agreed to one, but if there is none courts should not impose on the ex-employee a functionally equivalent substitute.

The injunction in the *Brink's* Case

Duration. The court declined to issue a two-year "preliminary injunction" as requested by Brink's because such an order would, in effect, grant 100% of the relief requested but at a time when the dispute's merits have not yet been adjudicated.

Geography. Greco objected to the request by Brink's to restrain him from working for a competitor located in Chicago. Although he had been employed in the Chicago office of Brink's, he maintained that the company's operations there were outside his responsibility for his final two years with that company. However, the non-competition covenant stated in relevant part that the territory covered includes the entire area served by the office where the employee was located at termination. So, Greco was ordered not to compete with Brink's in the territory serviced by its Chicago office, but he was not precluded from competing outside that region or providing non-competitive services within that area.

Inevitable disclosure. Brink's alleged that Greco was intimately familiar with its confidential "customer names, contacts, volume of business and routes for customers, service specifications, service delivery strategies, and staffing and pricing models." Agreeing with Brink's that the non-compete was necessary to protect the company's good will, the court concluded that Greco inevitably would cause irreparable harm by performing competitive services for Garda in the relevant territory. Most courts issuing an inevitable disclosure injunction would emphasize efforts the former employer made to protect the confidentiality of the trade secrets, a subject the *Brink's* court did not mention.

Takeaways

Greco was bound by both confidentiality and non-compete covenants. Any employer that wants to maximize protection of trade secrets should insist that high-level employees execute both. Whether the same result would have been reached in the absence of a non-compete, in other words, based solely on the inevitable disclosure doctrine, is unclear. The court's decision clearly was influenced by the near identity of Greco's job responsibilities with both employers and by his apparent misuse, as he was exiting, of the computer Brink's had provided to him. Attorneys representing employers seeking to enforce a confidentiality covenant should stress facts showing why misuse of trade secrets is particularly likely and that the trust placed in the ex-employee by the former employer was abused.

Eighth Circuit Affirms $31.1 Million Dollar Jury Verdict in Favor of Hallmark Cards over Private Equity Firm

By Timothy Hsieh (July 25, 2014)

In *Hallmark Cards Inc. v. Monitor Clipper Partners LLC et al*., 2014 WL 3409953 (8th Cir. July 15, 2014), the U.S. Court of Appeals for the Eighth Circuit affirmed a $31.3 million dollar jury verdict, which included $10 million in punitive damages, in favor of Hallmark Cards, Inc. ("Hallmark") against a private equity firm known as Monitor Clipper Partners LLC, which was found to have misappropriated confidential information from Hallmark, including data from Power Point presentations. Hallmark's Power Point presentations were also found to constitute trade secrets under the Missouri Uniform Trade Secrets Act (Mo. Rev. Stat. 417.450 et seq.).

Summary of the Case

Hallmark hired a Boston-based consulting company known as Monitor Company Group, L.P. ("Monitor") to compile research on the greeting cards market. Monitor then created several PowerPoint presentations to summarize its findings, and both Hallmark and Monitor signed confidentiality agreements to make the market research material confidential. Monitor then transmitted this confidential market research it had performed for Hallmark to another private equity firm known as Monitor Clipper Partners, LLC ("Clipper"). Clipper was a private equity firm founded by two of Monitor's original partners and was also located in the same office building. Furthermore, Clipper's primary investment strategy was to use Monitor's expertise in consulting various clients to understand specific fields or markets. Clipper then all of a sudden became interested in entering the greeting cards market, and used the confidential market research information prepared by Monitor to buy one of Hallmark's competitors known as Recycled Paper Greetings, Inc (RPG). Clipper also used data from at least five PowerPoint presentations prepared by Monitor to inform and finance its bid for RPG, which it won. After Clipper bought RPG, Hallmark began to suspect that Monitor had disclosed the confidential research on the greeting cards market to Clipper. After an arbitration which led to a settlement between Hallmark and Monitor of $16.6 million, Hallmark then filed suit against both Monitor (for breach of contract) and Clipper (for the theft of trade secrets in violation of the Missouri Uniform Trade Secrets Act) in the U.S. District Court for the Western District of Missouri. The jury in the trial court case awarded Hallmark both $21.3 million in compensatory damages and $10 million in punitive damages against Clipper. After the trial, Clipper moved for judgment as a matter of law and to amend the verdict. The district court denied both motions and Clipper appealed to the Eighth Circuit.

The Court's Rationale

The decision is essentially divided into the alleged trade secrets claim and the double recovery/punitive damages claim.

Alleged Trade Secrets

For the trade secrets claim, Clipper argued that Hallmark's PowerPoint presentations were not trade secrets under the Missouri Uniform Trade Secrets Act because (1) Hallmark had publicly disclosed one of the conclusions contained in the PowerPoint presentations, thereby destroying any claim that power point presentations were trade secrets, and (2) four years had elapsed between the time that the PowerPoint presentations were created and the time of alleged trade secret misappropriation: thus, such information was already stale and of no economic value when Clipper allegedly misappropriated it. The court concluded that the jury had sufficient evidence to find that Hallmark's PowerPoint presentations were trade secrets under the Missouri Uniform Trade Secrets Act. In response to (1), the court held that although Hallmark may have revealed one of the conclusions in the presentations, it did not reveal the underlying data supporting that conclusion or any methodology used to reach such a conclusion. In response to (2), the court held that information on the greeting card market was very limited even at the time of Clipper's alleged misappropriation (2005) and that this scarcity of data made even a four year old PowerPoint presentation valuable.

Double Recovery

Clipper also argued that the jury verdict in the district court case amounted to a double recovery for Hallmark because Hallmark had already settled a similar claim against Monitor for $16.6 million and after going to trial, was also awarded another $31.3 million in damages against Clipper. The court rejected this argument and held that the arbitration award and the trial award were two separate awards for two separate, independent injuries. Therefore, no reduction of the jury award was necessary, and punitive damages against Clipper were permissible under Missouri law as long as the defendant acted with reckless disregard for Hallmark's rights and the Due Process clause. Accordingly, the court affirmed the district court's denial of Clipper's motion for judgment as a matter of law and, alternatively, to amend the judgment. The court also affirmed the $31.3 million jury trial verdict.

Takeaways

As can be seen by this case, there can be large awards around the order of $31.3 million made in particularly egregious trade secret misappropriation cases, even for the theft of PowerPoint presentations. This serves as a reminder to potential trade secret thieves who may believe that such trade secret misappropriation may be all part of an aggressive but fair business strategy. Especially considering a market as competitive as the greeting card business, such damages may be viewed as appropriate in compensating parties harmed by trade secret misappropriation.

There Are Many Ways to Milk a Cow and Not All Are Protected Trade Secrets

By Sarah Izfar (July 29, 2014)

A consultant of a company entered into a consulting agreement with a competitor. The scope of his consultancy of the first company involved dairy-permeate processing systems and the second involved lactose-processing systems. The Court of Appeals of Minnesota found that these businesses were sufficiently distinct such that disclosure of information regarding one business would not violate the non-compete agreement prohibiting the disclosure of information regarding the other. The Court also drew a distinction between confidential information and trade secrets. *See RELCO, LLC v. A. Kent Keller*, No. A13–1633, 2014 WL 2921895 (Minn. Ct. App. June 30, 2014).

Background

Keller and RELCO entered into a consulting agreement in 2000 whereby Keller, an expert in designing and manufacturing systems and equipment for factories, would assist RELCO in establishing itself in the markets of both lactose-processing systems and dairy permeate-processing systems. The consulting agreement was accompanied by a non-compete and a non-disclosure agreement, prohibiting the disclosure of confidential information. Even though RELCO's business involved both dairy-permeate and lactose-processing systems, both the non-compete and non-disclosure agreements defined RELCO's business as limited to the business of dairy-permeate systems. The consulting agreement also came with an asset purchase agreement under which Keller would sell RELCO Whey Systems. The parties agreed that the dairy-permeate and lactose-processing systems were "two separate and distinct systems for processing milk by-products."

In late 2009, two employees left RELCO and went to work for Custom Fabricating and Repair, Inc. ("CFR"), which shortly thereafter created a wholly-owned subsidiary Cheese Systems, Inc. ("CSI"), a direct competitor to RELCO. In December 2010, Keller entered into a consulting agreement with CSI specifically on lactose-processing systems.

The Action

RELCO commenced suit, claiming, *inter alia*, misappropriation of trade secrets and confidential information and breach of contract.

In its misappropriation claim, RELCO first argued that Keller improperly shared information related to mass-balance sheets. The Court rejected the "conclusory" statements of RELCO and its expert and granted summary judgment in Keller's favor because RELCO submitted no evidence that the mass-balance sheets constituted protected trade secret information. In fact, RELCO had initially purchased the mass-data sheets from Keller. RELCO then argued that Keller misappropriated trade secrets by

disclosing Whey System's files. However, the Court found no evidence that Keller had disclosed the files that he retained.

In its breach of contract claim, RELCO argued that the non-compete agreement at issue was ambiguous such that the Court should look to the parties' intent. The Court rejected that argument and enforced the contract on its terms. Unfortunately for RELCO, the non-compete was limited to the business of dairy-permeate systems whereas Keller's consultancy with CSI related to lactose-processing systems. The Court declined to adopt a broader interpretation of "competitive" or "business" that would include lactose-processing systems.

RELCO also prohibited the disclosure of confidential information in its non-disclosure agreement with Keller. Although the Court recognized the principle that trade secrets and confidential information are not synonymous, it did not find any wrongful use of confidential information here. In RELCO's agreement with Keller, "confidential information" was also limited to that information which was related to RELCO's "business" of dairy-permeate systems. Thus, because Keller was not retained by CSI to work on dairy-permeate systems, he had not improperly disclosed confidential information by disclosing information about lactose-processing systems.

The Court, thus, affirmed the trial court's grant of summary judgment in favor of Keller on both RELCO's misappropriation of trade secrets and confidential information claim and its breach of contract claim.

Takeaways

Employers seeking to protect their competitive advantage should take care to craft broad non-compete agreements that are sufficiently tailored to their business. The express provisions in a non-disclosure and non-compete agreement matter. If the definition of information or business is limited, a court will not necessarily expand its meaning to include all types of information and competitive behavior, not included within the agreement.

Steps to Protect Trade Secrets in the Non-Profit Sector and Balance the Need for Transparency

By Andrew Masak (August 19, 2014)

Despite the altruistic nature of some non-profits, they too are entitled to trade secret protection. The American Red Cross, a venerable stalwart in the disaster relief sector, recently found itself in the precarious position of seeking trade secret protections in responding to a letter from the New York State Attorney General's office seeking information on how it spent Hurricane Sandy disaster relief donations after ProPublica, an independent news source, filed a public records request pursuant to New York's Freedom of Information Law (FOIL).

In response, and in a new development at the intersection of trade secrets and the non-profit industry, the American Red Cross requested an exception from FOIL disclosure under FOIL's trade secret exemption. Specifically, the Red Cross objected to the disclosure of what it deemed "highly proprietary and confidential…information relating to the American Red Cross's operational procedures and fundraising methodology" and "internal strategy" which included "detailed information about…internal and proprietary methodology and procedures for fundraising, confidential information about its internal operations, and confidential information that is not normally made publicly available both in regards to its response to Super Storm Sandy and disaster relief in general." Moreover, the American Red Cross alleged the disclosure of this information would cause economic harm because its competitors would be able to replicate its "business model" to their competitive advantage.

The Attorney General of New York agreed, finding the information proprietary trade secrets and citing case law in support. *See Matter of Physicians Comm. For Responsible Medicine v. Hogan,* 29 Misc. 3d 1220 (A) (Sup. Albany 2010). Specifically, the Attorney General's office withheld portions of the documents that "describe business strategies, internal operational procedures and decisions, and the internal deliberations and decision-making processes that affect fundraising and the allocation of donations" finding "that this information is proprietary and constitutes trade secrets, and that its disclosure would cause the Red Cross economic injury and put the Red Cross at an economic disadvantage."

While the American Red Cross's seeking trade secret protection has caused some attention in the blogosphere, it highlights a major tension for non-profits: balancing the need to protect trade secrets with the constant pressure of transparency. Non-profits thrive on the money raised by donors and thus donor lists – an apt analogy as to customer lists – as well as the potentially complex machinery that maintains and generates these funds are essential. Indeed, charities and non-profits should be aware of and take measures to proactively protect potential trade secrets in the unfortunate event they are hauled into court or required to respond to requests like the FOIL request made by ProPublica.

Some steps non-profits should consider are:

1. **Identify and consistently label trade secrets** – for example, label documents with this type of information "Confidential – Unauthorized Disclosure Prohibited."

2. **When possible use Confidentiality and Non-Disclosure Agreements with employees**

3. **Use technology wisely** – keep truly confidential information on select protected computers

4. **Limit the third-party disclosure of information**

But non-profits should be forewarned before rushing to protect potential trade secrets. The growing trend in the non-profit industry is more transparency, not less. Both government agencies and the public demand a greater picture of where money is allocated, the effectiveness of programs and services, and an accounting of executive and staff expenses. In fact, one organization, GuideStar, widely regarded as the industry leader in monitoring non-profit transparency, published a helpful list of suggestions as part of its 2009 report "The State of Non-Profit Transparency, 2008: Voluntary Disclosure Practices" which, combined with the steps outlined above on trade secret protection, should help organizations in this unique balancing act:

1. **Regularly update the organization's web presence with current, detailed programs and evaluation information, including general strategy and evidence-based evaluation metrics.**

2. **Post board, staff, and associate names, titles, job functions, and credentials.**

3. **Post the organization's annual report.**

4. **Post audited financial statements.**

5. **Post the organization's IRS letter of determination.**

Notwithstanding the FOIL decision, the American Red Cross recently revealed additional details regarding its spending for Super Storm Sandy to ProPublica.

Trade Secret Mediation: Advice from a Mediator's Perspective

By Guest Author Erica Bristol (September 3, 2014)

As a special feature of our blog – special guest postings by experts, clients, and other professionals – please enjoy this blog entry on mediation of trade secret cases by mediator Erica Bristol, Principal of EB Resolution Services.

-Robert Milligan, Editor of Trading Secrets

Trade secret litigation often involves deep levels of distrust, heated emotional exchanges, suspicion and anger on the part of parties and counsel. One source of the problem lies at the heart of a trade secret misappropriation claim: the allegation that a "theft" has occurred, and each party's perception of the other party resulting from that allegation. The plaintiff alleges its property has been stolen by the defendant. If the plaintiff desires to avoid the time and expense of trial, the victim must now negotiate with the thief, adding insult to injury. The defendant, on the other hand, may express outrage at being accused of theft, and suspect the litigation is merely a fishing expedition by the plaintiff to uncover the defendant's own trade secrets.

The allegation of theft sets the parties on a difficult path from the very outset, which can affect the likelihood of reaching a settlement during the mediation session. How then, can the parties overcome these issues and reach agreement during mediation? The following tips may be helpful when mediating trade secret disputes.

Know the Definition of "Trade Secret" in the Relevant Jurisdiction. Counsel sometimes approach trade secret mediation with an incorrect definition of what a "trade secret" is within the relevant jurisdiction. One example is the "customer list." Plaintiff's counsel will sometimes argue that customer names and addresses, without more, are sufficient for trade secret protection. However, courts have held that certain customer information, such as names of contact persons that can easily be obtained by a phone call and addresses that are obtainable via the internet and directories, is not a trade secret. Defense counsel may take the position that customer names and information are not trade secrets, without making sure the information is easily obtainable, in the public domain or otherwise qualifies as a trade secret. The lack of a clear definition can lead to disputes as to the level of protection afforded. Counsel should review trade secret statutes and cases within the relevant jurisdiction to determine the proper definition of "trade secret" and advise the mediator if the issue is disputed, so that it may be addressed during the mediation (and so that counsel does not argue an unsupportable position to the detriment of the client).

Respond to Communications From Opposing Counsel. Very often an overlooked or delayed response to an email, the failure to return a phone call or a rude comment may be interpreted by opposing counsel as a sign of disrespect, which can fan the flames in an already heated situation and affect a party's willingness to settle. Resist the temptation to lobby a rude or disrespectful comment in response to one received from opposing counsel. Promptly respond to communications in a

professional manner to reduce the chance of misunderstandings, and to keep the channels of communication open.

Try to Develop Some Level of Trust and Cooperation, If At All Possible. Trade secret mediations often turn on the level of trust and cooperation between the parties. It is extremely helpful to establish an agreement that the parties will act in good faith during the mediation session. If Plaintiff's counsel has any suspicion the defendant is playing "hide the ball," or defendant's counsel feels plaintiff is seeking to engage in a fishing expedition, it will be difficult to obtain concessions from a party or reach settlement. The more open, honest, transparent and authentic each party is (or each party *appears to be*), the less contentious the mediation will be and the more likely a settlement can be reached. Even if the parties cannot develop a level of trust, it is helpful to reach some basic level of cooperation to assist in reaching settlement.

Conduct a Thorough Investigation The First Time Around. Counsel (both in-house and outside law firm) who do not have experience with trade secret disputes or who are not familiar with the internal workings of computer software, networks, IT departments and staff, should promptly seek the advice of trade secret counsel or a consultant. This will help to ensure that employees and contractors are properly instructed on how to search internal systems/networks; to conduct successful witness interviews by asking the right questions; to ensure the investigation is complete so there are no surprises later on; and to avoid spoliation of evidence. An incomplete or faulty investigation, especially if discovered during the mediation, may raise suspicions and require the session to be suspended so that a supplemental investigation can be performed, resulting in increased time, expense and frustration for all involved.

Accept That You May Never Get all the Answers. Trade secret cases often involve a substantive investigation into a party's computers, networks, systems and personnel to discover if trade secrets have been wrongfully misappropriated. Depending on the manner in which systems and software are configured, whether company policies are/were in place and the availability and reliability of witnesses, it may not be possible to develop a full picture of whether misappropriation has actually occurred. There usually comes a time when counsel and client must accept this fact, and decisions must be made based on the information available at that moment. It may not be worth the effort and expense to continue an investigation or conduct additional discovery. The difficulty is knowing when to "stop," and convincing the client to do the same. Emotions and distrust may impede a party's ability to think clearly and make a rational decision on the matter, but it must be done, especially when it is in the best interest of the client to reach a settlement during the mediation session.

Make Sure Expert Reports are Easy to Understand. Sometimes a party will introduce an expert's forensic computer report during the mediation for the participants to review. Reports such as these are extremely helpful in determining what information resided in the defendant's computer system, and whether that information constituted plaintiff's trade secrets. On occasion, the expert's report is such a maze of jumbled, unintelligible graphs, charts, data and technical speak that it requires an instructional manual. Explaining difficult reports during mediation can waste precious time that could be better used for settlement discussions. Counsel should make sure the graphs, charts, legends and data in expert reports are clear and easy to understand; the explanatory text is written in layman's terms, not industry speak; and the results and implications are clear. Simple expert reports will minimize the time spent reviewing and explaining the report, and maximize the time spent on negotiating settlement terms.

Parties to a trade secret dispute may experience distrust, incomplete information and a lack of communication and cooperation. This can set the tone of the mediation session, impede the parties' willingness to cooperate and reduce the likelihood of reaching settlement. Overcoming these obstacles can be an uphill battle for the parties and the mediator. These obstacles can be overcome by working through, *and in spite of*, a lack of trust and incomplete information; finding areas of cooperation and

trust; keeping the lines of communication open; and working in the client's best interest to resolve the dispute so that the client can get "back to business." Counsel and clients must commit to the process in order to overcome the barriers to settlement and achieve success in trade secret mediation.

_____

Erica Bristol is an intellectual property attorney and mediator. She is the Principal of EB Resolution Services, a mediation service provider in Encino, California, specializing in Intellectual Property law disputes.

Today's Connected Employee: A License to Steal

By Guest Author Trent Livingston (September 25, 2014)

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 Trent Livingston, a Director of iDiscovery Solutions.

Do you recall the early days of the spy movie genre? Many of these movies depicted cloaked secret agents slinking around dark offices snapping pictures of evil plots to take over the world with their tiny spy cameras. Now a tiny spy camera is a bit passé given that every smartphone worth its salt makes this a standard feature. What is scary though is that camera is part of a digital storage device that can hold gigabytes of data, which coincidently, is connected to what we now commonly refer to as "the Cloud".

Companies may not be plotting to take over the world, but one can be sure there is data within corporate walls that ownership wants kept under wraps. Does that mean everyone out there with a smartphone is stealing company secrets? The statistics are a bit unnerving. And a connected smart device is literally a mechanism that puts the ability to mastermind digital theft at one's fingertips.

The Evolution of IP Theft

A five year old study conducted in 2009 by Ponemon Institute documented that when employees were dismissed, or voluntarily left their employer, more than 59% reported that they kept company data. Of the individuals surveyed, 61% reported to have taken it in the form of paper documents or hard files, 53% used CD or DVD media, 42% used media such as hard drive or USB memory stick, and 38% sent documents as attachments to a personal email account.

Fast forward to 2014 and bring your own device ("BYOD") policies have introduced an entirely new way to pilfer corporate information. It may be as simple as a contact list, or as complex as source code for a new software release. The issue is, when it comes to Cloud connectivity, a corporation may never know a theft of this type has happened until it is too late. Given that the total losses attributed to IP theft of all types are in the hundreds of billions of dollars annually, it is not something to ignore.

With the advent of Web 2.0, new ways to share files have emerged in the last half decade that were not as prevalent in 2009 when the Ponemon survey was conducted. Google and many others introduced their enterprise web applications in 2009, and cloud computing began to hit its stride. Portable media like the CD and DVD have essentially become obsolete with increased bandwidth allowing large files gigabytes in size to be transferred in the time it takes to create one CD that can only warehouse a fraction of the same data.

While emailing information to personal email accounts is a likely suspect in intellectual property theft, data can leave an organization through a myriad of communication channels, including Social Media. Currently 74% of all adults use some form of social networking website or application. Essentially this means that 3 out of every 4 employees within any organization are using some form of Social Media to

communicate. Of these individuals, 69% of them that are Facebook users say they visit the site at least once or more daily.

Social Media provides a means to obfuscate data theft, essentially allowing a perpetrator to abscond with information outside of the company's firewall. Social networking applications such as LinkedIn, Facebook, and Twitter all have means of private communication. Access to these accounts is easy with any type of mobile device capable of running a social application.

File sharing applications are also mobile. With a quick click, and attachment saved from a corporate email account can be uploaded from anywhere to the likes of Box.net or Dropbox. These applications serve both the corporate and personal markets, which means distinguishing access to a personal or corporate account using corporate IT based IP address blocking solutions can become quickly limited.

Takeaways

Given that mobile devices serve a dual purpose for both the employee and employer under a BYOD policy, social and file sharing applications are integrated into the everyday corporate environment without second thought to their destructive capability. It is important to set up controls and company guidelines that specifically address employee usage of both social and file sharing web services. While direct monitoring of these types of personal accounts is not permitted, a departing employee's ability to access sensitive company information should be quickly locked down. Without the proper controls in place, corporations are open to rampant IP theft should an employee have the desire to commit such an act.

Trent Livingston is a digital forensics expert who has given testimony in numerous cases involving topics such as evidence preservation, documentation of events, and computer forensic methodologies. Mr. Livingston 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. Livingston can be contacted at tlivingston@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.

When "The End" Is Not "The End": Asserting Trade Secret Claims After The Execution of a Mutual Release

By Eric Barton (October 3, 2014)

In many cases, the execution of a mutual release is often the last step in resolving a trade secret or non-compete case. Typically included in the release is an affirmation that all confidential information has been returned and the once former adversaries promise not to sue one another. Once the release is executed, the fight is usually over. Usually, but not always.

The recent opinion of *EarthCam, Inc. v. OxBlue Corp.*, 1:11-CV-2278-WSD, 2014 WL 793522 (N.D. Ga. Feb. 26, 2014), addresses an uncommon situation where a former employer filed suit against one of its former employees for allegedly violating the terms of his non-compete agreement; notwithstanding the fact that the former employer and employee had previously executed a general mutual release wherein both sides agreed to release one another from any and all claims concerning the former employee's non-compete agreement.

In response to the company's complaint, the former employee filed a motion for Rule 11 sanctions on the grounds that the claims were allegedly barred by the executed general release. The former employer contended that it had a good faith basis for believing that the release was obtained through fraud and that, accordingly, it was void. Specifically, the company alleged that the former employee fraudulently affirmed that he had returned all of the company's tools and materials, when in fact, he was now using these items to compete against the company.

The court noted that, in Georgia, to void a contract based upon fraud in the inducement, the party seeking the relief must prove five elements: (1) a false representation or concealment of a material fact; (2) that the defendant knew the representations or concealment were false; (3) an intent to induce the allegedly defrauded party to act or refrain from acting; (4) justifiable reliance by the plaintiff; and (5) damages as a result of the false representations or concealment.

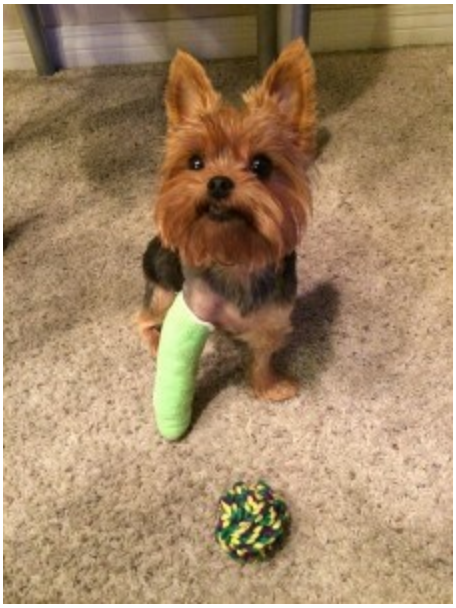
With this standard in mind, Judge William S. Duffey, Jr. held that "what matters here is not whether the fraud actually occurred, but whether [the company] has a colorable argument that the fraud *might* have occurred. If that is the case, then [the company] does not violate Rule 11 by asserting that the Release is void, allowing it to assert claims against [the former employee]." (Emphasis in original.) The court then examined the company's allegations of fraudulent inducement and stated that the "allegations are sufficient, albeit barely, to form a basis for the conclusion that some fraudulent inducement occurred. [The Company's] assertion that the Release is voidable is thus at least arguably credible, and there is an insufficient basis for imposing Rule 11 sanctions."

Takeaways

A general release does not automatically bar all future litigation between signatories if one of the parties subsequently discovers evidence enabling them to argue that the release should be voided based upon fraud in the inducement. While the standard for establishing fraud in the inducement is certainly high, asserting a colorable argument to survive a motion for sanctions is much lower. If you seek to assert such a claim, it is critical to plead all predicate elements or you run the risk of having your claim summarily dismissed, as well as being sanctioned.

High Times in Trade Secrets

By Anthony Orler (October 7, 2014)



(*N.B.*: *Neither the author, this article, nor this blog intends to make, nor makes, any comments for or against the legalization of marijuana in any jurisdiction*.)

What happens when you mix animal affection with a political issue? A Constitutional Convention? Tax dollars for pet shelters? Would you believe…trade secret litigation?

People love their pets. There are doggie day spas, specialty cat foods, and pet therapists.

Legalization of marijuana is a highly controversial political issue. Twenty-three states have already passed some form of marijuana decriminalization law. Colorado and Washington have essentially made cannabis as legal as alcohol for people over twenty-one. At least fourteen additional states are considering laws that reduce or eliminate criminal penalties related to marijuana. Although still illegal under federal law, the main argument for state legalization is, typically, additional tax revenue. Additional taxes usually means…additional profits for entrepreneurs, and people suing each other to see who gets those additional profits.

Thus, a lawsuit seeking an injunction and damages for "willful and malicious misappropriation of trade secrets" has been filed in Washington State (King County). The underlying subject matter of the case: cannabis-based health products for pets.

The plaintiffs, veterinarians Sarah Brandon and Greg Copas, claim they performed fifteen years of research and development on their trade secret cannabis-based formulas. These formulas were allegedly used to treat defendant Dan Goldfarb's pet in 2013. Washington legalized marijuana in December of 2012. Perhaps there was experimental use of the products going on prior to the laws being enacted? You do the math.

Goldfarb was apparently so pleased with his pet's recovery that he and the plaintiffs met regarding a possible business venture involving the development of pet health products using – what else – marijuana. The three formed Canna-Pet to manufacture and sell cannabis- and hemp-based pills, powder, and "canna-biscuit" products.

To keep people from stealing their pets' stash or getting their pets in trouble with the law, because, let's face it, Fido has enough anxiety already, the defendant's website assures potential customers that "your pet will not get 'high' or in trouble with the law" from their products. Since this stuff won't get Polly stoned, apparently your parrot cannot be arrested. And if your pet isn't receiving any of the typical benefits of this particular drug, what effect does the medication have, exactly?

As with many other agreements of this sort, the drug deal went bad. Goldfarb kept the Canna-Pet brand, while the plaintiffs formed Canna Companion to sell competing products using their proprietary formulas.

Trading Secrets

Goldfarb licensed the Canna-Pet technology to Cannabis Therapy Corp. in August 2014. The licensing agreement allegedly allows Cannabis Therapy to produce and sell cannabis-based pet products based on the plaintiffs' trade secrets.

It seems inevitable that the human affection for animals and the politics of pot would combine to produce pet products containing marijuana. It also seems logical that each different type of plant can be best cultivated using different, perhaps secret, techniques. Secret formulas and processes cover other goods and materials, why not the proprietary reefer concoction in Spot's evening treat?

What are these mysterious secrets that provide amazing health benefits to our animal friends? Would it be proper to ask a judge to recuse themselves if they had never inhaled? Who would be considered a qualified (or unqualified) juror in this action? Will pets have to testify to the restorative powers of these products? Will there be a smoke-filled jury room determining the culpability of the defendants? Or is this just a case of smoke and mirrors? Would it be fitting if the verdict was read at 4:20?

Trade secrets, even those involving controversial goods and services, are part of almost every business. It can be as little as a dog biscuit or as big as a jetliner. Regardless of the underlying subject matter, trade secrets often provide a competitive edge for any company.

In this particular trade secret case, the stakes may be extremely "high."

Trade Secret Attorneys Discuss Latest Issues in Trade Secret Litigation in *Corporate Disputes Magazine*

By Robert Milligan and Michael Wexler (October 13, 2014)

On October 1, 2014, Michael D. Wexler and Robert B. Milligan, partners and co-chairs of Seyfarth Shaw's Trade Secrets, Computer Fraud & Non-Competes practice group, participated in a Q&A mini-roundtable from *Corporate Disputes Magazine* on current trends in trade secret disputes and the steps companies can take to reduce these disputes. Below are fielded questions from the Seyfarth Shaw Reprint of Corporate Disputes Magazine, OCT-DEC Issue. We hope you find this informative.

CD: Could you provide a brief snapshot of current trends in trade secret disputes? Do companies need to be more aware of the potential risks in this area?

Milligan: Data theft of valuable company trade secrets through the use of portable electronic storage devices is occurring more and more, as is theft through cloud storage. We are also seeing an increase in more sophisticated hacking of company networks to obtain proprietary data by organised crime and foreign companies or states. Technological tools and employee use of personal mobile devices such as smartphones and tablets have given rise to a parallel trend of employers allowing – or requiring – their employees to use their own personal mobile devices at work. This 'Bring Your Own Device' (BYOD) movement can provide benefits to employees and employers, such as convenience, greater flexibility and productivity, as well as cost savings. However, BYOD programs can also create risks for employers. Companies need to be aware of potential data security issues, BYOD policies in a unionised workforce, employee privacy concerns and intellectual property issues. Moreover, the recovery of stolen information and workplace investigations can be hampered by employee-owned devices, not to mention challenges in litigation when trying to gain access to such devices where privacy considerations are often leveraged. Additionally, attacks on reasonable secrecy measures – part of the definition of a trade secret – is also on the rise: one court recently ruled that password protection alone was not enough to demonstrate reasonable secrecy measures.

Wexler: Further, like the EU, the United States is considering enhancing trade secret protections through additions to its laws. There are two bills pending in the United States Congress to create a civil cause of action for trade secret misappropriation in federal court. If passed, the legislation would provide companies with an additional forum and remedy to combat trade secret theft. With the increasing accessibility of data from a variety of electronic devices and threats by insiders and outsiders, companies also need to be more aware of potential risks to their data and ensure that they have appropriate policies and agreements in place with employees, vendors and business partners, as well as top of the class data security protections.

CD: How severe is the threat of losing trade secrets to a departing employee or departing executive? What are some of the common scenarios in which trade secrets can be compromised in this manner? Does the threat level change depending on the size of the company – small cap, mid cap, Fortune 50?

Wexler: The threat of losing trade secrets to a departing employee is real and not a matter of if, but when. Prudent companies will make sure that they have appropriate processes in place to address the threat when it occurs. As today's businesses meet the challenges of intensifying global competition, a more volatile workforce and information being transmitted at an unprecedented speed, they also face a greater risk of losing their valuable proprietary information to theft, inadvertent disclosure or coordinated employee departures. At a minimum, failure to take both proactive and immediate reactive measures could result in significant loss of profitability and erosion of an established employee and customer base. The threat of losing trade secrets to a departing employee or executive is enhanced if you don't have appropriate policies and agreements in place to prevent such theft or hold employees accountable for their unlawful conduct. And it can happen so easily and rapidly: one thumb drive can carry millions of pages of proprietary information and company information transferred to a personal email account or in a personal cloud all pose means for theft.

Milligan: Just look at recent headlines involving some of the world's largest companies who have seen their proprietary information compromised by insiders and outsiders. The crown jewels of many companies are at risk, and millions of dollars are in play. Lack of market secrecy measures, sloppy practices including poor supply side protections, lack of employee education and stale agreements and policies, poor security and different standards for executives who say one thing and do another are all common scenarios that put a company at risk. Common scenarios in which trade secrets can be compromised include letting an employee take company data when he or she leaves. Another red flag scenario is not utilising non-compete or nondisclosure agreements. There can also be scenarios where the particular industry is highly competitive and competitors are willing to take the enhanced risks to acquire the business or technology. In such scenarios, companies need to make sure they have in place appropriate onboarding and off-boarding practices and procedures, and use the appropriate agreements so they are not exposed. In our experience, the threat level does not necessarily change depending on the size of the company, but the magnitude of harm may increase. The larger the company, the more information to protect and the more employees and third parties to regulate and police. But small and mid-cap companies have similar concerns because they oftentimes have innovative technology that competitors or other third parties want, so these companies can also be vulnerable.

CD: What steps can companies take during the hiring process to reduce the threat that it may later be sued for trade secret misappropriation – particularly executives or those employees with higher level access to sensitive IP assets?

Milligan: Companies need to have a thoughtful, proactive process in place when hiring employees from competitors that is calculated to ensure that new employees do not violate their lawful agreements with their former employers, including using or disclosing their former employers' trade secrets, and retaining any of their former employers' property. It is important to regulate who interviews the job candidate and evaluate the candidate's non-compete or confidentiality agreement. Advise company personnel who are interviewing the candidate not to ask about a competitor's confidential information during the hiring process. Focus the interview on the recruit's general skills and experience in the industry. It's also important not to disclose company trade secrets to the candidate – be careful of the access permitted to the candidate. Candidates for employment should sign certifications that they will not disclose any trade secrets of their current employer. Additionally, make sure you analyse a recruit's agreements in advance of an offer being made. Should the candidate accept an offer, provide clear instructions to the employee that you don't want the former employer's trade secrets or property and

use agreements with the employee documenting the same. There are unique issues surrounding the retention and departure of high-level executives, particularly related to non-compete and trade secret issues. Since businesses can become targets of trade secret-related lawsuits if they hire executives and senior management who have worked at a competitor and misappropriate trade secrets or otherwise violate their restrictive covenants, it's important for companies to conduct due diligence on prospective employees and make sure that they have thoughtful plan in place before bringing on any high risk hires.

Wexler: Simple steps such as retaining hard drives when an employee leaves and inspecting computers, devices, cloud storage, and e-mail accounts can alert an employer to theft of information. More sophisticated methods such as forensic exam and monitoring software can also detect theft. Most of all, create a culture in which recruits and new employees are told 'we do not want anything from your prior employer'. Some additional best practice considerations follow below. Do not allow a recruit to do any work for your company until he or she has left his or her prior employer. Assist the employee in announcing the change in employment upon commencement of employment as appropriate. Focus on making the transition as smooth as possible for the current employer and encourage the departing employee to give proper notice and work out a mutually agreeable transition schedule with his or her current employer. With respect to the employee's new position, don't put the employee in a position in the company where he or she will necessarily need to reveal trade secrets. Finally, HR personnel needs to follow up with the employee to make sure that she is following her agreements and not pushing the envelope, and also follow up with managers to make sure the employee is doing the same.

CD: In what ways is the technology now available to employees changing the playing field in terms of loss or theft of trade secrets?

Milligan: The constant evolution of technology, particularly in mobile devices, data storage and security, and social media, has created legal challenges for companies and the playing field has changed tremendously. Portable electronic storage devices, online data storage and personal email are available to employees for nominal to no expense and can provide the means to trade secret theft. Additionally, business leaders often want data and information immediately and often want to make it accessible to various constituents, but companies don't necessarily keep up with the latest security in protecting such data. Companies need to stay on top of technology, including the latest in data storage and security and storage devices. Hacking of computers and mobile devices is more of a concern these days, and more mobility for employees also means more potential security issues for companies. Companies also need to stay on top of social media. Given its rapid and somewhat haphazard growth, social media carries with it a set of issues that traditional avenues of trade secret disclosure do not. For instance, unlike the departing employee who knowingly takes with him a box of documents, the relaxed and non-professional environment of social media sites could lead to employees disclosing confidential information without even realising they are doing so. Exposure of confidential company information and employee privacy rights are all issues that companies are now struggling with.

Wexler: Social media privacy legislation has become increasingly common in the United States and often impacts trade secret investigations. Issues related to social media privacy in the workplace are not going away and we expect to see more disputes 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 to adopt 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 trade secrets and restrictive covenant lawsuits, but make sure that their company's review and access of such information does not violate applicable law.

CD: How can companies avoid trade secret misappropriation and what should they do if they suspect misappropriation has occurred? What forensic investigation options might be available?

Wexler: Apart from civil liability, the Economic Espionage Act makes it a federal crime to steal trade secrets, and companies can be liable if they hire employees who misappropriate trade secrets for their new employers' benefit. Make sure your executives know the importance of playing by the rules. Employers can best avoid trade secret misappropriation with solid hiring practices and strong off-boarding procedures which are calculated to protect trade secrets and honour lawful agreements, coupled with effective ongoing employee training on trade secret protection and fair competition. Protecting your company information is critical to avoid trade secret misappropriation, and companies should work with their outside counsel to create solid policies and agreements, and solutions for onboarding to avoid exposure on restrictive covenants and trade secrets. It's also crucial to know your business partners, and have them vetted, so that they don't expose your valuable trade secrets. Critical to any trade secret matter is the thorough investigation of what, if any, wrongdoing occurred. Companies should work with legal counsel who is experienced in conducting such investigations. Comprehensive interviews and a review of relevant files, emails and workspaces are often the starting points of a competent investigation.

Milligan: We also regularly collaborate with forensic experts and computer specialists to find out how secrets were taken, and by whom, and to preserve any evidence necessary to future litigation. It is important to preserve data, review emails and talk to relevant witnesses to interpret the forensic data. A digital forensics examination often includes collecting and analysing artefacts from the operating system, internet history, and unallocated space. Routine e-discovery does not typically delve into questions about the source computer or storage device and ESI, although e-discovery may uncover the need to ask questions related to internet history, webmail, cloud storage, mobile devices and phone back-ups, and removable devices.

CD: How should companies interact with criminal prosecutors and federal/state law enforcement to complement civil claims for trade secret misappropriation?

Milligan: Private companies can investigate misappropriation claims and provide information to authorities for purposes of prosecuting Economic Espionage Act or Computer Fraud & Abuse Act claims as well as similar state criminal laws, but businesses need to be aware of two important points. First, allowing law enforcement access to the business can be a double edged sword creating interference with operations and disclosure of more information than the business may want. Second, when conducting an investigation, be certain to follow accepted forensic practices and chains of custody in collecting information. In sum, ensure that you have your house in order so you don't become the target of an investigation. When considering criminal prosecutions, always be cognizant of the ethical rule required of attorneys that generally prohibits threatening or initiating criminal proceedings to gain an advantage in a civil proceeding. Consultation with criminal authorities should be done in secrecy and ideally by non-attorneys so as not to run afoul of ethical rules. However, note an attorney can have contact with authorities; it is not prohibited in and of itself.

Wexler: It should also be noted that criminal prosecutors may make a request regarding the secrecy of the investigation or to hold off taking certain actions in the civil matter — or pursing the case altogether while the criminal case is ongoing — as they are focused on the criminal matter whereas a company and its counsel may be focused on the civil matter and damages. These differing interests can collide at times, so coordination is key. No private right of action exists yet under the Economic Espionage Act. The US Senate and House are currently considering legislation on this issue.

To view the full Article, click here.

Pythagoras and the Geometry of Intellectual Property: Where Do Trade Secrets Fit In?

By Anthony Orler (October 16, 2014)

Most people stop taking math in high school. Geometry was often the culprit that either made someone enjoy solving problems involving Greek letters or become completely disinterested. All those arcs and triangles…how does any of that apply to life as an attorney?

Well, here comes another geometry lesson: the Venn Diagram of intellectual property (IP), once thought to have only a minimal intersection between patents and trade secrets, may now include copyrights, and possibly trademarks, as protectable through trade secret law.

Where did *this* new math come from?

The California Court of Appeal, in Altavion, Inc. v. Konica Minolta Systems Laboratory Inc., held that *ideas* can be protectable as trade secrets.

Contrary to the Court's opinion in *Altavion*, patents do NOT protect "ideas." Patentable subject matter is limited to: new and useful processes, machines, articles of manufacture, or composition of matter, or any new and useful improvements thereof. Abstract ideas are specifically **excluded** from patent protection.

Lexicography aside, the Court of Appeal relied, at least in part, on the definition of a trade secret as "information" to determine if an idea (whatever the court meant by "idea") can be protected.

The Uniform Trade Secrets Act (UTSA), adopted in California as Civil Code § 3426 et seq., "creates a statutory cause of action for the misappropriation of a trade secret." The statute defines a trade secret as "*information*, including a formula, pattern, compilation, program, device, method, technique, or process, that: (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

The Court of Appeal concluded in *Altavion* that "if a patentable idea is kept secret, the idea itself can constitute information protectable by trade secret law." The logic of *Altavion* suggests that secrets that are legally protectable elsewhere could fall under the definition of "information" in California **even absent that other protection**. Perhaps I should keep this secret.

Don't lawyers apply the holding in one case to the facts in another case to show the court why one side should win? Wouldn't *Altavion's* exact holding apply to, say, facts involving "an expressible form of an idea or information that is substantive and discrete?"

The (summary judgment) argument might go: since an idea is protectable as a trade secret, and information is protectable as a trade secret, a substantive, discrete, expressible form of an idea or information **must be protectable** as a trade secret.

Trading Secrets

In the vernacular of a mathematical proof, "*quid erat demonstratum*."

By the way, a substantive, discrete, expressible form of an idea is … **a copyright.**

Would a trademark-eligible logo (isn't a logo just a "pattern"?) or character development in a script (a "compilation"?) provided to another under reasonable secrecy also be protected under the USTA?

Who was that Pythagoras guy again?

"Bridgegate" Triggers Proposed Expansion of New Jersey Whistleblower Protections

By Ada Dolph, Robert Syzba and Jade Wallace (October 20, 2014)

In an effort to preempt another "Bridgegate" scandal, New Jersey State Senator Loretta Weinberg has sponsored a bill to extend whistleblower protection to employees who disclose incidents of wasted public funds, governmental abuse, or gross mismanagement. On October 9, 2014, the New Jersey Senate's Labor Committee approved Bill S-768, which, if passed, will significantly expand New Jersey's Conscientious Employee Protection Act ("CEPA").

Last year, in a scandal dubbed "Bridgegate" by the media, Governor Chris Christie and his administration were accused of ordering a number of lane closures on the George Washington Bridge. The lane closures caused massive traffic jams that gridlocked Fort Lee, New Jersey (home of the New Jersey side of the bridge) during the morning rush-hour on Monday, September 9, 2013, which was Fort Lee's first day of school. Christie's administration was accused of retaliation against the Mayor of Fort Lee, Mark Sokolich, for not supporting Christie in New Jersey's 2013 gubernatorial election. As co-chair of the Legislative Select Committee on Investigation and a representative of Bergen County (home of Fort Lee), Senator Weinberg was a natural choice to propose legislation intended to preclude another "Bridgegate."

The proposed bill would expand CEPA, New Jersey's whistleblower protection statute. CEPA currently protects employees against employer retaliation when they disclose, testify, or refuse to participate in actions by their employer that are criminal or fraudulent, or that risk public safety and health. S-768 broadens employee safeguards by adding protection for employees who report waste of public funds or abuse or gross mismanagement of government authority. The bill defines "abuse of authority" as "a pattern of illegal, malicious, fraudulent, arbitrary or capricious actions" by a government employer "in a manner clearly deviating from the standard of care or competence that a reasonable person would observe in the same situation." "Gross mismanagement" is defined as requiring negligence or incompetence that has a "substantial adverse affect on the operations, clients, customers or employees" of the government agency.

Passed by the committee with a 3-1 vote, the bill now moves forward to the full Senate for consideration. Although the proposed bill's direct impact is limited to public employers, quasi-public and private employers should nevertheless be mindful of these efforts to expand CEPA, which pattern efforts across the country to increase protections for whistleblowers, especially in connection with drafting and enforcing non-disclosure obligations.

Don't Come to a Trade Secret Fight with a Patent Law Defense

By Michael Baniak (November 10, 2014

In what is at heart a trade secret misappropriation case, some Patent Law periodically materializes, like the smile of the Cheshire Cat.

This concept was evidenced by a recent case out of Texas. *Bianco, M.D. v. Globus Medical, Inc.*, 2:12 CV 147 (E.D. TX 10/27/14).

Dr. Bianco had an idea for a continuously adjustable spinal implant, which would fit between two adjacent vertebrae in the spine that had become compressed. Adjust the mechanism, and the vertebrae move apart. The prior art, to use a patent term, revealed mechanisms which would do the same, but were not continuously adjustable—they worked at best in increments, and could not be reversed (once you separated, that was that; no going back).

Dr. Bianco approached Globus with his idea, which apparently was not much more than some drawings and related general text, for a specific embodiment in the form of a scissor mechanism for performing the adjustability (think of a car jack).

According to the Court, Globus and the good Dr. entered into a written NDA (which apparently disappeared in the records, ultimately taking along with it a count for breach of written contract—the contract not materializing at trial). Globus had him submit a "new Idea Submission Form" with his proposal. Over the next two and a half years, Dr. Bianco inquired of Globus on multiple occasions about the Bianco device and Globus' decision. Sometime in later 2009-early 2010, Globus then told Dr. Bianco that it is "not interested in his technology."

Wait for it—one year later, according to the Court, Globus began marketing a continuously adjustable spinal implant. How did Dr. Bianco learn this? A Globus sales representative tried to interest him in the "new" product. (Practice Point 1: Don't try to sell an idea submitter his product development submitted to the company). Dr. Bianco, obviously now "upset," confronted his Globus liason with this news, who responds according to the record that "he understood that [Bianco] had intellectual property in this implant and that the company would make it right." (Practice Point 2: Whoa.)

With that as preamble, the case is of some note because of what we see develop out of Texas trade secret law (which is not atypical here), and the interplay of Patent Law in the process. The case ultimately turned upon not a written contract, but the confidentiality associated with the disclosure and relationship established between the parties surrounding the "idea." Evidence showed that what Globus actually developed and commercialized was not a "scissor mechanism," but something else (called a "ramp"). But Dr. Bianco pitched that his confidential disclosure was broader than just his "scissor" embodiment, and that it was his ideas tht promted Globus to pursue the continuously expandable and reversible implant. This "spurred" Globus engineers to the "ramp" concept. (Practice Point 3: Don't have a sketch of what would be the Globus commercial concept literally drawn by your engineer on the back of Dr. Bianco's submission papers—I couldn't make this up).

The Court does some dancing with the law on the protectability of an "idea" per se, stating axiomatically that "ideas" of course are not protectable under any intellectual property concepts, except, of course, if you keep that idea secret and protect it from discovery by improper means. One can agree to that protection by contract, implied or otherwise, or in "an informal fiduciary relationship." Here, the Court (in the context of evidence presented to the jury), reviewed how the parties did indeed proceed on the basis that the basic "idea" for a continuously adjustable spinal implant may have been conveyed, and then used to if nothing else, "spur" the Globus development.

Patent Law permeates the case where the Globus attempted to try to parse out details of the commercial product from the "idea" conveyed by the plaintiff—"we didn't use certain features, therefore we didn't use the trade secret." The Court noted that for liability, you don't have to use everything, as in a patent claim: ""[u]se does not require that a party use another's trade secret in the form in which it received it."

Patent Law then again materialized in damages. Dr. Bianco was awarded a royalty, both as to past and then going forward, but no injunction. This is very much a result of current Federal Circuit jurisprudence (our national Patent Appeals Court). Dr. Bianco wanted a disgorgement of profits, but the jury, and then post-hac the Judge, concluded that a reasonable royalty was really the measure of damages, largely based upon industry comparative licenses for use of developments by doctors in similar circumstances.

Seyfarth Attorneys to Present Paper on Trade Secrets and Lawyer Mobility at AIPLA Trade Secret Summit

By Daniel Hart and Erik Weibust (November 17, 2014)

At some point in his or her legal education, every law student discovers one of the more strikingly unique rules about the profession that he or she aspires to enter. Unlike laws governing physicians, accountants, engineers, and virtually all other professions, rules governing the practice of law impose a nearly absolute prohibition on lawyer non-compete agreements. At the same time, the law imposes on lawyers nearly ironclad obligations of confidentiality that generally do not apply to other types of professionals and business people.

Despite — or, perhaps, because of — these unique rules, protection of trade secrets in the legal profession poses unique challenges for both law firms and companies. In fact, during the past year, several cases delving into these topics have generated considerable buzz in the legal community, from Schlumberger Ltd.'s suit against its former deputy general counsel for alleged trade secrets theft to a widely publicized lawsuit by Elliott Greenleaf & Siedzikowski against a former partner for alleged hacking of computer files.

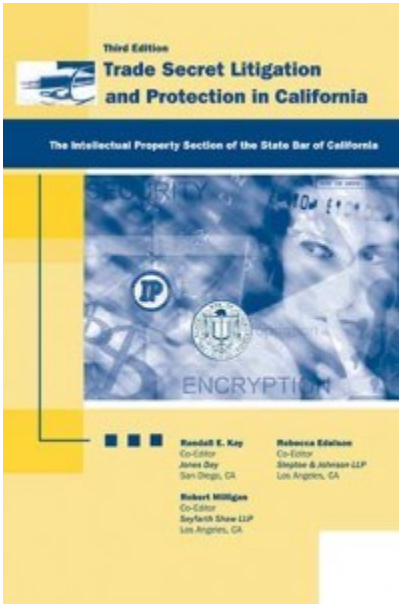
The irony, of course, is that attorneys are hired every day to enforce or seek to block enforcement of non-compete agreements and other post-employment restrictive covenants, yet they are not subject to such agreements themselves. Indeed, while no universal black letter law defines what lawyers can and cannot do in this regard, courts and bar associations facing this issue generally apply a balancing test to ensure that a lawyer's conduct comports with the rules of professional conduct, that client interests are protected, and that there is promotion of fair and open opportunities for lawyer competition. These considerations apply whether the putative restriction applies to in-house or outside counsel. Nevertheless, the overwhelming weight of authority appears to be that attorneys—in-house or outside counsel—are not subject to post-employment restrictive covenants other than under the most exceptional circumstances.

On December 4, 2014, Seyfarth Shaw attorneys will discuss these timely issues at the American Intellectual Property Law ("AIPLA") 2014 Trade Secret Law Summit in Santa Clara, California. At the summit, Erik Weibust (Boston) and Dan Hart (Atlanta) will present "Lawyer Mobility and Trade Secrets Protection: Restrictive Covenant, Confidentiality, and Non-Disclosure Considerations in the Legal Profession," a paper they co-authored with Seyfarth associates Robyn Marsh (Chicago) and Andrew Masak (Atlanta). Among other topics, the presentation will discuss:

- ABA Model Rules of Professional Conduct 1.6 and 5.6 and their impact on lawyer mobility,
- Recent cases and ethical decisions (including ethics opinions from the State Bars of New York, New Jersey, Illinois, Washington, and other jurisdictions) on lawyer restrictive covenants,
- Application of ethical rules on lawyer non-competes in the in-house context, and
- Practical considerations for protecting trade secrets and enforcing restrictive covenants in the legal profession.

Seyfarth Team Co-Edits and Co-Authors Prominent New Trade Secret Protection and Litigation in California Treatise

By Robert Milligan (December 1, 2014)



A Seyfarth team just finished co-editing and co-authoring a prominent new California trade secret treatise that is now available for purchase.

Los Angeles trade secrets partner Robert Milligan co-edited and co-authored a chapter in the recently released Third Edition of Trade Secret Protection and Litigation in California, a treatise published by the Intellectual Property Section of the State Bar of California.

Seyfarth partner Jim McNairy and Seyfarth attorney Joshua Salinas edited chapters in the treatise. Seyfarth attorney Anthony Orler co-authored a chapter in the treatise. Additionally, class action clerk Lauren Leibovitch provided invaluable assistance in coordinating the editing effort.

The twenty-seven chapter treatise provides a comprehensive review and analysis of California trade secret law. Written by California practitioners, the treatise explains the fundamentals and intricacies of California trade secret law. The treatise is a resource for anyone working with trade secrets in litigation or providing counsel on trade secret issues. The Third Edition includes two new chapters on digital forensics and the pursuit of trade secret claims at the International Trade Commission, as well as a model non-disclosure agreement and protective order. The new edition also provides updates of the recent case developments in the trade secret law since the 2nd Edition.

Chapters include:

- What is a Trade Secret?
- Misappropriation
- Trade Secret Protection Programs
- Advising the Corporation
- Injunctions
- Damages

Trading Secrets

- Criminal Prosecution
- Licensing Trade Secrets
- Digital Forensics

The treatise can be purchased by State Bar IP Section Members for $115 and by Non-Members for $155. Until December 15, 2014, IP Section members can get the special price of $95. Use the promo code IP Institute2014 and the discount will be applied at check-out.

Has the Patent Fee Shifting Analysis of Octane Fitness Influenced Fee Shifting in Trade Secret Cases?

By Matthew Werber (December 2, 2014)

In *TNS Media Research, LLC v. TiVo Research & Analytics, Inc.*, 2014 U.S. Dist. LEXIS 155914 (S.D.N.Y. Nov. 4, 2014), the Southern District of New York applied the Supreme Court's recent *Octane Fitness* decision in awarding attorney fees to patent defendant Kantar. *Octane Fitness v. ICON Health & Fitness* 134 S. Ct. 1749 (2014); http://www.seyfarth.com/publications/OMM050114-IP.

The district court also awarded Kantar fees it incurred in successfully defending trade secret misappropriation claims. Did *Octane Fitness* influence the court's fee award for the trade secret claim, notwithstanding the different standards for fee shifting between the Patent Act and state trade secret laws?

1. Fee Shifting in Patent and Trademark Cases Under *Octane Fitness*.

Fee shifting in patent cases is governed by 35 U.S.C. § 285 which reads, in its entirety: "[t]he court in exceptional cases may award reasonable attorney fees to the prevailing party." *Octane Fitness* seemingly made it easier for patent defendants to obtain fees by setting forth a flexible framework for determining if a case is "exceptional" under 35 U.S.C. § 285:

an "exceptional" case is simply one that stands out from others with respect to the substantive strength of a party's litigating position … or the unreasonable manner in which the case was litigated.

Id. 1756. In announcing this more flexible interpretation of "exceptional," the Supreme Court emphasized considering the "substantive strength" of the parties' claims and defenses, and dispensed with a prior formulation that generally required the defendant to show, by clear and convincing evidence, that infringement allegations were baseless and brought in bad faith. The prior formulation, the Supreme Court reasoned, was "so demanding that it would appear to render § 285 largely superfluous," given that district courts already possess the inherent power to award fees in cases involving misconduct or bad faith.

Fee shifting in trademark cases is governed by 15 U.S.C. §1117 which reads: "[t]he court in exceptional cases may award reasonable attorney fees to the prevailing party." In other words, the Lanham Act and Patent Act recite the same "exceptional" language, and courts have already proceeded to apply *Octane Fitness* in trademark cases. See e.g. *Fair Wind Sailing, Inc. v. Dempster*, Case Nos. 13-3305, 14-1572 (3d Cir., Sept. 4, 2014).

2. Fee Shifting in Trade Secret Cases.

State trade secret statutes do not contain the "exceptional" case language found in the Patent Act and Lanham Act. Instead, trade secret defendants in most states seek fees under Section 4 of the Uniform Trade Secrets Act ("UTSA"), which reads, in relevant part: "[i]f … a claim of misappropriation is made in bad faith … the court may award reasonable attorney's fees to the prevailing party." Interestingly, the comment to UTSA Section 4 references following "patent law" in considering fee awards: "patent law is followed in allowing the judge to determine whether attorney's fees should be awarded even if there is a jury, compare 35 U.S.C. Section 285."

While New York has not adopted the UTSA, Federal Courts applying New York law can rely on their inherent power to award fees to the defendant. *Ransmeier v. Mariani*, 718 F.3d 64, 68 (2d Cir. 2013) ("[a] court may exercise its inherent power to sanction a party or an attorney who has acted in bad faith, vexatiously, wantonly, or for oppressive reasons) (quotations omitted). Such inherent power is generally available to federal courts in connection with any type of lawsuit, and is not unlike the UTSA fee shifting language requiring bad faith by the plaintiff.

3. The S.D.N.Y's fee awards in the *TNS Media* Case.

The *TNS Media* case is a technology dispute relating to collecting data on television viewing. The plaintiff ("TRA") claimed that defendant Kantar engaged in acts of patent infringement and trade secret misappropriation (under New York Law). The district court entered summary judgment in favor of Kantar on both claims and Kantar sought fees from TRA.

In granting Kantar's motion for fees in connection with the patent infringement allegations, the district court applied *Octane Fitness* and found the case to be "exceptional" under Section 285, based in large part on the substantive weakness of the patent claims TRA maintained. For example, the court found certain TRA arguments on patent claim construction to be not only wrong, but also sanctionable.

TRA's proposed construction "does violence to the ordinary grammatical understanding of the past tense." No correct application of the rules of grammar could have supported TRA's proposed construction. Thus, TRA's proposed construction lacked merit and was frivolous. See e.g. *Id*. at * 24.

The district court continued by awarding Kantar fees in connection with the trade secret misappropriation claims based on its inherent power:

TRA's analysis lacked critical elements of a claim for trade secret misappropriation. For that reason, TRA's claims were frivolous. In fact, I find here that bad faith may be inferred because TRA's claims were "so completely without merit as to require the conclusion that they must have been undertaken for some improper purpose[.]" *Id.* at *37.

The district court explicitly recognized the difference in legal standards for fee shifting between the patent and trade secret claims — the later requiring bad faith. Yet, similarities in the analyses suggest that the *Octane Fitness* patent fee shifting standard was influential in the trade secret fee award. For example, both fee awards were driven in large part by TRA's maintaining claims perceived to be substantively weak:

Kantar, in order to collect any attorneys' fees or costs for its defense of the patent-related claims, must demonstrate it incurred those fees and expenses as a direct result of TRA's litigation misconduct or frivolous arguments (as described in this Opinion and Order).

Similarly, with respect to the non-patent-related attorneys' fees awarded under the Court's inherent power, Kantar must demonstrate that the fees it seeks to collect are only those fees that directly resulted from its defense against the five trade secret claims that were adjudicated at summary judgment. No fees or costs will be awarded as a result of the trade secret claims dropped subsequent to the April 23, 2013 status conference.

Id. at *39. Also, fee awards in favor of trade secret defendants have not been very common. In fact, a brief survey of the case law proffered by both sides in their briefing did not reveal any examples of a fee award being awarded to a trade secret defendant. Thus, the *TNS Media's* decision to award fees on the trade secret count appears to be fairly unique.

4. *Octane Fitness*' Impact on Trade Secret Litigation Going Forward.

Given the differences in legal standards, *Octane Fitness* is not likely to impact trade secret litigation as much as it has impacted patent and trademark litigation. Yet, some impact would not be surprising. For example, prevailing trade secret defendants in non-UTSA states, such as New York, may rely on *TNS Media* in seeking fees. Trade secret defendants in UTSA states may even consider relying directly on *Octane Fitness* based on the UTSA's comment referring to courts following "patent law" for fee shifting guidance.

California Court Extends Protections To "Silent Whistleblowers"

By Jeffrey Berman and Jonathan Brophy (December 5, 2014)

Employers, although contractually free to terminate the employment of at-will employees for any reason, at any time, cannot dismiss an employee in violation of public policy. A prime California public policy is that employers cannot retaliate against whistleblowers—individuals who have reported suspected unlawful employer conduct. In January 2014, the Legislature expanded the general whistleblowing statute, Labor Code section 1102.5, to prevent employers from taking retaliatory action in a belief that "the employee disclosed or may disclose" relevant information.

On November 21, 2014, in *Diego v. Pilgrim United Church of Christ*, the California Court of Appeal clarified that Section 1102.5, even in its pre-amended version, forbids employers to terminate "perceived whistleblowers," even if that belief is mistaken.

The Facts

Cecilia Diego worked as an assistant director of Pilgrim United's preschool. Diego claimed that a coworker had contacted the Licensing Division of the California Department of Social Services to report a foul odor in a classroom and inadequate sand beneath the playground equipment. The Licensing Division then conducted an unannounced inspection, but found no violations and issued no citations. Diego claimed that her supervisor then asked Diego why she had made the reports. Diego understood that her supervisor believed that she had been the source of the anonymous complaints to the Licensing Division, even though this was not the case.

Shortly after the inspection, Diego failed to appear at a meeting her supervisor had scheduled for her. Pilgrim United then discharged Diego for insubordination.

When Diego sued Pilgrim United, claiming that her termination was retaliatory and in violation of California public policy, the trial court granted summary judgment against her claim. The trial court found that Diego had failed to identify a significantly important public policy that was implicated by constitutional or statutory authority: Diego had failed to cite "any case holding that an employer's mistaken belief that the employee reported a violation can support a claim for wrongful termination in violation of public policy."

The Appellate Court Decision

The Court of Appeal reversed the trial court. It held that California's public policy "applies to preclude retaliation by an employer not only against employees who actually notify the agency of suspected violations but also against employees whom the employer suspects of such notifications." The Court of

Appeal reasoned that the policy embodied by former Labor Code section 1102.5 (which did not expressly address an employer's belief about whistleblowing) was not limited to employees who actually reported violations, because such a limitation would discourage employees from reporting violations in the first instance.

In addition, the Court of Appeal found that the alleged "insubordination" was not so well established, for purposes of summary judgment, to withstand Diego's proof that the employer's assertion of insubordination was a mere pretext for unlawful retaliation in the belief that Diego had been a whistleblower.

What Pilgrim United Means For Employers

California Labor Code section 1102.6 already provides that if an employee proves that the employee's protected activity was "a contributing factor in the alleged prohibited action," then the employer must show by "clear and convincing evidence that the alleged action would have occurred for legitimate, independent reasons even if the employee had not engaged in [protected] activities." Pilgrim United reinforces the point that employers should document performance issues and disciplinary decisions to help support later decisions to discipline an employee.

USPTO To Host Trade Secret Symposium

By Joshua Salinas and Robert Milligan (December 17, 2014)

The U.S. Department of Commerce's Patent and Trademark Office (USPTO) will host its first Trade Secret Symposium on Thursday, January 8, 2015, at USPTO Headquarters in Alexandria, Virginia. The symposium will provide an opportunity for members of the public to hear from representatives of academia, government, legal practice and industry on important trade secret issues facing innovators today.

The panels will touch on a variety of topics, including legislative proposals regarding trade secret protection, the challenges to estimating losses due to trade secret theft, the intersection of patents and trade secrets, issues in civil litigation involving trade secrets, international considerations, and the response to trade secret theft in the U.S. The schedule will allow time for questions from the audience.

The symposium will be held at the United States Patent and Trademark Office, Madison Building, Madison Auditorium South, 600 Dulany Street, Alexandria, Virginia 22314. The symposium will begin at 9:00 a.m. and end at 3:00 p.m. The agenda will be available a week before the symposium on the USPTO Web site, www.uspto.gov/.

Registration is available at www.uspto.gov/ip/init_events/trade_secret_symposium.jsp. Attendees may also register at the door. Attendance is free.

Further information about the symposium may be found in the Federal Register Notice.

Arizona Supreme Court Holds that UTSA Does Not Preempt Common Law Claims for Misuse of Confidential Information That Is Not a Trade Secret

By Daniel Hart (December 17, 2014)

The nineteenth century English jurist Lord Ellenborough once observed that "it is difficult to struggle with the common law." *Kerr v. Willan*, 171 Eng. Rep 570 (K.B. 1817). Nearly two centuries later, struggling with the common law is still a formidable task – especially in cases involving claims of trade secrets misappropriation under the Uniform Trade Secrets Act ("UTSA").

The UTSA, which has been enacted in one form or another by all but two states, provides a statutory remedy for trade secrets misappropriation. Like the version of the UTSA enacted by other states, Arizona's version of the UTSA, the Arizona Uniform Trade Secrets Act ("AUTSA"), contains a provision broadly providing that the law "displaces conflicting tort, restitutionary, and other laws of this state providing civil remedies for misappropriation of a trade secret." A.R.S. § 44-407(A). Also like the version of the UTSA enacted by other states, the AUTSA includes an important exception to this broad preemption provision:

This chapter does not affect:

1. Contractual remedies, whether or not based on misappropriation of a trade secret.

2. Other civil remedies that are not based on misappropriation of a trade secret.

3. Criminal remedies, whether or not based on misappropriation of a trade secret.

A.R.S. § 44-407(B).

These provisions are straightforward when a plaintiff sues for misappropriation of information that is clearly a "trade secret" as defined by the AUTSA. In those cases, the AUTSA is the plaintiff's sole remedy (other than criminal and contractual remedies) and the plaintiff cannot bring common law claims (such as claims for unfair competition, conversion, or unjust enrichment) for misappropriation of the same information. But what happens when a plaintiff sues for misappropriation of both "trade secrets" and confidential information that does not qualify as a "trade secret" under the AUTSA? Since the plaintiff cannot assert an AUTSA claim for misappropriation of run-of-the-mill confidential information that does not qualify for protection as a trade secret, is the plaintiff free to assert common law claims for misappropriation of that run-of-the-mill confidential information? Or is the plaintiff simply out of luck?

Courts throughout the country have grappled with this question since the UTSA was first adopted. Not surprisingly, courts have reached different opinions on the question. Courts in several states have held that the UTSA should be read broadly to preempt all claims related to the misappropriation of information, regardless of whether or not the information falls within the definition of a trade secret. Conversely, courts in other states have concluded that the UTSA preempts only claims for misappropriation of "trade secrets," as defined by the UTSA, and leaves available all other remedies for the protection of confidential information that is not a trade secret.

With its recent decision in *Orca Communications Unlimited, LLC v. Noder*, 337 P.3d 545 (Az. 2014), the Arizona Supreme Court joined this latter group and held as a matter of first impression that the AUTSA does not displace common law remedies for misappropriation of confidential information that does not qualify as a trade secret.

In that case, Orca Communications Unlimited ("Orca"), sued its former employee, Noder, for unfair competition after Noder left Orca to start a competing business. In its complaint, Orca alleged that, through her employment with Orca, Noder had "learned confidential and trade secret information about Orca," including "Orca's business model, operation procedures, techniques, and strengths and weaknesses," and that she intended to "steal" and "exploit" that information to gain a competitive advantage for her new company. After Noder filed a motion to dismiss, the trial court dismissed Orca's unfair competition claim, reasoning that the AUTSA preempted "common law tort claims arising from the alleged misuse of 'confidential information,'" even as to information "not asserted to rise to the level of a trade secret." On appeal, the Arizona Supreme Court disagreed and reversed the trial court's decision. Noting the split of authority on the scope of the UTSA's preemption of common law remedies, the court based its decision on the express language of the AUTSA cited above and observed:

On its face, § 44-407 displaces only conflicting tort claims for "misappropriation" of a "trade secret," terms AUTSA specifically defines, A.R.S. § 44-401(2), (4), and leaves undisturbed claims "that are not based on misappropriation of a trade secret," *id.* § 44-407(A), (B)(2). Nothing in this language suggests that the legislature intended to displace any cause of action other than one for misappropriation of a trade secret.

Moreover, the court noted that Noder's argument was inconsistent with the "well-established principle" that "[i]f the legislature seeks to preempt a cause of action, the law's text or at least the legislative record should say so explicitly" and that "[a]bsent a clear manifestation of legislative intent to displace a common-law cause of action, we interpret statutes with every intendment in favor of consistency with the common law." Accordingly, because the text of the AUTSA "creates reasonable doubt about the legislature's intent regarding displacement of common-law claims that do not involve trade secrets as defined in AUTSA," the court concluded that the trial court erred in dismissing the unfair competition claim to the extent that it was premised on misappropriation of confidential information that is not protected by the AUTSA.

The Arizona Supreme Court's decision in *Orca* illustrates a significant trend in trade secrets litigation in recent years: as an increasing number of states adopt the UTSA, courts throughout the country increasingly must consider how the UTSA impacts existing common law remedies, As reflected by the split of authorities that the Arizona Supreme Court cited in*Orca*, courts are literally all over the map in how they answer this question. Since interpretation of the UTSA (as enacted by each state) is a matter of state law, it is unlikely that a consensus will be reached on this issue anytime in the near future. And although creation of a federal civil cause of action for trade secrets misappropriation appears increasingly likely, current proposals in Congress provide that any federal civil action will not preempt state law. Assuming that Congress does not completely preempt state law trade secrets law, the split of authorities among state courts will likely continue even if a federal trade secrets law is passed.

Given the lack of uniformity on this issue, employers should stay abreast of how courts are interpreting the UTSA or other trade secrets law in the jurisdictions where they do business. For a quick reference on how your jurisdiction stacks up on trade secrets protection, refer to our 50 State Desktop Reference and contact a Seyfarth Shaw trade secrets lawyer.

Seyfarth Attorneys Present At 2014 American Intellectual Property Association Trade Secret Summit

By Erik Weibust, Daniel Hart, and Andrew Masak (December 19, 2014)

On December 4th and 5th, nearly 100 trade secret, non-compete, and economic espionage practitioners convened at the Intel Global Headquarters in Santa Clara, California for the annual American Intellectual Property Law Association Trade Secret Law Summit. Two Seyfarth attorneys, Erik Weibust and Daniel Hart, presented a paper co-authored with Andrew Masak and Robyn Marsh, titled "Lawyer Mobility and Trade Secrets Protection: Restrictive Covenant, Confidentiality, and Non-Disclosure Considerations in the Legal Profession." Specifically, the Seyfarth attorneys, sought to address the question of "what can law firms and companies do to protect themselves – like any other industry – from attorneys who leave to join a competitor? From their paper andpresentation,

Attorneys leaving their law firms or companies for other opportunities is nothing new. And, certainly, changing from one employer to another is not unique to the legal industry. As in many other industries, employees switching jobs among competitors can raise serious concerns about the misappropriation of trade secrets and confidential information, and client poaching. Yet, unlike most other industries, restrictive covenants limiting attorneys from competing with their former firms or companies, or taking clients with them, are generally unenforceable. In fact, most successful firm lawyers are recruited to other firms for the very reason that they have "portable" business.

This does not, however, mean that attorneys have free range to take and utilize confidential information and trade secrets about their prior firms or clients who choose not to go with them. Quite to the contrary, there are ethical rules barring such behavior. Nevertheless, the inability of companies and law firms to impose restrictive covenants on lawyers employed by the companies and firms poses practical challenges. Indeed, in-house counsel, who often act as much as business advisors as they do legal counsel, may be privy to the most sensitive business information of a corporation when they leave to join a competitor, yet they, too, are generally immune from restrictive covenants that restrict their ability to practice law, even for a competitor.

In addition to the Seyfarth team presenting their ethics in non-competes presentation, the conference included two days of presentations and debates, including:

- An FBI Briefing on Economic Espionage, "Honey Potting," and When to Include the FBI in Your Company's Litigation
- Emerging Best Practices for Protecting Trade Secrets in Employment and Business-to-Business Relationships;
- A Judicial Panel Providing Insights from the Bench on Trade Secret and Non-Compete Disputes;
- Debates on the Future of Non-Competes and Pending Federal Legislation;

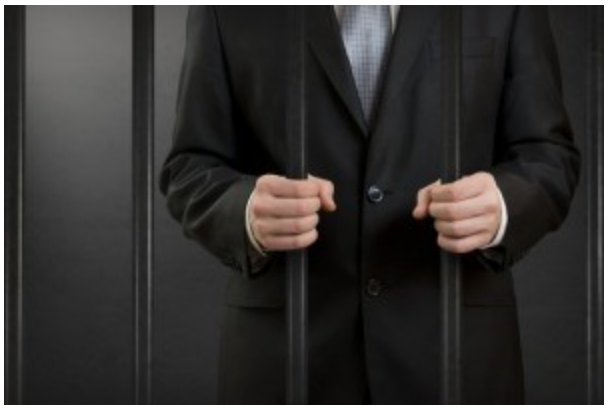
- Pros and Cons of Trade Secrets vs. Patents; and
- The Latest on Developing Cybersecurity Standards.

The AIPLA Trade Secret Summit is an annual conference designed for both in-house and outside counsel.

Computer Fraud and Abuse Act

Nosal Update: Nosal Sentenced to One Year in Federal Prison

By Erik von Zeipel (January 9, 2014)



On January 8th, after years of litigation and numerous delays, Executive Recruiter David Nosal was sentenced to one year and a day in federal prison for his April 25, 2013 conviction 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. The court also ordered Nosal to 400 hours of community service and three years of supervised release.

While Nosal's counsel had argued for mere probation, the one-year sentence was considerably shorter than the 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. The sentence was also shorter than the 27 months requested by federal prosecutors, and less than the 15 to 21 months provided for by sentencing guidelines.

The court based the sentence on its conclusion that Nosal's former employer's losses were less than $50,000, based on the value of the stolen information and time spent investigating the crime. Federal prosecutors had estimated the losses at close to $600,000, while Nosal's counsel argued that the former employer had suffered no real loss.

Following sentencing, the court released Nosal to return to the British Virgin Islands where he is vacationing with his family.

Although the sentencing is the end of a chapter, it is not the end of this saga. Federal prosecutors have asked the court to order Nosal to pay more than $1.3 million in restitution to his former employer, including almost $1 million in legal fees incurred by the former employer's counsel. Defense counsel has already filed a motion for Nosal to remain free pending appeal. The court will address those motions in a future hearing. The appeal process will likely take years to resolve. As referenced in an earlier post, this case will presumably once again end up before the Ninth Circuit which will determine whether the conviction will stand in light of its earlier en banc decision limiting the reach of the CFAA, finding that the statute was intended to punish hacking, not misappropriation of trade secrets in violation of an employer's acceptable use policies.

Courts Disagree on Meaning of "Interruption of Service" When Determining Loss Under the Computer Fraud And Abuse Act

By Paul Freehling (March 17, 2014)

District courts are divided as to whether there is a private right of action under the Computer Fraud and Abuse Act(CFAA) for persons whose computer service is not interrupted but who nevertheless incur costs (a) responding to a CFAA offense, (b) conducting a damage assessment, or (c) restoring computerized data or programs as they were prior to the offense. A Georgia U.S. district court judge recently sided with those jurists who hold that a service interruption is not required. *Southern Parts & Eng'r'g Co. v. Air Compressor Services, LLC*, Case No. 1:13-CV2231-TWT (N.D. Ga., Feb. 19, 2014).

Case Summary

Two employees of Southern, a manufacturer of air compressors, resigned and created a competitor corporation. Allegedly, both before and after their resignation, the two employees accessed Southern's computerized confidential information, but the employees did not cause an interruption in the company's computer service. Southern sued the employees in a Georgia federal court for violating the CFAA. The employees moved to dismiss on the ground that Southern had not sustained a compensable loss because no "interruption of service" had occurred. Acknowledging a split of authority, the Georgia judge ruled that a service interruption is not required, and so the motion to dismiss was denied.

Statutory Interpretation

A jurisdictional requirement under the CFAA is a "loss" of at least $5,000 caused by a violation of the Act. The CFAA defines a "loss" as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Courts are divided as to whether the phrase "incurred because of interruption of service" (a) modifies "any reasonable cost to any victim," or (b) applies only to "any revenue lost, cost incurred, or other consequential damages."

Different Interpretations

Some judges have concluded that the CFAA provides for recovery of expenses resulting from "responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense," regardless of whether there was an "interruption of service." The other view is that an "interruption of service" is a condition precedent to any recovery.

The judge in the *Southern Parts* case adopted the former interpretation — "interruption of service" is not a prerequisite — as have judges in the Middle and Southern Districts of Florida, the Middle District of Louisiana, and the Southern District of Texas, and one judge in the Eastern District of Michigan. By contrast, judges in the Northern District of Florida, the Northern District of Illinois, the District of Maryland, and the Southern District of New York, and a different judge in the Eastern District of Michigan, disagree. (Those are not the only courts to have ruled on the issue.) Clearly, reasonable minds can differ!

Takeaways

The victim of a CFAA violation must demonstrate that it has incurred $5,000 in expense in a single year. In the absence of an "interruption of service," there may be an opportunity for forum shopping. The victim might consider whether personal jurisdiction and venue would be proper in a court that allows CFAA suits to proceed even though no interruption occurred. If the victim selects such a forum, the alleged wrongdoer might consider the possibility of seeking to transfer the litigation either to a district that declines to adjudicate CFAA lawsuits when there has been no "interruption of service" or, at least, to a district that has not yet weighed in on the issue.

Computer Fraud and Abuse Act Claims in the First Circuit – Will the Narrow Approach Prevail?

By Dawn Mertineit (March 25, 2014)

The scope of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, remains unsettled in the First Circuit after two decisions issued just weeks apart adopted differing approaches to the treatment of such claims.

The CFAA prohibits the intentional access of a computer without authorization or exceeding a party's authorization to obtain information from a protected computer. As we have previously reported here, courts are split on the interpretation of what constitutes unauthorized access or access that exceeds authorization. In some jurisdictions, courts take a narrow view, limiting "unauthorized access" to true "hacking" cases, where a party improperly gains access to documents he or she is not authorized to obtain. On the other hand, certain circuits have favored a broad interpretation that would prohibit a party from accessing documents to which he or she typically would have access, if such access were for an improper purpose (for example, an employee who misappropriates documents to which she legitimately had "technical access" for the benefit of a competitor).

At the beginning of December, Judge Denise Casper of the U.S. District Court for the District of Massachusetts granted in part a preliminary injunction in *Enargy Power Co. Ltd. v. Wang*, C.A. no. 13-cv-11348-DJC, based on an alleged violation of the CFAA. The plaintiff had alleged that the defendant, a former employee, had instructed his assistant to encrypt certain files on the employer's computer server, and directed her to transmit those files to him, all in violation of the CFAA. Citing*Advanced Micro Devices, Inc. v. Feldstein*, et al., C.A. No. 13-40007, which we previously reported on here, Judge Casper noted that the defendant's actions "employed an element of deception in that he acted without his employer's consent or knowledge . . . and using his assistant as a conduit, who had every reason to trust that [the defendant] was acting within the scope of his authorization," and accordingly those actions likely exceeded the scope of his authorization.

Judge Casper's reliance on the "means of a deception" language used in *Feldstein* suggests a trend in the First Circuit to limit the previously adopted broad interpretation to those cases where a defendant exceeds his authorization through some deceptive act with fraudulent intent. It remains unclear whether a garden-variety misappropriation case, in which an employee obtains documents for the purpose of competing with his or her employer but without "hacking" into the employer's computer servers, would be viewed as sufficiently "deceptive" so as to constitute a violation of the CFAA under the *Feldstein* and *Enargy* line of cases.

Another case decided less than two weeks later took an even narrower view. In *Verdrager v. Mintz, Levin, Cohn, Ferris, Glovsky & Popeo, P.C.*, Judge Peter Lauriat of the Massachusetts Superior Court

analyzed a law firm's CFAA counterclaim against its former associate, who had alleged sex discrimination and retaliation. The firm, Mintz Levin, alleged that the associate had conducted searches for documents related to her case on the firm's document management system, and forwarded relevant documents to herself or her attorney. Determining that the associate clearly had access to the documents she viewed and transmitted, Judge Lauriat found that "it was not the obtaining of the documents that creates the basis for [Mintz Levin's] claims against [the associate], but for what use she sought to obtain them." Judge Lauriat held that the associate's disloyalty could not form the basis of a CFAA violation, and that Mintz Levin's failure to restrict the associate's access to sensitive documents related to her case "further weaken[ed] [Mintz Levin's] position" that the associate had violated the CFAA, and granted summary judgment in the associate's favor.

In light of the unsettled landscape of CFAA actions in the First Circuit, employers must remain vigilant. For example, where employers have reason to believe an employee may be using confidential documents for an improper purpose, immediate steps should be taken to restrict the employee's ability to access such documents. However, until Congress or the Supreme Court settles the matter for good, it remains unclear how courts in the First Circuit will treat CFAA claims against employees accused of misappropriation.

Third Circuit Signals Pro-Defendant Interpretation of the Computer Fraud and Abuse Act's "Authorized Access" Provisions

By Scott Schaefers (April 16, 2014)

On April 11th, the Third Circuit Court of Appeals reversed the conviction and 41-month prison sentence of a Computer Fraud and Abuse Act (CFAA) defendant, holding that he was tried and convicted in an improper venue. *U.S. v. Auernheimer*, No. 13-1816 (3rd Cir. Apr. 11, 2014). Though we usually do not post on procedural issues like these, we certainly post on substantive CFAA developments.

In footnote 5 of its opinion, the court said that the government failed to prove that defendant accessed the network "without authorization, or in excess of authorization" under New Jersey's state computer-crime law. That is the same language in the CFAA over which federal courts have been split for the last several years regarding employee liability for misuse of company files. The Third Circuit's footnote indicates that it is leaning toward the narrower, pro-employee / pro-defendant interpretation, espoused by the Fourth and NinthCircuits, which prohibits CFAA liability for employees who merely abuse their otherwise legitimate access to company files.

The defendant in *Auernheimer* (a/k/a "Weev") was convicted of "slurping," which, at least in this case, involved the automated scraping of user email addresses from their login screens on their computer tablets. Such slurping and scraping did not involve "hacking," or circumventing a code- or password-based barrier to a user account or network. Rather, the slurpers merely found loopholes in public-facing login screens, and gathered the username email addresses which the account providers unintentionally "published." In other words, slurping did not involve "accessing" an account "without authorization" from the provider or accountholder. It merely involved scraping together information which was publicly available, albeit inadvertently from the provider's and user's standpoint.

After defendant and his "co-conspirator" gathered 114,000 email addresses and went to the press with this alleged "security flaw," the New Jersey U.S. Attorney's Office obtained a two-count indictment against them for conspiracy to violate the CFAA, and for violation of New Jersey's computer crime statute. Defendants objected to venue in New Jersey, citing the facts that they "slurped" from their homes in California and Arkansas, and that the cell network's affected servers were located in Texas and Georgia. The district court overruled defendants' objections, and a jury eventually convicted them on both counts. The district court sentenced Weev to 41 months in prison.

In reversing the conviction, the Third Circuit said that venue in criminal cases implicated constitutional rights, which were violated in this case by defendants' being tried and convicted so far from home and where they allegedly broke the law. In pointing out that neither defendant "accessed a computer in New Jersey," the court noted that the government failed to prove that defendants' slurping of email addresses amounted to access "without authorization, or in excess of authorization" under the state cybercrime law. (P. 12, n. 5). Defendants merely wrote a program which scraped together publicly available information, the access of which could not be unauthorized.

This reasoning indicates that the Third Circuit is leaning toward the pro-employee, pro-defendant interpretation of the CFAA's "without authorization" and "exceeding authorization" provisions. The Fourth and Ninth Circuit Courts of Appeals have adopted that approach, holding that the CFAA does not apply to employees who copy files and send them to or use them for a competitor. The access itself was not unauthorized, even if the subsequent file use was. Thus, no liability under the statute's plain language. The Fifth, Seventh and Eleventh Circuits take the opposite stance; that employees who use their otherwise authorized access to company computers can be liable under the CFAA for their subsequent misuse of the files on those computers. Under normal agency law, employees have no authorization to use company files against the company. Their accessing the company's computers for that purpose, those courts held, violated the CFAA.

Granted, the *dicta* reasoning is not binding on district courts in the Third Circuit, or on the Third Circuit itself. But the court's interpretation of the very same CFAA language over which other federal courts have issued conflicting decisions for the past two decades *again* points up the need for the Supreme Court to resolve the split, or for Congress to amend the statute. The Obama administration lobbied the Senate in 2011 to adopt the Fifth, Seventh, and Eleventh Circuits' pro-employer position, but nothing yet. As it stands, whether a disloyal employee may be prosecuted or sued under the CFAA depends on the federal circuit in which he or she works.

Louisiana District Court Extends Pro-Employer Interpretation of the Computer Fraud and Abuse Act's "Authorized Access" Provisions to Impose Civil Liability on Former Employee

By James Beyer (May 2, 2014)

A worker's authorized access of an employer's computer system during the course of his employment, in which he acquired information that he later misused, gives rise to civil liability under the Computer Fraud and Abuse Act (CFFA), the U.S. District Court for the Eastern District of Louisiana held April 3 (*Associated Pump & Supply Co., LLC v. Dupre*).

Kevin Dupre worked as a salesman covering certain Louisiana parishes for Associated Pump & Supply Co. under a confidentiality and noncompetition agreement. Before terminating his employment, Dupre allegedly started a competing company and discussed employment with another competitor. Dupre also allegedly downloaded files containing confidential information and trade secrets and deleted files belonging to Associated Pump from his work computer. The employer filed suit against Dupre alleging a CFAA violation, amongst other claims. Dupre moved to dismiss the CFAA claim, contending that Dupre's access was not "unauthorized" or "exceeding authorization." A claim brought pursuant to the CFAA under 18 U.S.C. § 1030(a)(4) requires the plaintiff to prove the following elements: "(1) defendant has accessed a protected computer; (2) has done so without authorization or by exceeding such authorization as was granted; (3) has done so 'knowingly' and with 'intent to defraud'; and (4) as a result has 'further[ed] the intended fraud and obtain[ed] anything of value."

As we recently blogged in our Trade Secrets blog here and here, some federal courts have taken a pro-employee stance, while others have taken a pro-defendant interpretation of the CFAA's "without authorization" and "exceeding authorization" provisions. The Fourth and Ninth Circuit Courts of Appeals have adopted that approach, holding that the CFAA does not apply to employees who copy files and send them to or use them for a competitor. The access itself was not unauthorized, even if the subsequent file use was. Thus, they find no liability under the statute's plain language.
The Fifth, Seventh and Eleventh Circuits, however take the opposite stance: that employees who use their otherwise authorized access to company computers can be liable under the CFAA for their subsequent misuse of the files on those computers. Under normal agency law, employees have no authorization to use company files against the company. Their accessing the company's computers for that purpose, those courts held, violated the CFAA.

The Dupre case relied on the Fifth Circuit case of *U.S. v. John*, 597 F.3d 263 (5th Cir. 2010). The Fifth Circuit held in *John* that CFAA liability arises when employee access "exceeds the intended use of the system or when the access is 'in violation of an employer's policies and is part of an illegal scheme.' " In *John*, the employee used authorized access to view and print information but exceeded authorized access by violating company policies when she accessed accounts she didn't manage, removed sensitive information from the premises and used it to perpetrate fraud on the company and its customers. As in *John*, Dupre's alleged conduct violated company policies protecting the confidential information that he accessed, and he allegedly misused the protected information in violation of those policies and the confidentiality agreement. Although the Fifth Circuit's holding was specifically applicable to the criminal context, its reasoning "informs this court on how the Fifth Circuit would treat the instant matter," the district court said.

The *Dupre* case is another example of the very same CFAA language over which other federal courts have issued conflicting decisions for the past two decades. This again points up the need for the Supreme Court to resolve the split, or for Congress to amend the statute. As we have noted before, as it stands now, whether a disloyal employee may be prosecuted or sued under the CFAA depends on the federal circuit in which he or she works. Nonetheless, the *Dupre* case is another decision favoring employers.

Non-Competes & Restrictive Covenants

Federal Court in Alabama Rules That Non-Compete Signed Prior to Employment is Void

By Bob Stevens and Daniel Hart (January 16, 2014)

For many in Alabama, the holiday season does not end until after the college football national championship game, which has featured one of the state's two top college football programs (the Auburn University Tigers and the University of Alabama Crimson Tide) for each of the five past years. While not quite as exciting as Auburn's narrow fourth-quarter loss to Florida State in last week's BCS National Championship Game, a ruling by an Alabama federal district judge issued on the same day could prove to be much more significant for employers and employees in Alabama.

In *Dawson v. Ameritox, Ltd.*, 2014 WL 31809 (S.D. Ala. Jan. 6, 2014), Ameritox, a healthcare company, sought to enforce non-compete and non-solicitation covenants against its former Assistant Director of Medical Science and Health Outcomes Research, Dr. Eric Dawson, who had left Ameritox for a similar position with a competitor. Perhaps believing that its claims would be as safe a bet as hearing the cry of "War Eagle!" at an Auburn football game, Ameritox sought a preliminary injunction against Dawson. But as ESPN's Lee Corso might say, "Not so fast, my friend!" In a January 6 order, District Judge Kristi DuBose ruled that the covenants in question were void and unenforceable because Dawson had executed the agreement ***before*** his employment with Ameritox began.

Under Alabama Code § 8-1-1, a contract by which anyone "is restrained from exercising a lawful profession, trade, or business of any kind" is void, except that "one who ***is employed*** as an agent, servant or employee may agree with his employer to refrain from carrying on or engaging in a similar business and from soliciting old customers of such employer within a specified county, city, or part thereof, so long as the . . . employer carries on a like business therein." Relying on the Alabama Supreme Court's prior decision in *Pitney Bowes, Inc. v. Berney Office Solutions*, 823 So. 2d 659 (Ala. 2001), Judge DuBose noted that employee non-compete agreements are valid only if signed by an employee and that prospective employment is not sufficient to meet the exception in Section 8-1-1. Thus, because Dr. Dawson was not an employee of Ameritox at the time he signed the agreements, Judge DuBose reasoned that the agreements were void and unenforceable. The decision is currently on appeal to the Eleventh Circuit.

The decision in *Dawson* is an important reminder of a requirement in Alabama for enforceability of post-termination restrictive covenants. Most employers provide prospective employees with copies of required non-compete agreements before the employee's first day of work so that prospective employees will be aware of their non-compete obligations in advance. Indeed, some states (such as New Hampshire) expressly ***require*** employers to disclose such agreements before making a job offer. While such practices are prudent, a restrictive covenant may be void in Alabama if a prospective employee signs the agreement before his or her first day of work. To avoid this unintentional fumble, employers in Alabama should ensure that employees execute (or re-execute) such agreements on or

after their first day of employment, ideally in the presence of a representative of human resources. In addition, because continued at-will employment is sufficient consideration for new restrictive covenants in Alabama, employers with operations in Alabama should consider periodically reviewing their existing restrictive covenants and requiring employees to execute new agreements from time to time as appropriate.

Illinois Federal Court Finds Only 15 Months' Employment Sufficient Consideration For Non-Compete Agreement

By Paul Freehling (February 7, 2014)

In a ruling announced a few days ago, Chief Judge Ruben Castillo of the U.S. District Court for the Northern District of Illinois adjudicated the validity of a non-compete clause in an employment agreement where the employee had worked for only 15 months and then resigned and began competing. Notwithstanding the latest word from the Illinois Appellate Court — "Illinois courts have repeatedly held that there must be two years or more of continued employment to constitute adequate consideration in support of a restrictive covenant" (*Fifield*, 993 N.E.2d 938 (2013)) — Judge Castillo declined to invalidate the covenant for lack of consideration. However, he did dismiss the breach of contract count, finding that the provision's geographical and activity restrictions were excessive. *Montel Aetnastak, Inc. v. Miessen*, Case No. 13 C 3801 (N.D. Ill., Jan. 28, 2014) (Castillo, J.).

Summary of the Case

Montel, a manufacturer of shelving and storage racks, employed Miessen as its Midwest Regional Sales Manager. In that capacity, she provided highly confidential services to a Montel customer. Her employment agreement contained a provision prohibiting her, for two years after termination of her employment, from engaging in any business substantially related to that of Montel in the United States and Canada. Upon resigning from Montel, Miessen went to work for Bradford, a competitor, and performed similar tasks for the same customer. Montel sued Miessen, Bradford and Bradford's supplier, alleging common law and statutory violations. The court held that it had jurisdiction over Miessen, denied motions to dismiss several counts, but did dismiss the breach of contract claim and those common law counts pre-empted by the Illinois Trade Secrets Act.

The Trade Secrets

As a Montel employee, Miessen worked with its design and engineering team and with Montel's department store customer to meet its specific requirements at one of its many facilities. Montel expected additional orders from the customer. Montel's designs and pricing were closely guarded secrets. After resigning from Montel, Miessen went to work for Bradford. She became its direct point of contact with that same department store, assisting in reconfiguring Bradford's products for the customer.

Lawsuit and Rulings

Montel filed a seven-count complaint against Miessen, Bradford, and the manufacturer of the products sold by Bradford. Miessen moved to dismiss the complaint against her for lack of personal jurisdiction.

All defendants contended that Montel failed to state justiciable claims. Judge Castillo held that Miessen was subject to the court's jurisdiction. He dismissed some counts but not others.

Enforceability of the Non-Compete Clause

a. Consideration. The defendants argued that, because Miessen worked for Montel for only 15 months, the non-compete covenant failed the Fifield test. Judge Castillo disagreed. He said that some older Illinois appellate court decisions hold that one year is a sufficient period of employment, and that Illinois law does not "provide a clear rule to apply in this instance." He concluded that given the absence "of a clear direction from the Illinois Supreme Court," he would employ the "fact-specific approach employed by some Illinois courts." He held that "the length of her term of employment, along with her voluntary resignation, lead the Court to conclude that she was provided with a 'substantial period' of employment. Therefore, [she] was provided with adequate consideration to support the enforceability of the employment agreement."

b. Geographic and activity restrictions. Judge Castillo found the covenant unenforceable because of "the almost limitless geographic scope of the clause" and the fact that it barred her from working for a competitor, "even if she was employed in a noncompetitive activity." He noted that there was no severability clause and that the covenant's deficiencies were such that "a significant modification would be necessary to make it comport with the law." Accordingly, he declined the defendants' invitation to "blue pencil" the provision by judicially rewriting it, stating that "extensive judicial reformation of unenforceable post-termination restrictive covenants may be counter to public policy."

Takeaways

Judge Castillo's opinion is the first reported judicial critique of *Fifield's* "bright line" requirement of a minimum of two years of employment in order to provide adequate consideration for a non-compete covenant. Montel undoubtedly will be cited in litigation brought by Illinois employers endeavoring to enforce agreements against an employee who worked fewer than 24 months. Montel also may be cited by a former employee opposing extensive judicial modification of a covenant unenforceable as written because of virtually unlimited geographic and activity provisions. Of course, a federal judge's interpretation of Illinois law is not binding in any other case. Only time will tell whether jurists confronted with similar issues find Judge Castillo's reasoning persuasive.

Employers can enhance the likelihood that a non-compete agreement will be enforced by giving employees some tangible consideration for the covenant. Additionally, it should include reasonable duration, geographic, and activity restrictions. A severability clause also may be appropriate.

Texas And North Carolina Appellate Courts Repulse Efforts To Enforce Restrictive Covenants

By Paul Freehling (February 26, 2014)

In two unrelated cases decided earlier this month, employers failed in their attempts to enjoin former employees from competing. The Texas First District Court of Appeals vacated parts of the lower court's injunction order, one part because it did not detail with sufficient specificity the conduct that was enjoined, and another part where the order was sufficiently specific but erroneously enjoined activities that were permissible. *Lasser v. Amistco Separation Products, Inc*., No. 01-13-00690-CV (Tex. Court of App., 1st Dist., Feb. 6, 2014). The North Carolina Court of Appeals held that a covenant's array of prohibited activities was too broad to be enforceable.*CopyPro, Inc. v. Musgrove*, Case No. CCA13-297 (N.C. Court of App., Feb. 4, 2014).

Lasser v. Amistco Separation Products, Inc.

Summary of the Case

The appellate court held that "The requirements of Rule [of Civil Procedure] 683 are mandatory and must be strictly followed." The injunction order here violated the mandate of Rule 683 that orders "shall be specific in terms."

The Covenant

Lasser, a salesman for ACS, signed a covenant which prohibited him — for two years after his termination — from (a) copying or using for his personal benefit ACS' "confidential information," and (b) soliciting "sales of competing goods to customers of ACS." Thereafter, ACS sold its assets, including Lasser's covenant, to Amistco, a company which makes metal separation and connection products. He became one of its salesmen. He resigned 15 months later and went to work for a new employer which then opened a division Amistco considered to be a competitor.

The Lawsuit and Injunction

Amistco made a forensic examination of Lasser's company-owned laptop and concluded that he had accessed confidential information before he resigned. Amistco sued him for breach of contract, misappropriation of trade secrets, and other misconduct. The company obtained a preliminary injunction which directed Lasser to cease using, and to return, all of Amistco's "confidential information and trade secrets," without specifying what intellectual property was encompassed. In addition, the order prohibited him from deleting any files or communications from any electronic device in his possession, regardless of whether the files or communications relate to allegations of wrongdoing. Finally, he was enjoined from soliciting any of Amistco's customers. Lasser appealed.

Reversal

The appeals court held that the injunction order violated Rule 683 by "failing to identify, define, explain, or otherwise describe" what proprietary data Lasser was directed to return. The purpose of Rule 683's specificity requirement for injunctions "is to ensure that parties are adequately informed of the acts they are enjoined from doing and the reasons."

The injunction also was faulty because it compelled him to refrain from deleting his personal electronic records unrelated to the litigation. Moreover, the injunction was improper because it prohibited all solicitation of Amistco's customers whereas the restrictive covenant precluded only solicitation of orders for competing goods.

CopyPro, Inc. v. Musgrove

Summary of the case

Restrictive covenants prohibiting employees from associating with a business rival of the employer in a vast geographic area for three years after termination were unenforceable.

The Non-Compete Agreement

CopyPro, a company primarily engaged in leasing office equipment in 33 North Carolina counties, required its employees to sign a nondisclosure agreement and a covenant not to compete. The covenant prohibited the employee from having any connection with a CopyPro competitor operating anywhere in those 33 counties. Musgrove was a CopyPro salesman whose customers were almost exclusively in just two of the 33 counties.

The Lawsuit, Injunction, and Reversal

When Musgrove resigned and became employed by a competitor, CopyPro sued him and obtained a preliminary injunction that encompassed the entire territory referenced in the covenant. The Appellate Court held that entry of the injunction order constituted reversible error. It "far exceeds [restrictions] necessary to protect [CopyPro's] legitimate business interests" since the company had no right to restrain Musgrove "from working in a capacity unrelated to that in which" he previously was employed.

Takeaways

Care should be taken not to over-reach when drafting confidentiality, non-compete, and non-solicitation covenants, and when filing motions for injunctive relief to enforce the covenants. There is a societal benefit in enforcement of contracts, but courts will invalidate covenants that serve only the interests of the person or entity seeking enforcement without regard to the public interest or interests of the person or entity resisting enforcement. The longer the covenant's duration, the wider its territorial restriction, and/or the more extensive its limitation on activities, the less likely it is to be enforced. Over-reaching can lead not only to an adverse court ruling but also to expense and generation of ill will among the parties.

Beware: Over-Inclusive Non-Compete Agreement May Be Unenforceable

By Paul Freehling (March 21, 2014)

An employment agreement non-competition provision stated that, for 18 months after termination, the employee shall not become employed by or act "directly or indirectly, as an advisor, consultant, or salesperson for, or become financially interested, directly or indirectly, [in an entity] engaged in the business of selling flavor materials." Earlier this month, the North Carolina Court of Appeals held that the provision was ***impermissibly broad***. *Horner Int'l Co. v. McKoy*, Case No. COA 13-964 (N.C. App., Mar. 4, 2014).

Summary of the case

McKoy, a plant manager in North Carolina, was a party to an employment agreement with Horner, a manufacturer of flavor materials for use in food and tobacco products. The agreement contained non-competition and trade secret confidentiality clauses. McKoy had been in the food processing and flavor industry for decades. He resigned after six years with Horner and went to work in New Jersey for a company that manufactured food and beverage flavoring items. Horner sued him and sought preliminary injunctions with respect to both clauses. Earlier this month, the trial court's ruling — denying the motion for an injunction with respect to the non-compete but granting the injunction motion relating to the confidentiality provision — was affirmed on appeal.

The appellate court's rulings

The appeals panel stated that it was guided by the familiar rules that employee covenants not to compete are disfavored but are enforceable if they are no broader than necessary to protect the employer's reasonable business interests. The non-competition covenant here had no geographic limitations and was not restricted to performance of tasks similar to those McKoy performed for Horner. Further, the covenant purported to prohibit him from associating with any company selling flavoring materials even if that company's products did not compete with Horner's. Finally, because he was precluded from investing "directly or indirectly" in such a company, the appellate court concluded that the non-compete was intended to prevent him even from owning shares in a mutual fund that was a Horner stockholder. For all of these reasons, the court held that the covenant exceeded permissible boundaries.

The injunction relating to the confidentiality clause, however, was upheld. North Carolina law permits injunctions for actual or threatened misappropriation of trade secrets the employee knows and has the opportunity to use or disclose. McKoy had access to Horner's trade secrets. By averring "with great detail and specificity the information Defendant has allegedly provided to his new employer," Horner met the "sufficient particularity" pleading standard.

Takeaways

Trading Secrets

Non-compete covenants must be limited in scope not only with respect to time and geography, but also concerning the activities which are prohibited. Horner teaches that an employer's use of virtually limitless phrases such as "directly or indirectly" and "financially interested" can be risky. Also, purporting to extend the covenant to services beyond those actually performed for the employer, and locales where the employee did not work, may doom the enforceability of the non-compete. Violation of a confidentiality clause may be enjoined, however, if the employee's access to the employer's trade secrets is demonstrated, they are described in sufficient detail, and the likelihood the employee may exploit or divulge the confidential information is shown.

Ohio Court Issues Significant Non-Compete Decision: Damages for a Breach are the Payor's Lost Profits, Not the Amount of Consideration

By Paul Freehling (April 23, 2014)

The usual measure of monetary damages for violation of a covenant not to compete, even where the violator was paid a discreet sum for the covenant, is the amount that puts the injured party in the same position it would have been in if the contract had been performed. *Briggs v. GLA Water Management*, 2014 Ohio 1551 (Ohio App., Apr. 11, 2014).

Summary of the Case

In November 1999, Briggs sold GLA, an industrial water treatment company he owned, to Hamrick, a long-time and high-ranking GLA employee. Briggs executed a covenant not to compete with GLA in Ohio, Indiana or Michigan for 15 years. As consideration for the covenant, the company promised to pay him $3,500 per month from January 2000 through December 2014. Hamrick guaranteed GLA's promises to make these payments. After a few years, payments for the non-compete allegedly stopped. Briggs sued GLA and Hamrick for breach of contract. GLA counterclaimed, asserting that Briggs had violated the non-competition covenant and demanding damages equal to the contractual consideration for it. A jury determined that both GLA and Briggs breached their contracts, awarding approximately $119,000 to Briggs and $354,000 to GLA. The trial court entered judgment for GLA in the amount of the difference, approximately $235,000. On appeal, the judgment was reversed. The appellate court held that GLA was not entitled to damages because it produced no evidence that Briggs' breach injured the company.

Motions and Trial

In response to Briggs' summary judgment motion, GLA offered evidence of his competition but did not claim that his breach resulted in lost profits or other injury. Briggs denied competing but insisted that, in any event, there were no recoverable damages. He made the same argument in motions for a directed verdict at the close of the evidence, and for judgment notwithstanding the verdict or for a new trial after judgment was entered, but all of his motions were denied. Although recognizing that the measure of damages for breach of a non-compete agreement usually is lost profits, the trial judge ruled that there were triable issues of fact such as whether the parties intended the agreed-upon monthly payments to constitute the value of the non-compete clause. The judge also observed that, under Ohio law, when a contract is breached the innocent party may recover the contractual benefits received by the breaching party.

Appeal

The Court of Appeals held that there was sufficient evidence for a jury to find that Briggs breached the non-competition covenant, but the correct measure of damages was the sum which would put GLA in the position it would have been in if the contract had been performed, that is, lost profits. Here, "GLA

would not have been entitled to receive the money back that Briggs had been paid for his agreement not to compete if the contract had been performed." Since GLA had contracted to make the monthly payments, and there was no evidence that Briggs' misconduct injured GLA, it sustained no recoverable damages.

Takeaways

The covenant, which was executed by sophisticated business persons in conjunction with a sale of assets, seemingly did not unlawfully restrain trade — even though it had a 15-year term and a three-state geographical restriction — because it appears to have been no more restrictive than necessary to protect GLA's investment. In any event, Briggs did not protest the duration or area of the restriction. What was problematic, however, was the company's argument that the parties intended the monthly payments to be liquidated damages for Briggs' breach. First, that argument flies in the face of the fact that the contract did not express any such intention. Second, a liquidated damages clause must reflect a reasonable approximation of actual damages or else it may constitute an unenforceable penalty provision. Here, there was no evidence that Briggs' alleged violation of the covenant caused *any* injury to GLA, much less the more than $350,000 GLA was awarded. The parties' agreement might have provided explicitly that if there was difficulty proving actual damages for a breach of the covenant, a specified modest sum would be payable to GLA.

Sometimes in contract violation cases involving no provable substantial injury or loss, *nominal* damages are awarded. A nominal damages award to GLA here might have been upheld on appeal.

Massachusetts Moves to Ban Non-Competes – Dawn Mertineit Explains What Employers Should Do Now

By Dawn Mertineit (April 28, 2014)

https://www.youtube.com/watch?v=C_qa4Y9PiPs

As we discussed on the blog not too long ago, Massachusetts Governor Deval Patrick recently introduced legislation that would eliminate virtually all employee non-compete agreements, with a few minor exceptions. On April 23, Dawn Mertineitspoke with LexBlog's Colin O'Keefe in a live online interview to discuss what this proposed legislation could mean for employers with Massachusetts operations. Specifically, Dawn noted critics' and opponents' differing views as to the value of non-compete agreements should Massachusetts adopt the Uniform Trade Secret Act, and also offered some tips for employers seeking to protect themselves should the bill pass (and even if it doesn't).

Unemployment Compensation Awarded To Ex-Employee Refusing Employer's Order To Execute Non-Compete Covenant

By Paul Freehling (May 1, 2014)

Don't want to sign that new non-compete agreement that your employer just rolled out? Unemployment compensation may be an option at least according to one new court decision.

An employee does not necessarily forfeit unemployment compensation if he or she is discharged, or resigns rather than waiting to be discharged, for declining to sign a mandated restrictive covenant. *Darr v. Roberts Marketing Group, LLC*, MO Court of Appeals, Eastern District, Case No. ED100197 (Apr. 22, 2014).

Summary of the Case

Darr, an insurance salesman, had been working for Roberts Marketing for three months when he and all other employees were told that continued employment was contingent on signing a non-competition agreement. They were given less than a week after being provided with a copy of the agreement to execute it or be discharged. Darr consulted with an attorney who advised him not to sign. Roberts Marketing refused to negotiate the terms, and so Darr refused to execute the agreement. Faced with imminent termination, he resigned and filed for unemployment compensation. A hearing officer concluded that Darr was entitled to receive benefits, but the Labor and Industrial Relations Commission reversed on the ground that he had voluntarily left his employment. On appeal to the Missouri Court of Appeals, the Commission's decision was reversed.

The Covenant

Darr argued that the covenant was onerous with regard, for example, to its duration, geographical area covered, and scope of activities. It prohibited employees, for 36 months after the cessation of employment, from engaging "directly or indirectly . . . in any manner" in the telemarketing of life insurance anywhere in the U.S. and all of its territories. The 36-month term did not begin to run until the date the employee stopped violating the agreement. In the event of an actual or threatened breach, the company was entitled to "apply to any Court of competent jurisdiction for entry of an immediate restraining order or injunction."

The agreement also stated that the employee agreed to waive all defenses and objections to the terms and conditions of the covenant, promised not to advance any contrary position, and waived trial by jury. An employee found to have committed a violation would be required (a) to pay the company, as "liquidated damages, and not a penalty" all sums the employee received, "directly or indirectly," as a result of the violation, and (b) to reimburse the company for all costs and expenses, including reasonable attorneys' fees, incurred in enforcing the agreement.

Court of Appeals Decision

According to the Court of Appeals, Darr was a "reasonably prudent" employee who was justified in declining the "mandatory acceptance of contractual conditions" which would unduly constrain his ability to earn a living, and would invite future lawsuits. The court also noted that Darr demonstrated good faith by attempting, albeit unsuccessfully, to negotiate the terms of the covenant with his employer. The court suggested that, in connection with seeking unemployment compensation, an employee might be justified in quitting if the employee reasonably believes that termination will result for refusing to execute a non-compete agreement mandated by the employer, even if the agreement does not contain egregious terms.

Takeaways

The most important lesson the *Darr* case teaches is that an employer who threatens to fire employees who refuse to sign a restrictive covenant may be liable to them if they in fact are discharged, or even if they resign, and then claim unemployment compensation.

Hiring Employees with Non-Compete Agreements: Tread Lightly

By Sarah Izfar (May 6, 2014)

Excited about the prospect of a talented new hire and think that her non-compete doesn't affect you? Think again. Under Virginia law, a future employer, who is aware of a prospective employee's non-compete agreement, risks legal liability for tortious interference of contract and, through that, business conspiracy.

"Upset at you for breaching the non-compete? Of course not."

In *DePuy Synthes Sales, Inc. v. Jones*, 2014 WL 1165852 (E.D. Va. Mar. 21, 2014) (adopting magistrate's report and recommendation in 2013 WL 8118533 (E.D. Va. Nov. 5, 2013)), the Eastern District of Virginia recently applied Virginia law to deny a motion to dismiss claims of tortious interference of contract and statutory business conspiracy on the grounds that the future employer knew of the existence of the non-compete agreement and nonetheless proceeded to hire two salespersons in a capacity that would require them to violate their non-compete agreements.

Case Background

DePuy Synthes Sales, Inc. ("DePuy") employed two salespersons, Michael Jones and Jacob Schools, to market DePuy's line of orthopaedic medical devices to doctors. Both men left DePuy and began working with Sky Surgical, Inc. ("Sky Surgical"), a competitor, in violation of their non-compete agreements. DePuy filed a complaint alleging, in part, Sky Surgical's tortious interference with Jones and Schools' non-compete agreements and statutory civil conspiracy under Virginia Code Sections 18.2-499 and 500.

Tort of Tortious Interference

The court denied Sky Surgical's motion to dismiss this claim. Under Virginia Law, to state a claim for tortious interference, DePuy only had to plead four elements: (1) existence of a valid contractual relationship or business expectancy; (2) knowledge of the relationship on the part of the interferor; (3) intentional interference inducing or causing a breach or termination of the relationship; and (4) damage to the party whose relationship was disrupted.

The critical issue here was whether the contract was terminable at will. If a contract is terminable at will, Virginia also requires that the interference be accomplished by "improper methods," like bribery or fraud. However, whether a contract is terminable at will is not always clear cut. In another case, the Virginia Supreme Court has explained that the extent of permissible third party interference increases as the degree of enforceability of a business relationship decreases. Here, the court looked to the non-compete agreement, not the customer relationships with doctors (which were admittedly at will) to determine whether improper methods must be plead. Because the non-compete agreements were not terminable at will, DePuy was not required to plead "improper methods."

Business Conspiracy

Under Virginia Code Section 18.2-499 and 500, injured parties can recover **treble damages** for conspiratorial conduct performed for the purpose of "willfully and maliciously injuring another in his reputation, trade, business or profession by any means whatever." The conduct of the conspirators must be considered unlawful. In a recent case, *Dunlap v. Cottman Transmissions Systems, LLC*, 754 S.E.2d 313 (2014), the Supreme Court of Virginia resolved a long-standing ambiguity, holding even though breach of contract is not sufficient to constitute an "unlawful act," tortious interference with contract and tortious interference with business expectancy do each constitute the requisite "unlawful act" to proceed on a statutory business conspiracy claim. Therefore, by adequately pleading tortious interference with contract, DePuy was also able to plead statutory business conspiracy against Sky Surgical.

Takeaway

No matter how excited an employer may be about a prospective hire, when non-compete agreements come into play, an employer must carefully analyze the applicable terms of the non-compete and seek the advice of legal counsel **before** extending the offer. Likewise, a former employer may have two possible causes of action against the employer that pilfered its employees.

Bob Stevens Reflecting On Georgia's Non-Compete Law at its Third Anniversary

By Bob Stevens (May 15, 2014)

https://www.youtube.com/watch?v=mDp68Hi7L2Y

Georgia's restrictive covenant statute turns three years old this week and Seyfarth Shaw partner Bob Stevens offers insight into the significant changes in the law and how Courts are interpreting those changes. The legal changes are not only significant but anecdotal evidence from trial courts reflects that at least some trial courts view the change in law as an almost bright line regarding whether employment related restrictive covenants are enforceable in Georgia. Please also see some of our previous coverage on this important change in Georgia law.

Employee's Competition With Former Employer Restricted Despite Absence Of Signed Non-Compete

By Paul Freehling (May 21, 2014)

The former employer failed to prove that the parties entered into an effective non-compete agreement, and also failed to prove that the ex-employee had disclosed or had threatened to disclose trade secrets. But, an Ohio federal judge entered a preliminary injunction forbidding her, until further order, from contacting her former employer's clients and certain of its prospects. *PharMerica Corp. v. McElyia*, Case No. 1:14-CV-00774 (N.D. Ohio, May 9, 2014) (Gwin, J.).

Summary of the Case

McElyia was one of several salespersons employed by PharMerica, a provider of pharmacy products and services to skilled nursing facilities. At the time she became a PharMerica employee, she covenanted to keep its client information confidential. She never signed a non-competition agreement. On the eve of her resignation, she downloaded to her personal computer extensive PharMerica documents. Then she went to work for a competitor as its sole salesperson. PharMerica sued her and her new employer. She quickly returned the PharMerica documents. But PharMerica nonetheless sought a TRO and preliminary injunction to prevent both defendants from competing with PharMerica. The court denied PharMerica's motions directed at McElyia's new employer and the motion for a TRO against McElyia. But after holding an evidentiary hearing on the preliminary injunction motion directed at her, the court enjoined her until after a trial from contacting PharMerica's clients or any prospective clients she had called on during her final six months of employment by that company. The injunction was conditioned on PharMerica posting a $50,000 bond.

Non-Compete Injunction without a Non-Compete Covenant

Judge Gwin concluded that there was insufficient evidence of an effective non-competition covenant. PharMerica had asked McElyia to sign one. It provided that she would not work for a competitor for six months, and would not solicit current clients and employees for one year, after her termination. However, she declined to execute it.

The judge found that when she took the PharMerica documents she intended to share them with her new employer, but he added that there was no evidence that she did disclose, or was threatening to disclose, PharMerica's trade secrets. Judge Gwin said that McElyia had not solicited any of PharMerica's clients.

Although the phrase "inevitable disclosure doctrine" does not appear in Judge Gwin's opinion, perhaps it was a basis for entering the injunction. He stated that "some Ohio courts do permit injunctions in the absence of a non-compete agreement and without a prior instance of disclosure" of trade secrets. He cited only one decision. While no injunction was entered in that case, the court there did reference (but distinguished) several "inevitable disclosure" cases.

Courts typically find "inevitable disclosure" only when there is a high probability, not a mere possibility, that trade secrets will be revealed. Usually, (a) the parties executed a non-compete covenant, and/or (b) the ex-employee had disclosed or destroyed, or at least had threatened to disclose or destroy, confidential information. Not so in *PharMerica*. Further, injunctions to prevent "inevitable disclosure" of confidential information despite the absence of a non-compete covenant usually pertain to engineering data or technical manufacturing processes rather than mere marketing information as in*PharMerica*.

Curiously, the opinion in *PharMerica* does not suggest the presence of either of two factors some courts have used to justify entering an "inevitable disclosure" injunction:

(a) the former employer went to considerable lengths and expense to develop the purloined information and to keep it confidential; and

(b) the ex-employee was a high-level executive for the former employer.

Takeaways

The facts and circumstances present in *PharAmerica* would more often warrant *denial* of an injunction against competition rather than justifications for entering one. If the court was relying on the "inevitable disclosure" doctrine at all, it seems to have been treated as a *de facto* (partial) non-compete covenant even though the parties did not agree to one. Moreover, the description of the "confidential" PharMerica information McElyea supposedly possessed was extremely general: "pricing, contract terms, and marketing and product packaging strategies." If the court intended to enjoin its use, more specific and identifiable data would have been required so that McElyia knew precisely what she was forbidden to disclose.

Significantly, the injunction did not order McElyea to refrain from using PharMerica's trade secrets. It simply circumscribed the universe of prospective clients she could contact.

In the end, PharMerica may have achieved a pyrrhic victory. Judge Gwin's preliminary injunction is unlikely to be long-lasting, and the company has been required to post a rather large bond. Perhaps the court simply intended to send a message to the parties that failure to resolve the case amicably could entail substantial risk.

Divided Appellate Court Voids Employer's Non-Compete Covenants Because One Employee Did Not Sign

By Paul Freehling (June 18, 2014)

In a decision marked not-for-publication, a Minnesota Appeals Court affirmed the trial court's invalidation of a two-year non-competition agreement signed by a long time employee. He was discharged 11 years after he signed. He then went to work for a competitor of his former employer. The majority reasoned that the non-compete lacked independent consideration since it was not executed by 100% of similarly situated employees who had been asked to sign it.

Summary of the Case

In April 1999, Nott Company (a supplier of fluid-power components and systems) notified all outside salespeople by letter that the company would be implementing a new compensation program effective May 1, 1999. That program, which included a two-year non-compete covenant replacing a one-year agreement, added the possibility of a bonus to the prior salary-plus-commission arrangement. The letter directed each recipient to sign and return the covenant by April 30. All of the outside salespeople except one executed the new, longer term agreement. In 2010, Nott discharged Eberhardt, a signer of the two-year covenant, who went to work for a Nott competitor. Nott sued Eberhardt and his new employer. At trial, at the close of Nott's case, the court entered judgment for the defendants partially on the ground that Eberhardt's non-compete was invalid. The judgment was affirmed on appeal. *Nott Co. v. Eberhardt*, Case Nos. A13-1060 and 1390 (Minn. App., 6/2/14) (Hudson, J.) (Stauber, J., dissenting).

The Signers and Non-signers

Prior to 1999, all of Nott's outside salespersons were signatories to one-year non-competition agreements. One of those signatories, Cable, signed in 1995. Eberhardt did not become an outside salesman until 1999.

All of the outside salespersons, except for Cable, executed the new two-year covenant. The date Eberhardt signed was disputed. Nott claimed he signed in April 1999, before the new program went into effect on May 1. He insisted that he did not sign until September 1999.

The Lower Court and Appellate Decisions

The trial court found three reasons for tossing Nott's case. The appellate tribunal unanimously held that the lower court erred with respect to two of those reasons, but the third, lack of independent consideration, was upheld by a 2-1 vote.

a. Opinion of the Court of Appeals majority: The majority emphasized that Minnesota courts disfavor and scrutinize non-compete covenants. Relying largely on a 1983 Minnesota Supreme Court

decision (*Freeman v. Duluth Clinic, Ltd.*, 334 N.W.2d 626), the majority said that Eberhartdt's covenant was not supported by independent consideration. They reasoned that since Cable, the non-signer, was given the same new compensation package as all the signers, the "court cannot find that an employee's signing of the non-compete agreement was a condition of receiving the compensation plan."

b. The *Freeman* case: *Freeman* involved a medical clinic. A 1979 employment contract replaced an earlier, nearly identical, agreement but added a non-compete covenant. All of the physicians received the same benefits. Of the 70 physicians in 1979, only 56 — including Dr. Freeman — signed the covenant. In 1982, the clinic fired Dr. Freeman, and he started his own private practice. The clinic sued and won at trial. With two justices dissenting, the Supreme Court reversed, holding that the provision was unenforceable for lack of consideration. The majority wrote: "[T]he covenant signed by Dr. Freeman was not bargained for. Absolutely no distinction was made between [the 56] signers and [the 14] non-signers."

c. Judge Stauber's dissent in *Eberhardt*: Judge Stauber quoted the comment by the dissenting justices in*Freeman* that there was "a mutuality of promises, which has always been held to be adequate consideration in contract cases." He noted that Nott's and Eberhardt's employment relationship under the new contract lasted more than a decade, with benefits to each, before he was terminated. The judge added that 14 physicians in *Freeman*, not just one outside salesman in *Eberhardt*, failed to execute the covenant. Finally, Judge Stauber stated that "a holding that one-hundred percent of all similarly situated employees must execute a non-compete agreement for its viability is not commercially practical in a free and competitive society."

Takeaways

A recent *New York Times* article reported that judges appear to be getting annoyed by a seeming avalanche of non-competition violation lawsuits, and many covenants are being invalidated. Perhaps annoyance was an under-current of the*Eberhardt* decision. In any event, the lessons to be learned are that, when a current employee is asked to sign a new covenant, (a) to be safe an employer should give something valuable in exchange (in *Eberhardt*, the opportunity to receive a bonus was new; nothing new was given in *Freeman*), and (b) the covenant should recite just what the consideration is. On the other hand, some courts hold that employment itself may be adequate consideration for a covenant signed prior to starting work.

Enforcing Non-Compete Agreements in the Pharmaceutical Industry

By Katherine Perrelli and James McNairy (June 19, 2014)

Employee mobility in the pharmaceutical industry is a significant concern for employers given the industry's very significant investment in and reliance upon generating and protecting confidential, proprietary and trade secret information that is used to develop products and create and maintain customer relationships.

Non-competition and customer non-solicitation agreements are one of the primary tools available in most states to protect proprietary information and customer goodwill. Whether non-compete/customer non-solicit provisions are enforceable often turns on whether such provisions seek to protect legitimate employer interests (such as proprietary information and customer goodwill) and are of a reasonable geographic scope and duration.

This blog post is the second in a series about protecting trade secrets and enforcing non-competition agreements in the pharmaceutical industry, and focuses on the role non-competition and customer non-solicitation agreements may play in the industry.

I. Timing is Important

Like any contract, non-compete agreements are potentially effective only if they are operative when needed. The three most frequent employment events that employers should keep in mind when using non-compete agreements are (1) employee onboarding; (2) significant changes in job duties for existing employees; and (3) when exiting an employee that has been terminated or has resigned. Although these timing considerations are important regardless of industry, they are particularly applicable in the pharmaceutical industry because of the intellectual property-intensive nature of the industry and significant numbers of personnel devoted to the research and development function. R&D personnel sometimes are overlooked as a population to which non-competes should apply given their often "inward facing" responsibilities when compared to their executive, business development, marketing, and sales counterparts within the organization.

Onboarding is critical for two reasons: (1) It is the best time to ensure that a new employee will be subject to a non-compete and doing so at the inception of employment often dispenses with any arguments as to whether or not the non-compete is supported by sufficient "consideration," as the vast majority of states that allow non-competes find that non-competes entered into at the inception of employment are supported by adequate consideration (the restriction on the employee is made in exchange for employment, compensation, being provided company confidential information etc.); and (2) It is another opportunity to confirm with new employees whether they are subject to an existing non-compete entered into with a prior employer. Ideally, the topic of the potential existence of a non-compete will have come up in and have been addressed in the interview process, but addressing this subject again in the onboarding process is an opportune time to discuss with a new employee any

restrictions placed on him/her via a non-compete with a prior employer, particularly if the prior employer is a competitor within the pharmaceutical industry.

Significant changes in job duties, such as a promotion or moving into a significantly different role, are an opportunity to provide the company better protections for employees subject to an existing non-compete that has become outdated due the passage of time and/or change in law. Many, but not all, states that enforce non-compete agreements recognize that "continued employment" is sufficient consideration to support the use of a non-compete agreement. For those states where continued employment is not regarded as sufficient consideration, changes in job duties may present an opportunity to provide additional consideration in the form of a raise, grant of stock options, a bonus etc. that may, depending on one's particular jurisdiction, enhance the likelihood that a non-compete will be enforceable. In the pharmaceutical industry, job changes such as a move from bench scientist to manager or an executive position are examples of job changes that may afford the company with an opportunity to enhance its non-compete protections and spot and address any potential issues with "consideration" in imposing a new non-compete.

Exiting employees is a critical time to remind employees of their non-compete obligations and for the company to revisit any specific provisions within the non-compete that require awareness or action on the company's part. A proper exit interview is critical and may reveal that the exiting employee is going to a competitor or that the employee expressly denied going to a competitor only to later be discovered that the denial was disingenuous. Learning at the employee's exit that she/he is going to a competitor may also trigger "clawback" or "forfeiture" provisions within agreements. *Smythe v. Raycom Media, Inc.,* Case No. 1-13-CV-12 (CEJ) (E.D. Mo., Aug. 15, 2013) (because former employer's Board was vested with discretion to determine former employee's eligibility under the stock plans, the Board's decision to effect forfeiture of stock unredeemed by former employee cannot be overturned unless the Board acted fraudulently or in bad faith); see also *Lenel Systems Int'l., Inc. v. Smith*, 106 A.D. 3d 1536, 966 N.Y.S.2d 618 (N.Y. App. Div. 2013) (where employee voluntarily terminates employment and joins competitor, company's decision to effect forfeiture of employee's unexercised stock options enforceable because employee had choice between compliance with non-compete or retention of stock options). The intellectual property-intensive nature of, and prevalent use of stock options/grants within the pharmaceutical industry make adoption of employee non-compete exiting best practices essential. This also counsels in favor of careful drafting of forfeiture or clawback provisions within non-compete agreements as the law as to these provisions can vary significantly from state to state.

II. One Size Fits All Agreements May Make For Easier Agreement Administration, But Beware of Outliers

Employers, particularly large employers, often gain efficiencies in administering uniform non-compete/non-solicitation agreements across employee types. But like other technology-based industries, the pharmaceutical industry should take care to evaluate whether a one size fits all agreement is appropriate in light of (1) the often very diverse make-up of pharmaceutical company employee types (e.g., sales, executive, research and development), and (2) the core elements that nearly all jurisdictions consider when determining the validity of such agreements: (a) geographic scope, (b) duration, and (c) whether the restriction is reasonable (protects a legitimate business interest, such as protecting confidential information and/or company goodwill).

A non-compete agreement with a geographic scope tied to those areas where a pharmaceutical sales representative has actually called upon or served customers may be perfectly appropriate, whereas the same type of restriction would be insufficient to protect the company's interest when applied to a senior executive or scientist within the company R&D group. For example, if the employee subject to the restriction has been working to develop the company's next potential blockbuster drug and/or is a

senior business development executive, a relatively broad geographic scope may be called for and tolerated, depending on the state in which one seeks to enforce the agreement. *See, e.g., Estee Lauder Companies Inc. v. Batra*, 430 F. Supp. 2d 158, 180-81 (S.D.N.Y. 2006) (upholding worldwide non-compete where scope of business and former employee's responsibilities were international and included exposure to and use of trade secrets). Although worldwide non-competes are rare and difficult to justify, the nature of the proprietary information at issue and scope of the duties of the person subject to restriction are important considerations when drafting restrictive covenants.

The takeaway is that pharmaceutical companies should be purposeful in their use and tailoring of non-compete agreements to help ensure that those within their organizations who present the greatest risk in terms of capitalizing on company proprietary information and goodwill are subject to appropriate non-compete agreements, where permitted under applicable law.

III. Enforcement Best Practices–Planning and Pursuit

There are several things that employers within the pharmaceutical industry can do to enhance the likelihood that their efforts to enforce non-compete agreements are successful. Planning on the front end through use of reasonable agreements and then taking appropriate action when a potential breach is detected will go a long way toward protecting company interests. Specifically:

1. Use agreements that are up to date and contain appropriate restrictions based on the law of the jurisdiction in which you contemplate potentially enforcing the agreement;

2. Recent case law has potentially enhanced the enforceability of forum selection clauses. *See, e.g., Atlantic Marine Const. Co., Inc. v. U.S. Dist. Court for W. Dist. of Texas*, 134 S. Ct. 568 (2013). Consider designating the jurisdiction and law most favorable to enforcement of your agreements;

3. Set up communication channels so that the appropriate personnel are aware of when high-risk employees are leaving (e.g., R&D talks to HR, HR talks to Legal, Legal talks to IT)

4. Conduct thorough exit interviews, including ascertaining whether the former employee may be joining a competitor and in what capacity;

5. Determine risk level based on employee type, job duties, and exposure to proprietary information. Log items that should be and were/were not returned (e.g., electronic devices, inventor's notebooks, etc.);

6. Where former employee refuses exit interview or is otherwise evasive, consider running forensics on electronic devices to potentially ascertain if former employee is going to a competitor and whether she or he has taken any company data on the way out the door; and

7. Create a record of your diligence: exit interview checklists and certifications; reminder of obligations letter(s); and cease and desist letters (former employee and, as appropriate, new employer). However, balance "making a record" with tipping your hand and allowing the employee to get the jump on litigation by filing first in a non-desirable jurisdiction.

Florida Court Finds That Employer Without Knowledge That Employees It Just Hired Have Non-Competes Are Not Liable For Tortious Interference With Contract

By Paul Freehling (July 9, 2014)

A defendant company was unaware, when it hired two individuals, that they had entered into non-competition agreements with their prior employer. As a result, according to a Florida federal court, the prior employer did not have a valid cause of action against the new employer for intentionally interfering with those non-compete obligations.

Summary of the Case

During their employment by Aerotek, a recruiting company, Zahn and Jiminez signed non-compete covenants. Shortly after termination of their Aerotek employment, they allegedly violated the covenants by going to work for that company's competitor C-T. Aerotek sued C-T for tortious interference with contract. C-T responded by moving to dismiss on the ground that it did not know about the covenants when it hired the two ex-Aerotek employees. The motion was granted. Aerotek, Inc. v. Zahn, Case No. 6:14-cv-293-orl-31TBS (M.D. Fla., 6/17/14).

The Court's Rationale

The court reasoned that to state a claim for tortious interference, Aerotek was required to prove that C-T intentionally interfered with Zahn's and Jiminez's covenants at the time they supposedly committed a breach of contract. However, the court said, the employees breached when C-T hired them, and that occurred several months before C-T learned about the covenants. At that time, CT lacked the requisite intent to interfere with the contracts. What occurred thereafter may have been a continuation of injuries and damage, but it was not a continuing tort. In the court's words, Aerotek "conflates the moment of the breach with the period of the injury."

The court relied on a case concerning the date the statute of limitations began to run on a trade secret misappropriation claim against the new employer who allegedly received the former employer's confidential information from a new hire. The ruling there was that the misappropriation occurred the day the ex-employee started working for the new employer. What occurred later were the effects of that one act, not a continuing tort.

Takeaways

The ruling in *Aerotek*, if generally followed, seemingly would provide some cover for an employer ignorant with regard to its hires' non-compete covenants. Vaguely reminiscent of the military's former "don't-ask-don't-tell" policy, on its face *Aerotek*suggests that the new employer may benefit from not questioning a new hire concerning the existence of a non-compete with a prior employer. But the

strategic decision by the new employer not to seek that information before making a job offer, and not to assess the risks before investing time and money in the new hire, can be perilous if the new hire did promise not to compete.

First, even if the former employer does not sue its successor, the former employer may file a complaint against the new hire for torts and breach of contract. Any such lawsuit almost certainly will be distracting to both the new hire and the new employer, and will be expensive for one or both. Second, a court order might be entered enjoining the new hire from competing, which could result in an inability (at least temporarily) to perform all or part of the job for which he or she was employed.

Third, the prior employer may make claims against the new employer which are held to state valid causes of action. If tortious interference is alleged, the court might not follow the lead of the *Aerotek* judge and dismiss the allegations. Moreover, the complaint may allege misconduct other than or in addition to tortious interference. Fourth, if a lawsuit is filed against the new employer and/or the new hire, bad publicity may result regardless of the outcome in court. The better course usually will be to inquire sooner rather than later regarding non-compete obligations that a prospective hire may have.

Eleventh Circuit Affirms Alabama Federal Court Ruling that Non-Compete Signed Prior to Employment is Void

By Daniel Hart (July 14, 2014)

A few months ago, we reported on a federal court decision in the Southern District of Alabama declining to enforce a non-compete and non-solicitation agreement against a former employee who executed the agreement ***before*** he began his employment. Last week, a panel of the Eleventh Circuit affirmed the District Court's decision in anunpublished opinion.

As we reported following the District Court's decision, in*Dawson v. Ameritox, Ltd*., 2014 WL 31809 (S.D. Ala. Jan. 6, 2014), Ameritox, a healthcare company, sought to enforce non-compete and non-solicitation covenants against its former Assistant Director of Medical Science and Health Outcomes Research, Dr. Eric Dawson, who had left Ameritox for a similar position with a competitor. Although Ameritox sought a preliminary injunction against Dawson, the District Court denied the motion and ruled that the covenants in question were void and unenforceable because Dawson had executed the agreement before his employment with Ameritox began. Under Alabama Code § 8-1-1, a contract by which anyone "is restrained from exercising a lawful profession, trade, or business of any kind" is void, except that "one who ***is employed*** as an agent, servant or employee may agree with his employer to refrain from carrying on or engaging in a similar business and from soliciting old customers of such employer within a specified county, city, or part thereof, so long as the . . . employer carries on a like business therein." Relying on the Alabama Supreme Court's prior decision in *Pitney Bowes, Inc. v. Berney Office Solutions*, 823 So. 2d 659 (Ala. 2001), the District Court noted that employee non-compete agreements are valid only if signed by an employee and that prospective employment is not sufficient to meet the exception in Section 8-1-1. Thus, because Dr. Dawson was not an employee of Ameritox at the time he signed the agreements, the District Court reasoned that the agreements were void and unenforceable.

In its unpublished opinion affirming the District Court's decision, the Eleventh Circuit agreed with the District Court, noting that Ameritox's attempts to distinguish *Pitney Bowes* were unpersuasive. The Eleventh Circuit reasoned that, because the agreement was void under Alabama Code § 8-1-1, Ameritox failed to show a substantial likelihood of success on the merits. Thus, the District Court did not abuse its discretion in denying Ameritox a preliminary injunction.

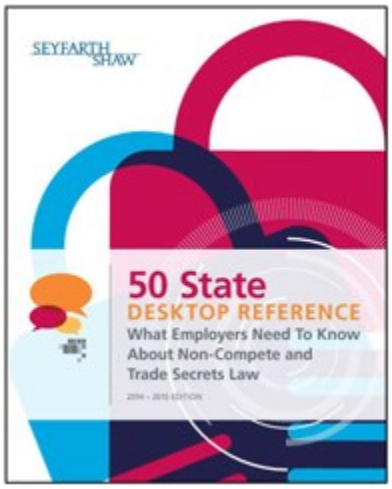
The Eleventh Circuit's panel decision reaffirms the importance of practical pointers we noted in our prior post. While it is prudent — and, in some states, required — to provide prospective employees with copies of required non-compete agreements before the employee's first day of work, employers in Alabama should ensure that employees execute (or re-execute) such agreements on or after their first

day of employment, ideally in the presence of a representative of human resources. In addition, because continued at-will employment is sufficient consideration for new restrictive covenants in Alabama, employers with operations in Alabama should consider periodically reviewing their existing restrictive covenants and requiring employees to execute new agreements from time to time as appropriate.

Seyfarth Offers 2014-2015 Edition of 50 State Desktop Reference: What Employers Need to Know About Non-Compete and Trade Secrets Law

By Robert Milligan (July 17, 2014)

What Employers Need To Know About Non-Compete and Trade Secrets Law



There is no denying that there exists a variety of statutes and case law across the country when it comes to employee non-competition and non-solicitation agreements, as well as the protection of proprietary information. All too often, what is enforceable in one state may be questionable in another and entirely prohibited in the next.

Seyfarth's Trade Secrets, Computer Fraud & Non-Competes Practice Group has created a one-stop Desktop Reference surveying many of the questions related to the use of employee covenants and intellectual capital protection in all fifty states. For the company executive, in-house counsel or HR professional, we hope that this booklet will provide a starting point to answer your questions about protecting your company's most valuable and confidential assets.

How to get your Desktop Reference:

This publication may be requested from your Seyfarth contact or Trading Secrets editor Robert Milligan (rmilligan@seyfarth.com) in hard copy or is available as an eBook, which is compatible with PCs, Macs and most major mobile devices*. The eBook format is fully searchable and offers the ability to bookmark useful sections for easy future reference and make notes within the eBook. To request the 2014-2015 Edition of 50 State Desktop Reference as an eBook, please click the button below:

Rebecca Woods on Recent Kentucky Supreme Court Decision Holding that Non-Compete Failed for Lack of Consideration

By Rebecca Woods (July 22, 2014)

In a recent ruling by the Supreme Court of Kentucky, *Creech v. Brown* (June 19, 2014), the court affirmed that in Kentucky, noncompetition agreements must be supported by adequate consideration in order to be enforceable. The circumstance addressed by the court involved an employee who was presented with a noncompetition and confidentiality agreement after working for the employer for 16 years. The employee was offered no payment, no change in employment terms, and was not threatened with termination if he failed to execute the agreement. The court held that under this set of facts there was a lack of consideration and the court deemed the agreement unenforceable. The ruling makes clear that while consideration is necessary, it may be deemed from after-the-fact changes in employment circumstances.

https://www.youtube.com/watch?v=fJFu9cJ3llk

Liquidated Damages, A Permanent Injunction, and Attorneys' Fees Awarded For Violating Non-Disclosure/Non-Compete Agreement And Preliminary Injunction

By Paul Freehling (July 31, 2014)

In a well-written recent opinion concerning violation of both a confidentiality/non-compete agreement and a preliminary injunction, a federal judge explained in detail why she was awarding liquidated damages, entering a permanent injunction, and assessing legal fees.

Summary of the Case

Two financial planners, one an individual and the other a corporation, negotiated a merger of their businesses. Before being provided with details concerning the corporation's methodologies and strategies, the individual executed confidentiality and non-competition covenants. When the merger negotiations collapsed, the financial planners went their separate ways. However, the corporation subsequently sued the individual for breach of the covenants. A preliminary injunction was entered against her which, after a trial, she was found to have violated. The court entered an order of contempt, issued a permanent injunction, and awarded the corporation liquidated damages and attorneys' fees. *Retiree, Inc. v. Anspach*, No. 12-2079-JAR (D. Kan., 7/2/14) (Robinson, J.).

Merger Negotiations

Diana Anspach and Retiree, Inc. each had financial planning practices. Both financial planners were accomplished in the business, although their approaches were different. They entered into merger negotiations in the course of which she signed the covenants. They included a $250,000 per violation liquidated damages clause. Retiree disclosed to her its algorithms, formulas, and software trade secrets developed over the course of several years in a collaboration with engineers and mathematicians. After the merger negotiations failed, she enhanced her planning tools in a manner that seemed, in part, to mimic some of those furnished to her in confidence by Retiree.

The Lawsuit

In a complaint filed against Anspach, Retiree alleged that she was violating the covenants by (a) using Retiree's confidential information in competition with Retiree, and (b) disclosing that information in a book and on her website. Retiree demanded liquidated damages, preliminary and permanent injunctions, and an award of fees.

Preliminary and Permanent Injunctions

Following a hearing, Judge Robinson granted Retiree's motion for a preliminary injunction against disclosure and competition. Subsequently, after conducting a bench trial, the judge found that Anspach had violated the preliminary injunction, held her in contempt of court, and issued a permanent injunction. Anspach argued that the liquidated damages clause was unreasonable. Judge Robinson disagreed, determined that Retiree's damages were irreparable and incalculable, and awarded Retiree $500,000 in liquidated damages. Further, the court set the matter for a hearing to determine the amount of attorneys' fees to be awarded to Retiree.

Takeaways

Retiree succeeded in obtaining an award of liquidated damages, entry of a permanent injunction, and a finding of contempt of court, by making a focused presentation of evidence and argument addressed to an attentive and articulate jurist. Judge Robinson's opinion contains an excellent discussion of the circumstances, in litigation concerning an alleged breach of confidentiality and non-competition covenants, which may warrant the relief she awarded. If you seek a similar judgment, or are opposing an adversary's effort to obtain such relief, this opinion should be studied in great detail.

Seyfarth Attorneys Present on Latest Developments in Trade Secrets and Non-Compete Law At ABA Annual Meeting

By Kate Perrelli and Robert Milligan (August 7, 2014)

Seyfarth partners Robert Milligan and Kate Perrelli will lead a CLE program for the ABA IPCentral Conference during the ABA's Annual Meeting in Boston on August 7th.

They are scheduled to be joined by in-house counsel Pamela Davidson from U.S. Foods, Karen Tompkins from Stryker, Lisa Seilheimer from CDW, and Jerry Cohen from Burns & Levinson LLP.

The panel will discuss recently passed trade secret legislation in Texas, New Jersey, and other jurisdictions, as well as the recent efforts to create a federal civil cause of action for trade secret theft and the recent attempt to ban non-compete agreements in Massachusetts. They will also discuss significant non-compete decisions in Illinois and Kentucky regarding the required consideration for non-competes. Panelists will also review recent cases on forum selection/choice of law, pleading standards, identification requirements, summary judgment, and damages.

Best practices for protecting trade secrets and risks to proprietary information, as well as the latest cases addressing reasonable secrecy measures will also be addressed.

The ABA-IPL Trade Secrets Committee will also provide the audience with its annual 2013/2014 survey of the latest developments in trade secrets and non-compete law.

For more information about the program, please click here.

If you are in Boston, please come over for what is sure to be a great program.

Appellate Court Orders Trial Judge To Rewrite Parties' Non-Compete Covenant To Make It Enforceable

By Paul Freehling (August 27, 2014)

An asset purchase and sale agreement included unusual non-competition provisions. They authorized a court to redo any time, scope and area restrictions held to be unenforceable.

The North Carolina Court of Appeals held that the covenant's territorial restriction was overbroad. Notwithstanding the state's "strict blue pencil doctrine," which limits a judge's authority to revise a non-compete clause, the appellate court directed the trial judge to rewrite the invalid restriction and then to try the issue of whether the clause was violated. *Beverage Systems of the Carolinas, LLC v. Associated Beverage Repair, LLC*, No. COA 14-185 (N.C. App., 8/5/14) (Hunter, J., joined by McGee, J.; Elmore, J., dissenting).

Summary of the Case

In connection with a purchase and sale of two companies, the parties executed a five-year non-competition, non-solicitation and confidentiality agreement. Subsequently, the purchaser sued the sellers in a North Carolina court, alleging that they were violating the non-compete covenant and engaging in other wrongdoing. Without giving any specific reasons, the lower court granted the defendants' motion for summary judgment. A few days ago, in a 2-1 decision, the appellate tribunal reversed, remanded, and directed the trial judge "to revise the territorial area of the non-compete to include" only those areas where the acquired companies had customers at the time of the transaction. The appellate court also held that the plaintiff presented evidence showing genuine issues of material fact which precluded summary judgment.

The Asset Sale

Beverage Systems was organized in 2009 to provide and service beverage dispensing equipment, and to sell beverage products. In September of that year, the company bought the assets of two entities engaged in those activities. The purchase price included $10,000 specifically for the non-compete covenant.

The Covenant

The agreement of purchase and sale provided that, for the earlier of five years or "such other period of time as may be the maximum permissible period of enforceability," the sellers shall not have any involvement with a North or South Carolina company engaged in the same business as the purchaser. Although not mentioned by the appellate court, the agreement (a copy of which is in the record on appeal) also stated that the parties believe the restrictions as written "are reasonable and necessary to protect the [purchasers'] legitimate business interests" and "are not overbroad, overlong or unfair."

Further, the parties consented (a) to substituting "automatically" the maximum reasonable period, scope and geographical area for any stated period, scope or area "held to be invalid, illegal or unenforceable in any respect," and (b) to allowing a court "to revise the restrictions contained [in the covenant] to cover the maximum period, scope and area permitted by law."

North Carolina's "strict blue pencil doctrine"

A judge in that state is permitted, but not required, to alter "a distinctly separable part of a [restrictive employment] covenant in order to render the provision reasonable." However, a jurist "may not otherwise revise or rewrite the covenant."

The Trial Court's Decision

The parties' briefs in the trial court focused on the question of whether the territorial restrictions were reasonable. Without expressly answering that question, the court entered summary judgment for the defendants and explained only that the decision was based on "review of the file, the Briefs . . . and upon consideration of oral argument of counsel for all the parties."

The Appellate Decision

The appellate tribunal's majority concluded that the broad territorial restriction, encompassing some areas where the sellers had not been engaged in business, was invalid. Citing *Outdoor Lighting Perspectives Franchising, Inc. v. Harders*, 747 S.E.2d 256 (N.C. App. 2013), a case not mentioned by the parties in any brief in the trial or appellate courts, the majority said that the purchase and sale agreement as written rendered the "strict blue pencil doctrine" inapplicable. Accordingly, the trial judge was ordered "to revise the non-compete provisions after determining where in North Carolina and South Carolina it would be reasonable to enforce" those provisions. Then, "once the trial court revises the non-compete to include only those areas reasonably necessary to protect plaintiff's business interests," that court must decide whether the covenant has been violated.

The *Outdoor Lighting* Case

The majority said *Outdoor Lighting* construed "similar language" and indicated "a willingness of our Courts to recognize and enforce revised non-compete agreements when the parties contract for the right to" make revisions. There, a franchise agreement gave the *franchisor* "the right to modify the non-competition provision" by reducing its scope. The franchisor attempted to exercise that right, but the propriety of this "private 'blue penciling'" was not adjudicated because, even as modified, the provision was held to be unreasonable.

Judge Elmore's Dissent in *Beverage Systems*

Judge Elmore expressed his opinion that *Outdoor Lighting*provides no basis for the *Beverage Systems* majority to direct "the trial court to undertake the revising and rewriting of the non-compete." He stated that *Outdoor Lighting*"addressed a franchisor's (a party to the non-compete), . . . right to modify a non-compete outside the scope of a business sales contract." That case, he said, was distinguishable. It did not concern an assets purchase and sale transaction, did not involve a contractual provision allowing a non-party to revise a non-competition clause, and did not reflect an appellate tribunal's direction to a trial judge to rewrite the clause.

Judge Elmore continued: Under the blue pencil doctrine, a "trial court has the authority to *enforce* portions of a non-compete that are reasonable and disregard the remaining portions if the non-compete

divides the restricted area into distinct units. While the non-compete in the case at bar divides the restricted territory into North Carolina and South Carolina, . . . neither of those restrictions taken separately [is] reasonable." Further, he disagreed with the majority's conclusion that there were material disputed issues of fact. Thus, in his view, summary judgment for the defendants was proper.

Takeaways

The *Beverage Systems* contract contained the parties' stipulation that they considered the non-competition, non-solicitation, and confidentiality provisions to be reasonable and that, if invalidated, they should be salvaged to the maximum extent possible. The contract also stated that a court could redo the duration, territory, and scope of prohibited activities clauses to the extent they were determined to be illegal. The lesson learned is that, in the instance of a non-compete in a purchase and sale transaction, **careful drafting** might serve to persuade a judge to rewrite an unreasonable provision. This result could be achieved notwithstanding a "strict blue pencil doctrine" which, as Judge Elmore wrote, "drastically restricts a court's authority to modify" an unlawful restriction.

Ten-Day Interruption In Employment Necessitates New Non-Compete

By Paul Freehling (September 12, 2014)

An employee who had executed a two-year non-compete was let go. He returned to work 10 days later but was not asked to sign a new agreement. More than two years after his return, he was terminated and became an employee of a competitor. A lawsuit seeking to enforce the non-compete was dismissed on the ground that it had expired.

Summary of the Case

Helmuth, like all employees of Nightingale Home Healthcare, signed a non-competition covenant with a term of two years from the date of termination. He was fired in mid-October 2009 but was recalled 10 days later. He was not asked to sign a new covenant. In March 2012, his employment with Nightingale ended, and he went to work for a competitor. Nightingale sued him and his new employer, but the trial judge entered summary judgment for the defendants. On appeal, the judgment was affirmed. The appellate court held that the covenant's restriction ended in mid-October 2011, two years after his first termination by Nightingale and five months before he was employed by the competitor. *Nightingale Home Healthcare, Inc. v. Helmuth*, No. 29A04-1403-PL-121 (Ind. App., 8/28/14).

The parties' perception of what occurred in October 2011

Nightingale pointed out that Helmuth returned to the same job position at the same salary, with the same benefits, and without being required to reapply or complete any paperwork. The company characterized these events as a revocation, rescission and voiding of his first termination. Helmuth claimed that there was no continuity because he had been discharged and subsequently was rehired.

The Appellate Court's Ruling

Stressing that Helmuth was required in mid-October 2009 to turn in his company-owned laptop, identification badge, and keys, his access to company property came to an end, and he was not paid for those 10 days, the appellate tribunal held that he had ceased to be a Nightingale employee. The court wrote: "[B]ased on the evidence, Nightingale's conduct is more properly defined as a separation from the company which was unconditional and intended to operate as a permanent termination of the employment relationship between Nightingale and Helmuth." (Although not cited by the Indiana court, a 2013 unpublished New Jersey appellate court ruling — *Truong, LLC v. Tran*, Docket No. A15752-1171 — involved similar facts and reached a similar result.)

Nightingale argued that, by returning to work on the same terms and conditions, Helmuth impliedly acquiesced to an extension of the non-compete. The court of appeals held that this argument was

inconsistent with the clause “no modifications, extensions, amendments, or waivers of this Agreement or any of its provisions shall be binding unless in writing and signed by” a Nightingale officer. The court also said there was no ambiguity in the covenant, and so parol evidence concerning the parties’ intentions was inadmissible.

Takeaways

The appeals tribunal stressed that Indiana courts respect freedom to contract, but that non-compete covenants in an employment agreement are restraints on trade, are not favored, must be strictly construed against the employer, and are enforced only if reasonable (many other states concur). Where there is a break in service but no relevant express contractual provision, an employer’s safest course is to obtain a new covenant upon the employee’s return. Alternatively, a contention that employment was continuous could be supported (a) as in Helmuth’s case, by reinstating the same position, salary and benefits, (b) especially where the employee was not employed during the break, by compensating as if there had been no interruption, and (c) by written confirmation that all of the prior contractual terms and conditions, including the non-compete, remain applicable.

Non-Compete and Forum Selection Clauses in Franchise Agreement Binding on Franchisee Who Signed It and on His Wife Who Didn't

By Paul Freehling (September 23, 2014)

A Florida franchisee executed a franchise agreement (FA) containing a non-compete provision and a Pennsylvania forum selection clause. Following termination of the FA, the former franchisee's wife opened a similar business in another part of Florida. The franchisor filed suit in Pennsylvania against the former franchisee and his wife, and they moved to dismiss or, alternatively, to transfer the case to Florida. The motion was denied. *AAMCO Transmissions, Inc. v. Romano*, Civ. Ac. No. 13-5747 (E.D. Pa., 8/21/14).

Summary of the Case

An AAMCO Transmissions FA prohibited competition by the franchisee within 10 miles of any AAMCO franchise for two years from the date of termination. The FA required that any litigation regarding the FA take place in Pennsylvania where AAMCO is headquartered. Prior to expiration of the FA, the franchisee and AAMCO entered into a termination agreement. It gave the franchisee a complete release except with respect to a few identified surviving provisions such as the non-compete, but the forum selection clause was not mentioned. Shortly after termination, the franchisee's wife opened a competitive shop 100 miles from the former shop but approximately two miles from another AAMCO franchisee. AAMCO sued the franchisee and his wife in Pennsylvania. Without success, they asserted that the forum selection clause did not survive the termination, that the covenant's geographic restriction was unreasonable, and that venue was inconvenient.

Applicability of the Non-Compete and Forum Selection Clauses to a Non-Signatory

Robert, the franchisee, owned and operated an automotive maintenance and repair shop in Hollywood, Florida. After the FA was terminated, his wife Linda opened a similar shop in Stuart, Florida, less than 10 miles from another AAMCO franchise. In support of their motion to dismiss, Robert and Linda contended that he did not own or operate her shop, and she did not sign the non-compete. The court cited several cases holding that a non-signatory to a covenant who is "closely related" to a signatory is entitled to the agreement's benefits but also bound by its obligations. Moreover, (a) AAMCO alleged that Linda was Robert's agent in his franchised business in Hollywood, and (b) documents attached to the complaint indicated that they jointly own and operate the Stuart facility. At the motion to dismiss stage, the trial judge said, it must be assumed that Linda also is subject to the covenant.

Survival of the Forum Selection Clause

The termination agreement contained a broad release with only a few specified exceptions. One was the non-compete. However, since the forum selection clause was not listed as an exception, the defendants argued that it did not survive the termination. The trial judge disagreed. She cited a half-dozen cases from around the country holding that if a non-compete continues after a contract

termination, a forum selection clause does as well. Further, the dispute obviously related to the FA which stated expressly that any legal "proceedings which arise out of or are connected in any way with this Agreement" must take place in a Pennsylvania court. Finally, the judge observed that there was no evidence of a clear intent to make the clause inapplicable.

Geographic Restriction

Under Pennsylvania law, according to the judge, "Unreasonableness of the geographic scope of a non-compete is an affirmative defense on which the [defendants] bear the burden of proof." Further, "because reasonableness is a fact-intensive inquiry, it should not be determined on the pleadings unless the unreasonableness is clear from the face of the complaint." Decisions within the Eastern District of Pennsylvania are split concerning the reasonableness of AAMCO's 10-mile restriction. So, the court denied, without prejudice to renewal later, the motion to dismiss based on that restriction.

Inconvenient Forum

The defendants pointed out that they were appearing *pro se* because they could not afford a lawyer, and that litigating in Pennsylvania would be prohibitively expensive. They emphasized that the relevant events occurred, and the witnesses and records are located, in south Florida. That argument failed to carry the day because of the forum selection clause, the FA's choice of Pennsylvania law, and the location of AAMCO's headquarters. The judge said the financial burden on the defendants litigating in Pennsylvania is no greater than the burden on AAMCO if it must litigate in Florida.

Takeaways

Not surprisingly, persons who are "closely related" to the signer of a non-compete can be held equally bound by it. Further, the judge's conclusion that venue was *proper* in Pennsylvania, because AAMCO is headquartered there and the FA selected Pennsylvania as the forum state, was predictable.

More significant is the court's refusal to transfer the case to Florida. This case teaches that a court may choose to deny defendants' well-supported motion to transfer to a "more convenient forum" where the plaintiff chooses to sue in the state referenced in a contractual forum selection clause and has a significant relationship with that state.

Competitor Avoids Injunction Because Competition Was Not Significantly Aided And Abetted By A Signatory To Non-Compete

By Paul Freehling (September 26, 2014)

In a recent Texas federal court ruling, a competitor closely aligned with, and seemingly assisted by, a signatory of a non-compete covenant narrowly avoided a preliminary injunction because the assistance was not shown to have been substantial.

Summary of the Case

In connection with the purchase and sale of a partnership's assets, a partner of the seller signed a covenant which provided that, for five years, he would not participate in a business competitive with the seller anywhere in or adjacent to the county where the seller's business was located. Shortly thereafter, a company owned by the signatory's wife commenced competition in that territory. Alleging that the signatory was aiding and abetting the competitor, the assets purchaser sued the signatory, the signatory's wife, and others. The purchaser's motion for entry of a preliminary injunction was granted solely against the signatory. It was denied as to the remaining defendants because the purchaser was held to have failed to meet its burden of demonstrating that the signatory ***significantly*** aided and abetted competition. *Henson Patriot Ltd. Co., LLC v. Medina*, Civ. Ac. No. SA-14-CV-534-NB (W.D. Tex., Sept. 11, 2014) (Rodriguez, J.).

The Defendants

Andrew Medina was a partner of, and the signatory for, the seller. For 15 months after the transaction, he was employed by the purchaser Henson Patriot Ltd. in production and then in sales. His wife Clara and her future business partner were lower level employees there. They were not signatories. The three of them — Andrew, Clara and her future partner — resigned from Henson more-or-less simultaneously, and almost immediately Clara (with her partner) set up a company within the territory of the non-compete. Both Henson and Clara's company were specialty commercial printers. When Clara's company took several good Henson customers who Andrew had serviced, Henson sued Clara's company and the three individuals for violating the non-compete. The defendants maintained that Andrew played no role in Clara's company. However, messages found on his phone at Henson after he left, various emails, and other evidence strongly suggested that he had been involved with "the launch and conduct" of that company.

The Covenant

In addition to the provisions relating to its duration and territory, the covenant stated that Andrew "shall not either directly or indirectly . . . engage, [consult] with, advise or otherwise participate in any business that is in competition" with the seller.

The Court's Ruling on Plaintiff's Motion for a Preliminary Injunction

The defendants contended that the length of the term, the breadth of the area encompassed by the non-compete, and the activities prohibition were unreasonable, but the court disagreed. Previous Texas decisions in asset sales cases upheld similar provisions. Concluding that "The facts are approaching enough to show Andrew Medina significantly aided, abetted, and consulted with the other defendants," Judge Rodriguez entered the injunction against Andrew, the signatory. More problematic was Henson's effort to enforce the non-compete against the non-signatory defendants.

The judge stated that Texas law would "allow an extension of Andrew Medina's non-compete to entities or persons he significantly aided, abetted, consulted, or advised to compete with Plaintiff." Clara, her company, and her partner insisted that Andrew's involvement was inconsequential. Judge Rodriguez responded that he was "not convinced Andrew Medina did not aid, consult, or advise [Clara's company and its principals, but] the Court exercises caution at this time due to the extraordinary nature of a preliminary injunction." The Court added that Henson "has not shown enough for the Court to conclude Andrew Medina *significantly* aided, consulted, or advised the other defendants." Emphasis the court's. Therefore, as to those defendants, the court held that "Plaintiff, at this time, has failed to establish a substantial likelihood of success on the merits."

Takeaways

Henson teaches that, in order to obtain a preliminary injunction against an alleged violator of a non-compete covenant, an employer may have to prove that the violation but, in addition, that the violation was not trivial, at least in this Texas court. The hard evidence presented by the plaintiff, rebutted only by the defendants' denials, seems to have indicated that Andrew did what the non-compete prohibited. But almost every time Judge Rodriguez referred to the covenant's prohibition against "aiding, abetting, consulting, and advising," he added the modifier "significantly" (once in italics) although that word is not found there. Thus, he construed the covenant as implicitly precluding only extensive violations. Perhaps he was influenced by the legal principle set forth in a few cases — none of which were cited — that aiding and abetting the commission of a tort is actionable only if the assistance is "substantial."

Customer Non-Solicitation Covenant Runs From Date Employment With Asset Seller Terminated, Not From Later Date Employment With Asset Purchaser Ended

By Paul Freehling (October 20, 2014)

An employee executed an employment agreement which included a two-year covenant not to solicit the employer's customers. When the employer sold the company's assets, the sale included that agreement. The employee then went to work for the assets purchaser but subsequently resigned. The Texas Appellate Court held that the two-year period began to run on the date the assets seller ceased to be the signer's employer. *Lasser v. Amistco Separation Products, Inc.*, No. 01-14-00432-CV (Tex. App. Court, Oct. 2, 2014).

Summary of the Case

The employment agreement between Lasser and the assets seller, ACS, included a confidentiality provision as well as the non-solicitation covenant. Lasser worked for the assets purchaser, Amistco, for 15 months and then resigned, accepting a job with its alleged competitor. Amistco sued and sought a preliminary injunction. The trial court's first injunction order was dissolved by the Texas Court of Appeals because of a lack of specificity. After the lower court issued a more detailed order, the appellate tribunal affirmed as to confidentiality but dissolved the non-solicitation injunction, holding that the covenant expired two years after Lasser left ACS' employ.

Chronology

Lasser's employment with ACS terminated on February 29, 2012. He went to work for Amistco the next day and remained employed by that company until June 1, 2013. He immediately went to work for Woven Metal Products which assigned him to head a new division that allegedly competed with Amistco.

Amistco's Lawsuit and First Injunction Motion

Amistco promptly sued Lasser, claiming that he was about to violate the confidentiality provision and non-solicitation covenant in his ACS employment agreement. Amistco moved for entry of a preliminary injunction against Lasser's (a) solicitation of Amistco's customers, and (b) use of Amistco's trade secrets and confidential information. The trial court entered the injunction, and Lasser appealed.

Two Appeals

Early in 2014, the appellate court reversed the injunction order on the ground that it was insufficiently specific (*Lasser I*). Amistco then moved for entry of a more detailed preliminary injunction which the trial court entered. Lasser appealed again. Last week, the appellate court affirmed the injunction order

insofar as it related to confidentiality but reversed the remainder of the order, holding that the non-solicitation clause lapsed on March 1, 2014 (*Lasser II*).

The holdings in *Lasser II*.

(a) *The holding regarding the non-solicitation clause.* The appeals court held that Lasser covenanted with ACS not to solicit its customers for two years after termination of his employment. By the time *Lasser II* was decided in October 2014, the non-solicitation prohibition had expired and no longer was enforceable.

(b) *The holding regarding the confidentiality clause.* After Lasser left Amistco, that company retained a computer forensics expert to analyze Lasser's company computer to determine whether he had downloaded any of Amistco's trade secrets. The expert concluded that Lasser had taken with him more than 1000 confidential Amistco files. On appeal, Lasser denied that the files contained secret data. He also challenged the second injunction as insufficiently specific.

The first injunction restrained Lasser simply from "using, . . . [or] directly or indirectly disclosing, copying or otherwise reproducing, or giving others access to any of [Amisco's] confidential information and trade secrets." Commenting in *Lasser I* that "the order neither defines nor in any manner indicates from its context the meaning of the phrase 'confidential information,'" the Court of Appeals held that the injunction was "not sufficiently clear to provide Lasser with adequate notice of what acts he is compelled to complete and what conduct he is restrained from performing. In other words, he is left to speculate what conduct might satisfy or violate the order. This is impermissible."

The trial court's second injunction identified two dozen categories of "confidential information and trade secrets" that were the subject of the order. In *Lasser II,* the Court of Appeals held that "The specific examples of the items comprising 'trade secrets' and 'confidential information,' when read in the context of the suit, provided Lasser with adequate notice of the information that he is prohibited from using or disclosing."

Takeaways

Assignment of Lasser's employment agreement provided Amistco (a) a cause of action to prevent his disclosure of confidential information, but (b) no defense against his post-termination solicitation of Amistco's customers. In order to protect against such soliciting, apparently, Amistco would have had to obtain its own covenant from Lasser.

Non-Compete And Non-Solicitation Covenants Contained In Bovine Artificial Insemination Employment Agreements Held Unenforceable

By Paul Freehling (October 28, 2014)

Several ex-employees now may compete with their former employer, and may solicit its employees and customers, after a federal judge in the Eastern District of Washington held that the restrictive provisions in their employment agreements are unenforceable.

The agreements, drafted by the former employer, contained a choice-of-law provision which the former employer tried unsuccessfully to invalidate. The court also held that a low-level at-will employee's non-compete covenant lacked sufficient consideration to be enforceable where all he received for signing it was a job offer. *Genex Cooperative, Inc. v. Contreras*, Case No. 2:13-cv-03008-SAB (Oct. 3, 2014) (Bastian, J.).

Summary of the Case

Genex was in the business of, among other activities, inseminating dairy cows and marketing bovine semen. Four of its employees resigned and the next day began servicing its customers on behalf of its competitor. Genex filed a complaint against all four, seeking in part to enforce non-competition covenants signed by three of the four defendants and non-solicitation covenants signed by two of the four. The court invalidated all of the covenants on the ground that they were unnecessary in order to provide reasonable protection to Genex or were otherwise contrary to applicable law.

Choice of Law Provision in Defendant Verduzco's Agreement

The employment agreement signed by Verduzco stated that it was governed by Wisconsin law (Genex is incorporated there). Although the provision was drafted by Genex, the company argued that the court should apply the law of the forum, Washington, for three reasons: (a) Verduzco worked there both for Genex and, subsequently, for its competitor, (b) he signed the agreement there, and (c) Wisconsin law violated "a fundamental policy" of Washington because its judges have the power to blue pencil otherwise unenforceable contracts whereas Wisconsin jurists are not permitted to do so. Judge Bastian held that judicial discretion to blue-pencil is a "general rule of contract law" in Washington, not "a fundamental policy." Therefore, the agreement's designation of Wisconsin law is enforceable.

Covenants Not to Do Business with Genex Customers

Defendant Contreras' non-compete agreement prohibited him, for one year after termination, from doing business with any Genex customer with whom he had had contact during the 18 months prior to his leaving Genex. Judge Bastion held that Genex failed "to meet its burden to establish reasonableness of the covenant." He noted that "Contreras — who cannot read or write in English — was a low-level agricultural worker with an at-will employment relationship with Genex." The question of

"Whether non-compete agreements can ever be enforceable against at-will employees, without providing specific consideration such as a promise for future employment or training, is an open question in Washington." However, both nationwide and in Washington, a covenant with "an at-will employee who did not have unique or professional skills" is unlikely to be deemed reasonable.

Verduzco's covenant prohibited post-termination solicitation of anyone from whom he had *sought* new or increased business in the last 18 months of his Genex employment. The court observed that this prohibition forbad him from soliciting prospects who placed no orders with him during those 18 months, and that such a covenant is unenforceable under the law applicable to his agreement, that of Wisconsin.

Defendant Senn's agreement restricted him, for 18 months after termination, from engaging "in either the artificial insemination of cattle or the sale of semen in the area in which [he] has been employed [by Genex] and rendered service." Because, once again, even local dairy farms not previously serviced by Genex were out of bounds, the court held that the covenant was not "necessary for the protection of Genex's business or goodwill."

Covenants Not to Solicit Genex's Employees

The non-solicitation clause in Verduzco's employment agreement directed him not "to induce or attempt to induce" any Genex employee to terminate his or her employment with Genex. Judge Bastian stated that under Wisconsin law a "no-hire" prohibition like that is invalid because it constitutes "a 'harsh and oppressive' restriction on the rights of an employee."

Contreras' agreement committed him not to "directly or indirectly encourage any Genex employee to terminate his/her employment with Genex." The company admitted that this provision was intended to prohibit him from seeking to "inspire" employees to leave Genex's employ. The court held this restriction was unenforceable, especially since his "decision to terminate his at-will employment may have *inspired* the other defendants with the courage to quit as well." Emphasis added.

Takeaways

The *Genex* opinion deals with and resolves a variety of issues. It teaches that the draftsperson of a rational choice of law provision in an employment agreement has an uphill battle trying to avoid it. Further, the opinion tells us that employers should be wary of trying to enforce covenants signed by low-level employees or those without separate, meaningful consideration. Finally, restrictive employment covenants are less likely to be enforced if they are intended to expand the prohibitions beyond those necessary to provide the former employer with reasonable protection.

Trading Secrets

Non-Compete And Confidentiality Clauses In A Beverage Maker's Contracts With A Bottler And A Consultant Held To Be Unenforceable

By Paul Freehling (November 25, 2014)

Courts will decline to enforce contractual restrictive covenants in agreements that unreasonably restrain trade or lack adequate consideration.

Summary of the Case

Innovation Ventures (IV), developer of an energy drink, entered into contracts with a bottler and with a production consultant. Both contracts contained non-compete and confidentiality clauses. Shortly after the bottler's and consultant's business relationships with IV ended, IV sued them, together with their principals, in a state court in Michigan for breach of contract. The trial court granted summary judgment to the defendants. Recently, that decision was affirmed on appeal on the grounds that the agreement with the bottler unreasonably restrained competition, and the contract with the consultant lacked adequate consideration. *Innovation Ventures, L.L.C. v. Liquid Mfg., L.L.C.*, Case No. 315519 (Mich. Court of Appeals, Oct. 23, 2014) (unpublished).

The Parties and the Contracts

The bottler. In 2007, pursuant to a contract with IV, Liquid Manufacturing commenced bottling IV's "5 Hour Energy" using the bottler's own equipment. Three years later, the bottler, by its principal, and IV executed an agreement terminating that contract. The termination agreement permitted Liquid Manufacturing to use the equipment for bottling other producers' products (a) if IV gave its consent, and (b) provided that the other producers covenanted not to disclose that the equipment had been used for bottling "5 Hour Energy." Post-termination, Liquid Manufacturing sued the bottler and its principal for breach of contract.

The consultant. In 2008, IV entered into an oral agreement with a consultant company to design, manufacture, and install certain production and packaging equipment for IV. The agreement was memorialized in writing for the first time in 2009. Less than two weeks later, IV exercised its right to end the relationship without cause. IV then sued the consultant and its managing member for violating the restrictive covenants.

The Appellate Tribunal's Decision

1. The appeals court ruled that the bottler's principal, who executed the termination agreement as an agent of the corporation, could not be sued for breach of contract because he did not sign on his own behalf.
2. Although the bottler may have failed to obtain the covenant described above, any such violation was held to have been cured in a timely manner.

3. IV's attempt in the termination agreement to reserve to itself virtually unfettered discretion to decide which products Liquid Manufacturing could bottle constituted an unreasonable restraint on trade. A provision reflecting the bottler's stipulation that the termination agreement was reasonable was held to be void because courts, not the parties, determine whether contracts are unreasonable.
4. The confidentiality clause in the termination agreement was held to be waived by expressly authorizing the bottler to use supposedly confidential information in order to bottle competing products.
5. Consideration for the contract between IV and the consultant was the parties' implied promises to continue their relationship for a reasonable period of time. IV's cancellation after less than two weeks was held to have nullified the contract.

Takeaways

This decision teaches that restrictive covenants in commercial contracts are not always enforceable. Just as with a comparable provision in an employment agreement, a non-compete clause in a commercial contract must be no more protective of a manufacturer's good will than is reasonably necessary. In other words, unfair competition may be restrained, but not fair competition. The ruling also shows that purported consideration in a commercial contract must not be illusory. Absent an express contractual provision to the contrary, a court may decline — for want of adequate consideration — to enforce a non-compete covenant in a contract which the non-covenanting party terminates without cause almost immediately after execution.

Court Thwarts Employer's Effort To Block Vested Profit-Sharing Plan Participant from Obtaining Employment with a Competitor

By Paul Freehling (December 8, 2014)

Other than to protect good will or trade secrets, a non-compete provision intended to prevent a former employee from acquiring an interest in, or becoming an officer or director of, a competitor of the ex-employer may not be enforceable.

Summary of the Case

A stand-alone agreement executed by employee-participants vested in their employer's profit-sharing plan contained an unusual non-compete provision. It prohibited participants, for five years after termination, from owning or becoming an official of a "similar" trade or business located within 25 miles of the employer's facility in Columbus, Nebraska. A participant resigned his employment and sought from a Nebraska state court a declaration that the provision was an unreasonable restraint. The trial court entered the requested judgment order, and the employer appealed. A few weeks ago, the Nebraska Supreme Court affirmed. *Gaver v. Schneider's O.K. Tire Co.*, 289 Neb. 491 (Nov. 14, 2014).

The Covenant

The express purpose of the non-compete provision was to assure that profit-sharing plan participants did not use plan benefits "to the detriment of the Employer." Participants were permitted to become mere employees of a competitor but not to be officers, directors, or owners of a financial interest.

The Decision Below

The trial court reasoned that the provision would prevent ex-employees from engaging in any form of competition. In that court's view, the covenant provided greater protection to the employer than was necessary.

The Decision on Appeal

The appellate tribunal affirmed. It held that while an employer may legitimately seek to preserve its good will and confidential information, that was not the goal of this restrictive covenant. Instead, it was intended to limit the use employees could make of their own funds, earned and already received.

Takeaways

This decision conceivably could have broad implications for future lawsuits involving non-competes and profit-sharing plans at least in Nebraska, but more likely it will be limited to its peculiar facts. For example, the appellate tribunal declined to decide whether the employer could have enforced the non-compete provision if it had been included in the profit-sharing agreement rather than in a stand-alone document. Nor did that court state whether what it called the "time and space" of the non-compete, five years and 25 miles from the employer's place of business, were valid (however, the court did include a citation to a Nebraska deferred compensation case holding that a "4- to 5-year time restriction contained in [a] forfeiture-for-competition clause" was unreasonably long). Finally, there was no ruling as to the meaning, much less the legality, of the prohibition's purported scope (restrictions applicable to businesses "similar to" that of the employer).

No Stick Without a Carrot: UK Court Refuses to Enforce Post-Employment Restrictive Covenants

By Razia Begum (December 16, 2014)

The recent decision of the High Court in *Re-use Collections Limited v. Sendall & May Glass Recycling Ltd.* serves as a useful reminder for employers: restrictive covenants introduced during the employment relationship (rather than at the point of hiring) require specific consideration if they are to be enforceable. Under UK law, changes to employment terms require consideration if they are to be relied on. The fact the employee keeps their job does not amount to consideration, unless the employee would genuinely have been dismissed if they did not agree. UK law would only rarely justify termination for failure to agree new post-termination restrictions.

It is good practice to periodically review restrictive covenants, to reflect the latest UK case law and any changes to the employee's role or the business. To give the best chance of enforcing restrictions, employers should however take care to link any new covenants to some form of benefit for the employee. This can be monetary (e.g. linking the new restrictions to pay review) or other benefit (e.g. a promotion) for existing employees. In the instant case, the continued employment of the employee was not considered a benefit, as there was no suggestion that the employee would have been dismissed if he refused to agree to the covenants.

Court Refuses To Enforce Settlement Agreement Containing Non-Compete Covenant Citing Lack of Assent

By Paul Freehling (December 23, 2014)

Plaintiff's motion to enforce a settlement agreement in principle was denied because some material terms of that agreement were not included in the version the plaintiff sought to enforce. *GeoLogic Computer Sys., Inc. v. MacLean*, Case No. 10-13569 (D. Mich., Dec. 10, 2014).

Status of the Case

Counsel for the parties to a software copyright infringement lawsuit purportedly reached an agreement in principle to settle the litigation. One of the material terms of the preliminary agreement was a status quo non-compete. However, the parties could not reach a consensus with respect to the wording. The plaintiff then settled with some of the defendants, deleting from that settlement any reference to a non-compete, and moved to enforce the old agreement in principle — minus the non-competition clause — against the non-settling defendants. They objected to the motion on the ground that they could not be forced to accept a compromise significantly different from the one to which they had acquiesced. The court agreed and denied the motion to enforce.

The Settlement in Principle

After three years of hard-fought pretrial litigation in a federal court in Michigan, the district court judge referred the case to a magistrate judge for settlement negotiations. In October 2013, the parties' attorneys informed the magistrate judge orally that they had an agreement. The judge directed them to recite on the record "the overarching terms," and they purported to do so. One was that two corporate defendants would pay approximately $1.5 million to the plaintiff over time, with the payments guaranteed by the individual defendant owners of those corporations. Another term was that certain other defendants who were salespersons — people the court referred to as the "Non-Compete Defendants" — would compete with those corporations only with respect to relationships already existing. The purpose of the covenant was to restrict the Non-Compete Defendants from interfering with the earning potential of those corporations to such an extent that they might be unable to liquidate their indebtedness to the plaintiff. The magistrate judge directed the attorneys to memorialize the settlement.

A Partial Settlement

Unfortunately, the parties were unable to achieve unanimity, but the plaintiff and the Non-Compete Defendants did reach agreement. They would pay the plaintiff $730,000. Reference to a non-competition covenant was omitted. The Non-Compete Defendants committed that they would — and they did — support the plaintiff's subsequent motion to enforce as against the non-settling defendants the settlement agreement in principle (minus, of course, the non-compete).

Objections

In their opposition to the motion to enforce, the non-settling defendants — the two corporations and their owners — contended that during settlement negotiations all parties had agreed that the non-compete was a material term, and no party had expressed any objection to it. Moreover, by protecting the corporations' income stream, the non-compete also served potentially to shield the individual guarantors from a default by the corporations which would trigger their own duty to pay. Also, the non-settling defendants pointed out that if payment in full was not made, the plaintiff might claim entitlement to valuable rights relating to the software, and those defendants wondered aloud whether the plaintiff might be surreptitiously promoting non-payment. In response, the plaintiff countered that the draft non-compete provision was solely for the plaintiff's benefit, to increase the likelihood that it would be paid, and therefore the non-settling defendants would not be prejudiced by deletion of that provision.

The Court's Decision

The trial judge agreed with the parties objecting to the motion to enforce. The settlement in principle was not identical in all material respects to the order the plaintiff sought to have entered. The court said that the subjective purpose of the omitted non-compete — here, supposedly to protect the plaintiff — is irrelevant. The defendants never agreed to a settlement without that provision, and so the court was precluded from granting the motion to enforce.

Takeaways

This case reminds us that a motion to enforce a "settlement agreement in principle" will be denied unless all parties assented to every significant term. Here, the agreement the plaintiff sought to enforce differed in several material respects — most notably, the deleted non-compete — from the settlement to which the parties purportedly had agreed several months earlier. Those differences doomed the contested motion to enforce.

Legislation

Breaking News: Massachusetts Governor Deval Patrick to Propose Legislation Eliminating Non-Compete Agreements in Certain Industries

By Erik Weibust and Dawn Mertineit (April 10, 2014)

The Boston Globe reported this morning that Massachusetts Governor Deval Patrick will propose legislation today that would eliminate non-compete agreements in technology, life sciences, and "other industries," with his secretary of Housing and Economic Development, Greg Bialecki, stating that the administration "feel[s] like noncompetes are a barrier to innovation in Massachusetts." No word just yet on what "other industries" might include.

While Governor Patrick had previously been more tempered in his views on non-compete agreements, his current position supporting the outright elimination of such restrictive covenants is hardly surprising in light of comments made by Bialecki at a hearing before the Massachusetts Legislature's Joint Committee on Labor and Workforce Development just seven months ago. At that hearing, on which we previously reported here, Bialecki foreshadowed today's move, stating that the Patrick Administration supported the outright elimination of non-compete agreements, stating that such agreements "stifle movement and inhibit competition."

While the proposed legislation has not yet been filed, the Globe has reported that it is modeled after California's ban on non-compete agreements, and that it will include a provision adopting the Uniform Trade Secrets Act (the "UTSA"). As we have previously noted here, Massachusetts is currently one of only a handful of states that has not adopted the UTSA.

More details to follow once the proposed legislation is publicly available, including what other industries may be affected by the administration's proposal. It is not often that you hear states wanting to be more like California particularly on labor and employment issues.

Update: Massachusetts Governor Proposes Sweeping Legislation Banning Non-Compete Agreements

By Katherine Perrelli, Erik Weibust, and Dawn Mertineit (April 17, 2014)

As we reported last week, Massachusetts Governor Deval Patrick has proposed sweeping legislation that would eliminate employee non-compete agreements in Massachusetts. Now that we have had an opportunity to review the Governor's bill, entitled "An Act to Promote Growth and Opportunity" (HB4045), we wanted to report back on its content and the implications should it pass. While the bill includes a number of proposed changes and additions to existing laws on a variety of subjects, two main provisions are of particular interest here.

Outright Elimination of Employee Non-Compete Agreements

First, as expected, the bill includes a provision that would invalidate *all* employee non-compete agreements in the Commonwealth.

In our last post on the topic, we wondered whether the proposed legislation would apply solely to non-competes in the technology and life sciences industries, as this *Boston Globe* headline suggested, or if it would apply to a broader category of industries. We can now report that the bill, as currently drafted, would invalidate ***all*** non-compete agreements in Massachusetts, with a few very limited exceptions, regardless of industry.

This would bring Massachusetts in line with only California and North Dakota, the only other states that completely prohibit employee non-compete agreements.

The limited exceptions to the proposed Massachusetts statute include non-competes entered into in connection with the sale of a business (or the sale of substantially all of the assets of a business), where the restricted party owns at least 10% of the business and received significant consideration for the sale, and non-compete agreements arising outside of an employment relationship.

Additionally, the bill would not affect non-solicitation agreements (both those prohibiting solicitation of an employer's customers and those prohibiting solicitation of employees), non-disclosure agreements, forfeiture agreements, or agreements not to reapply for employment to the same employer. While the bill does not explicitly reference "garden leave" or "bench" provisions (where the employee is compensated not to compete during the restricted period), it would seem to bar such provisions, as they would presumably be deemed to prohibit or restrict an employee's ability to seek or accept other employment. This is something the legislature should clarify and/or the courts may ultimately need to consider in interpreting the bill, should it pass.

One of the most notable provisions of the bill, however, provides that the prohibition on non-compete agreements applies to agreements executed *before* the bill's effective date. This retroactive application is certain to impact negatively businesses in Massachusetts that currently use non-compete agreements to protect their legitimate business interests (e.g., protection of good will, trade secrets, and confidential information), and plan to do so until they are invalidated by statute. Companies whose only protection of confidential and proprietary information or customer relationships consisted of non-compete agreements (which has never been advisable) will have to ensure that they have appropriate protections in place moving forward.

Adoption of the Uniform Trade Secrets Act

Second, the bill includes a provision adopting the Uniform Trade Secrets Act ("UTSA")—making Massachusetts the 49th state to have adopted some version of the UTSA—and another provision that would repeal the current statutory provisions related to liability for trade secret misappropriation and injunctive relief (Sections 42 and 42A of Chapter 93 of the Massachusetts General Laws).

Unlike the current statutory scheme in Massachusetts, the UTSA explicitly permits injunctive relief for actual *or threatened* trade secret misappropriation (whereas under the current scheme, actual misappropriation must be established). The UTSA also specifies that damages can include not only the actual loss caused by the misappropriation, but also unjust enrichment damages.

Like the current statutory scheme, courts can award multiple damages for trade secret misappropriation: The UTSA would allow awards of exemplary damages of up to twice the amount of actual loss or unjust enrichment, where the misappropriation is willful and malicious.

Another significant change that adoption of the UTSA would bring about is an attorneys' fees provision, where the court would be permitted to award fees to the prevailing party if: (i) a claim of misappropriation is made or defended in bad faith, (ii) a motion to enter or terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists. We have addressed the implications of a nearly identical provision in the Texas Uniform Trade Secrets Act here. Notably, unlike the section of the bill eliminating non-competes, the section relating to the UTSA would not apply retroactively.

Now What?

While the UTSA may be welcomed by businesses operating in Massachusetts, we anticipate mixed responses to the proposed elimination of all non-competes (and its proposed retroactive application), with passionate arguments on both sides of the issue.

Of course, the mere introduction of the bill does not ensure its passage and, as we have previously reported, other legislation regarding the enforceability of non-compete agreements in Massachusetts has been pending in one form or another in the state legislature since 2009.

Faced with incredibly disparate opinions in the business community, and the fact that Governor Patrick's administration is in its final months, it may be that the bill in its current form will wither on the vine. Instead, previous bill sponsors may continue their hard work to find a compromise between outright elimination of non-competes and a codification of the common law, which has evolved in the Commonwealth, to enforce those non-competes that are narrowly tailored and address the employer's legitimate business needs to protect its good will, confidential information, and trade secrets. While some studies have suggested a connection between enforcement of non-competes and limited regional growth (for example, comparing the boom of Silicon Valley, where non-competes are

unenforceable, to the more tempered success of the Route 128 area in Massachusetts), other studies have noted that a variety of factors distinguish these regions, such as cultural and structural differences between the East and West Coasts. Accordingly, we anticipate that critics of this bill will point out that the Patrick administration's claim that non-competes "are a barrier to innovation in Massachusetts" may not be quite that cut and dry.

The bill was filed in the Massachusetts House of Representatives and has since been referred to the Joint Committee on Economic Development and Emerging Technologies. We will keep you updated on this sweeping bill's progress.

Massachusetts Governor Proposes Sweeping Legislation Banning Non-Compete Agreements

By Katherine Perrelli, Erik Weibust, and Dawn Mertineit (April 18, 2014)

Last week, Massachusetts Governor Deval Patrick proposed sweeping legislation that would eliminate employee non-compete agreements in Massachusetts. While it remains to be seen whether this bill will actually become law, employers should be aware of the potential implications of this far-reaching bill, and should implement steps sooner rather than later to protect their trade secrets and confidential information should non-competes become unenforceable in the Commonwealth.

Eliminating All Employee Non-Competes in Massachusetts

The Governor's bill, entitled "An Act to Promote Growth and Opportunity" (HB4045), includes a provision that would invalidate *all* non-compete agreements in Massachusetts, with a few very limited exceptions, regardless of industry. This would bring Massachusetts in line with only California and North Dakota, the only other states that prohibit employee non-compete agreements.

The limited exceptions to the proposed Massachusetts statute include non-competes entered into in connection with the sale of a business (or the sale of substantially all of the assets of a business), where the restricted party owns at least 10% of the business and received significant consideration for the sale, and non-compete agreements arising outside of an employment relationship.

Additionally, the bill would not affect non-solicitation agreements (both those prohibiting solicitation of an employer's customers and those prohibiting solicitation of employees), non-disclosure agreements, forfeiture agreements, or agreements not to reapply for employment to the same employer. While the bill does not explicitly reference "garden leave" or "bench" provisions (where the employee is compensated not to compete during the restricted period), it would seem to bar such provisions, as they would presumably be deemed to prohibit or restrict an employee's ability to seek or accept other employment. This is something the legislature should clarify and/or the courts may ultimately need to consider in interpreting the bill, should it pass.

One of the most notable provisions of the bill, however, provides that the prohibition on non-compete agreements applies to agreements executed *before* the bill's effective date. Companies whose only protection of confidential and proprietary information or customer relationships consisted of non-compete agreements (which is not advisable) will have to ensure that they have appropriate protections in place moving forward.

Adoption of the Uniform Trade Secrets Act

The bill also includes a provision adopting the Uniform Trade Secrets Act ("UTSA")—making Massachusetts the forty-ninth state to have adopted some version of the UTSA, with only New York

lagging—and another provision that would repeal the current statutory provisions related to liability for trade secret misappropriation and injunctive relief (Sections 42 and 42A of Chapter 93 of the Massachusetts General Laws).

Unlike the current statutory scheme in Massachusetts, the UTSA explicitly permits injunctive relief for actual *or threatened* trade secret misappropriation (whereas under the current scheme, actual misappropriation must be established). The UTSA also specifies that damages can include not only the actual loss caused by the misappropriation, but also unjust enrichment damages.

Like the current statutory scheme, courts can award multiple damages for trade secret misappropriation: The UTSA would allow awards of exemplary damages of up to twice the amount of actual loss or unjust enrichment, where the misappropriation is willful and malicious.

The UTSA also includes a provision permitting a court to award attorneys' fees in trade secret misappropriation cases to the prevailing party if: (i) a claim of misappropriation is made or defended in bad faith, (ii) a motion to enter or terminate an injunction is made or resisted in bad faith, or (iii) willful and malicious misappropriation exists. Unlike the section of the bill eliminating non-competes, the section relating to the UTSA would not apply retroactively.

What Does This Mean For Your Business?

Faced with incredibly disparate opinions in the business community, and the fact that Governor Patrick's administration is in its final months, it may be that the bill in its current form will wither on the vine. Instead, previous bill sponsors may continue their hard work to find a compromise between outright elimination of non-competes and a codification of the common law, which has evolved in most instances in the Commonwealth, to enforce those non-competes that are narrowly tailored and address the employer's legitimate business needs to protect its good will, confidential information, and trade secrets.

While some studies have suggested a connection between enforcement of non-competes and limited regional growth (for example, comparing the boom of Silicon Valley, where non-competes are unenforceable, to the more tempered success of the Route 128 area in Massachusetts), other studies have noted that a variety of factors distinguish these regions, such as cultural and structural differences between the East and West Coasts. Accordingly, we anticipate that critics of this bill will point out that the Patrick administration's claim that non-competes "are a barrier to innovation in Massachusetts" may not be quite that cut-and-dried.

Notwithstanding the fact that the bill may ultimately not become law, employers with operations in Massachusetts should take steps to prepare themselves in the event the bill is passed, in which case even those agreements that were executed prior to its passage would be invalidated.

Best practices include:

- Identifying the various types of valuable information within a company and assessing the secrecy measures protecting such information.

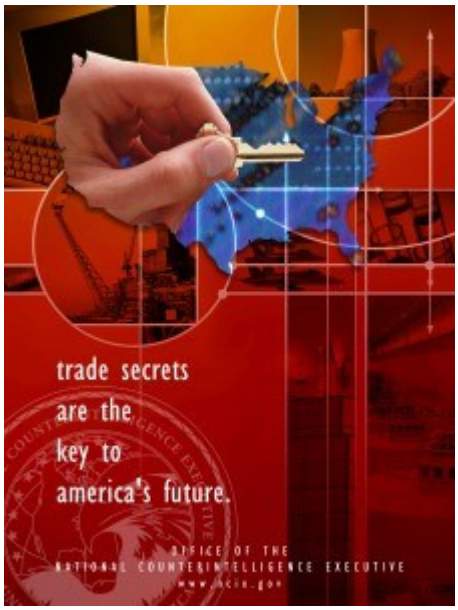
- Drafting and enforcing robust confidentiality and invention assignment agreements that clearly define the sort of information and documents the company considers a trade secret or confidential;

- Implementing entrance interview protocols to educate employees about their non-disclosure obligations from the very start of their employment;
- Implementing exit interview protocols to both remind departing employees of their continuing non-disclosure obligations, and also to ensure that employees return all documents and software at termination;
- Conducting regular employee education programs that create a culture of confidentiality whereby employees understand the value of protecting company data;
- Labeling confidential information as such where appropriate;
- Limiting access to trade secrets, including implementing computer access codes, passwords, identification badges, and locked files for hard copies;
- Regular evaluations of effective trade secret protection measures that take into account new technologies and trends, such as social media and cloud computing issues;
- Notifying departing employees' new employers about your concerns of trade secret disclosure (whether advertent or inadvertent) or misappropriation;
- Reviewing computer records (including email activity, USB drive usage, and phone records) to determine whether a former employee disclosed or maintained sensitive information leading up to or after termination; and
- Use of non-solicitation agreements to limit a departing employee's ability to call on your customers or other employees.

Implementing these practices will help protect your business should Governor Patrick's bill pass. In the meantime, non-compete agreements that are reasonably tailored to protect your company's legitimate business interests are still enforceable, and may add another layer of protection.

Big Changes May Be Ahead for the Nation's Trade Secret Laws

By Robert Milligan and Joshua Salinas (May 13, 2014)



A significant new bill was recently introduced in Congress seeking to add a federal civil cause of action for trade secret theft.

On Tuesday, April 29, 2014, in a bipartisan effort, Senators Christopher Coons (D-Del) and Orrin Hatch (R-Utah), both members of the Senate Judiciary Committee, introduced the bill.

Senators Coons and Hatch's bill, entitled the "Defend Trade Secrets Act of 2014," authorizes a trade secret owner to bring a civil action for a violation of sections 1831(a) or 1832(a) of the Economic Espionage Act. It also permits an owner to bring an action for a "misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce."

"The intellectual property that drives the U.S. economy has never been more valuable, or more vulnerable," Coons said in the written statement."This bipartisan bill will empower American companies to protect their jobs by legally confronting those who steal their trade secrets. It will finally give trade secrets the same legal protections that other forms of critical intellectual property already enjoy."

According to the Senators' news release, an estimated $160 to $480 billion dollars are lost to trade secret theft in the United States each year. In today's electronic age, they observe that trade secrets can be stolen with a few keystrokes and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. The bill seeks to combat the loss of intellectual property and jobs by providing the private sector with access to the federal courts to protect its intellectual capital.

According to the news release, the Economic Espionage Act as presently constituted is insufficient as the Department of Justice brought only 25 criminal trade secret theft cases last year. According to the Senators, the federal courts are better suited to working across state and national boundaries to facilitate discovery, effectuate service on parties, and to prevent a party from leaving the country.

Senators Coons and Hatch have also identified three main objectives that the legislation would accomplish. First, it will harmonize U.S. law by building on the Economic Espionage Act to create a uniform standard to allow companies to craft one set of non-disclosure policies on a fifty state basis. Second, it provides for injunctions and damages to protect companies whose trade secrets are stolen. Third, it is consistent with the approach taken to protecting other forms of intellectual property which are already covered by federal law.

The bill provides for *ex parte* orders for the preservation of evidence and seizure. Based upon an affidavit or verified complaint, the court may, should it find that the order is necessary to prevent

irreparable harm, provide orders for: 1) the preservation of evidence, including the copying of electronic storage medium that contain the trade secret; 2) injunctive relief to prevent any actual or threatened trade secret violation; and 3) permit affirmative actions to be taken to protect a trade secret.

The bill authorizes the court to issue an order providing for the seizure of any property used, in any manner or port, to commit or facilitate the commission of trade secret theft, similar to the seizure procedures used to protect against trademark infringement under the Lanham Act.

The bill also provides for robust remedies, including injunctive relief, damages, unjust enrichment, a reasonable royalty in certain instances, and exemplary damages in an amount not more than three times actual damages. It also provides for attorneys' fees if a claim of misappropriation is made in bad faith, a motion to terminate an injunction is made or opposed in bad faith, or a trade secret is willfully and maliciously misappropriated. The statute of limitations is five years after the date on which the misappropriation is discovered, or by exercise of reasonable diligence should have been discovered.

Lastly, the bill does not preempt any other provision of law.

Among the noticeable benefits for plaintiffs under the proposed legislation are: 1) access to federal court for trade secret theft; 2) seizure and preservation orders; 3) greater exemplary damages than provided under the UTSA; 3) a longer statute of limitations than provided under the UTSA; 4) no express trade secret identification requirement; and 5) arguably, no preemption of common law claims.

As currently drafted, the bill may still face some challenges in obtaining effective service of process and personal jurisdiction over foreign bad actors, as the Department of Justice has recently faced such challenges in criminal actions brought under the Economic Espionage Act.

The bill represents Senator Coons' third attempt at introducing trade secret legislation to create a private civil cause of action after submitting similar bills in 2012 and 2011. Proponents of the legislation can only hope that the third time is a charm. The ABA Intellectual Property Section previously passed a resolution supporting the creation of a civil cause of action for trade secret theft in federal court.

Why is this recent legislation different? The Defend Trade Secrets Acts appears to have removed the "nationwide service of process" and "sworn declaration of misappropriation" provisions, which were some of the mechanisms provided in the 2012 bill to establish standing under the statute. Instead, the statutory language authorizing a private civil cause of action mirrors the language under the Economic Espionage Act, including the recent amendments under the Theft of Trade Secrets Clarification Act.

The bill has won the support of the National Association of Manufacturers, the U.S. Chamber of Commerce, BSA/ The Software Alliance, and companies including 3M, Abbott, AdvaMed, Boston Scientific, Caterpillar, Corning, DuPont, GE, Eli Lilly, Medtronic, Micron, Microsoft, Monsanto, Philips, P&G, and United Technologies.

Rep. Zoe Lofgren (D-Calif.) also introduced last year 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. The bill, however, was much more limited than Senator Coons' proposed 2011 and 2012 bills and the most recent bill.

Another bill seeking to add a federal cause of action for trade secret theft was also introduced by Sen. Jeff Flake (R-Ariz.) entitled the " Future of American Innovation and Research Act" (FAIR), S. 1770, in November 2013.

FAIR differs from the Defend Trade Secrets Act because it does not amend the Economic Espionage Act. FAIR is also focused on combating foreign trade secret misappropriation (i.e., misappropriation occurring outside the U.S. or for the benefit of a foreign person or entity). FAIR also allows plaintiffs to obtain an *ex parte* seizure order, which is more restrictive than the Defend Trade Secret Act's seizure order. It provides that any seized property will be held by a U.S. Marshall or other federal officer appointed by the court pending further hearings/objections by the defendant.

On May 13, 2014, the Senate Judiciary Subcommittee on Crime and Terrorism will have a hearing on trade secret theft entitled "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?"

We will keep you apprised of any further material developments.

Robert Milligan Explaining the Defend Trade Secrets Act of 2014

By Robert Milligan (May 19, 2014)

https://www.youtube.com/watch?v=rSesM_EVvW8

As we discussed on the blog not too long ago, a significant new bill was recently introduced in Congress seeking to add a federal civil cause of action for trade secret theft. In a bipartisan effort, Senators Christopher Coons (D-Del) and Orrin Hatch (R-Utah), both members of the Senate Judiciary Committee, introduced the bill in late April 2014. On May 12, Robert Milligan spoke with LexBlog's Colin O'Keefe in a live online interview to discuss the bill and what it may mean for companies if Congress passes it.

Inching Closer to California: An Update on Massachusetts Non-Compete Legislation

By Erik Weibust and Dawn Mertineit (June 11, 2014)

As we have previously reported, in April of this year, Massachusetts Governor Deval Patrick introduced a sweeping economic growth bill (HB4045) that, if passed, would ban employee non-competes in the Commonwealth. The bill has taken a somewhat convoluted path to date, and we wanted to update you on some notable twists and turns.

First, in mid-May, yet another bill (HB4082) was introduced that stripped those portions of Governor's Patrick's bill *not* dealing with trade secrets and non-competes (in other words, the vast majority of the 42-page bill), leaving only those sections that would adopt the Uniform Trade Secrets Act, repeal the current statutes regarding theft of trade secrets (Sections 42 and 42A of Chapter 93), and ban employee non-compete agreements. This new bill is virtually identical to those provisions of Governor Patrick's original bill (which, as of early this week, has now been stripped of the non-compete and Uniform Trade Secret Act provisions). The introduction of HB4082 was likely due to concerns that Governor Patrick's bill would not make swift enough progress, considering the wide scope of its other provisions that did not relate to employee non-compete agreements. Earlier this week, this new bill was referred to the Joint Committee on Economic Development and Emerging Technologies.

Next, on May 29, 2014, the Joint Committee on Economic Development and Emerging Technologies held a hearing on Governor Patrick's bill, including the provisions related to trade secrets and employee non-competes (which, until this week, were still included in the legislation). We attended the all-day hearing and, unsurprisingly, much of the testimony was devoted to these provisions.

As the New York Times reported on Sunday, many of those who testified at the hearing opined that employee non-competes stifle competition. For example, several legislators spoke of constituents who they deemed "trapped" in jobs because of non-competes signed years earlier, and insinuated that many employees are "ambushed" with non-compete agreements after they have quit their former jobs and rejected other offers. The *Boston Globe* and the *Boston Herald* have each recently published articles about the purported perils of employee non-compete agreements, both of which (as well as the New York Times article) referenced a summer camp in Wellesley, Massachusetts that makes its camp counsellors sign them.

Others, however, noted their concern with the way the bill was drafted, and expressed skepticism that an outright ban on employee non-competes would have uniformly positive effects. For example, some testified that notwithstanding the fact that California bans employee non-competes, and likely *because* of this prohibition, there is increased trade secrets litigation in that state (which is typically much more costly and time consuming than non-compete litigation). Indeed, should this phenomenon occur in Massachusetts, some of those testifying noted that expensive trade secret

litigation could bankrupt small employers and startups—the same group of employers that Governor Patrick's bill (as well as HB4082) was purportedly designed to help.

Nevertheless, many of those who were opposed to the proposed ban on employee non-competes stated that they would be in favor of some form of non-compete reform (some citing with approval the compromise bill previously introduced by Senator William Brownsberger and Representative Lori Ehrlich in late 2012), but that an outright prohibition on the use of non-competes was simply a step too far. The compromise bill, however, appears to be stalled if not dead on arrival.

In yet another twist, just last week Massachusetts House Speaker Robert DeLeo announced plans to file an economic development package that would be similar to Governor Patrick's bill in many respects, but conspicuously omits any provision affecting the enforceability of non-competes. According to the *Boston Globe*, Speaker DeLeo said that "he has heard from many more companies that oppose a ban on noncompete agreements than favor one, in the weeks since Patrick outlined his proposal." It remains to be seen which approach will carry the day.

We will continue to monitor these bills, as well as any others that may be filed, and report back on any progress. Please join us for our upcoming webinar on the latest legislative developments in trade secret, non-compete, and social media law.

Another Public Hearing Scheduled for Massachusetts Non-Compete Bill: What's Next?

By Kate Perrelli and Erik Weibust (June 27, 2014)

We reported in our post of June 11th that Governor Patrick had introduced a sweeping economic growth bill (HB4045) — that, if passed, would ban employee non-competes in the Commonwealth. We also explained that subsequent to Governor Patrick's bill, another bill (HB4082), was introduced that stripped Governor's Patrick's bill and left only those portions dealing with trade secrets and non-competes. This new bill would adopt the Uniform Trade Secrets Act, repeal the current statutes regarding theft of trade secrets (Sections 42 and 42A of Chapter 93), and ban employee non-compete agreements. HB4082 was likely introduced because of concerns that Governor Patrick's bill would not make swift enough progress, since the other provisions that did not relate to employee non-compete agreements were so broad in scope.

The second bill, HB4802, was referred to the Joint Committee on Economic Development and Emerging Technologies in early June, and now that Committee has scheduled a public hearing for **July 1, 2014 from 11:00 a.m. to 2:00 p.m. in Room B-1 at the Statehouse**. Similar to the committee hearing held previously on Governor Patrick's broader economic bill (HB4045), we expect to hear testimony from constituencies on both sides of the non-compete debate. As the Boston Globe noted after the hearing on Governor Patrick's bill, "[t]he sides are generally split according to size, with large, established employers … working to maintain the status quo, and people from the startup world — including venture capitalists who invest in early-stage companies — pushing to let workers jump to rivals whenever they want.We will be attending the hearing, and will report out after.

Also, still in play are the House and Senate's economic development bills. As we reported previously, the House economic development bill is notably silent on the issue of non-competes and adoption of the Uniform Trade Secrets Act. The Senate economic bill, which was released this morning, is also silent on the issue of non-competes, but adopts the Uniform Trade Secrets Act. Both economic bills are pending. After votes on any amendments to the Senate bill next week, a conference committee will be appointed with three members from each body to reconcile the House and Senate versions. Since neither of the economic bills mention non-competes at all, the final version of the bill (after they reconcile the House and Senate bills) sent to the Governor for his signature (by July 31) will not change state law on non-competes. Separate and apart from the pending economic bills, whether or not a standalone bill like HB4802 will get to the Governor for signature by January 31st remains to be seen.

Against this backdrop, you may wonder what is next on the legislative path for HB4802 after the July 1st hearing. As we understand it, the Committee will meet after the hearing to decide next steps. This could happen as soon as Tuesday after the hearing, or sometime thereafter. The bill could emerge from the Joint Committee as is, or it could include amendments. Some are suggesting that the bill will be amended and a compromise bill will emerge that will then go to the House Ways and Means

Committee, where any changes to bills are reported. It could then be reported out to the full House for consideration, or it may have to go back to committee.

In sum, it is difficult to predict at this juncture whether HB 4082 will survive in its current form, or evolve toward a compromise bill like the one previously introduced by Senator William Brownsberger and Representative Lori Ehrlich in late 2012. Keep in mind that after July 31, there will be no more formal sessions of this legislature. While informal sessions will still occur, typically those only address "non-controversial" legislation, such as the changing of a street name. It is also worth noting that this is the last year of the two year legislative session, so unless the legislature acts on HB4802 before end of July, the legislation would have to be reintroduced into a new congress in January — with a new governor.

We will continue to monitor all the pending bills, as well as any others that may be filed, and report back after the July 1 hearing. You may be interested in today's Boston Business Journal's article on the non-compete debate in Massachusetts.

On the Eve of The Esplanade July 4th Fireworks Celebration – Massachusetts May Not Blow Up Non-Competes After All – A Compromise is in the Air

By Katherine Perrelli (July 2, 2014)

There are signs that the debate over whether to ban non-competes may end in a compromise, a result many, including this blog, have predicted.

As we reported in Friday's post, the Joint Committee on Economic Development and Emerging Technologies held a public hearing yesterday at the Statehouse on HB4802, which would adopt the Uniform Trade Secrets Act ("UTSA"), repeal the current statutes regarding theft of trade secrets (Sections 42 and 42A of Chapter 93), and ban employee non-compete agreements. The three hour hearing was packed with legislators, lawyers, and business people on both sides of the non-compete debate. Also, in attendance and presenting testimony were individuals negatively impacted by non-competes, many of whom were wearing "Create Jobs in Massachusetts/Ban Non-Competes" stickers.

The Committee's Chair, House representative, John Wagner noted at the commencement of the hearing that unless convinced otherwise he was somewhere along the spectrum between leaving the law as it is on non-competes, and banning them outright. The hearing testimony was kicked off by Governor Patrick's economic development chief, Gregory Bialecki, who presented the Patrick administration's position that non-competes stifle innovation and job growth and should be banned, but he told the committee that the administration would be open to a compromise.

Another House Representative, Lori Ehrlich, who has been involved in the non-compete debate since 2009 (please see ourlink to previous blog entries on the topic), and worked previously with then House Representative William Brownsberger, on a compromise bill, offered proposed changes to the HB4802. She explained that the changes are designed to address the unpredictability of the current common law, and incent employers to use narrowly tailored non-compete restrictions. Ehrlich's proposal would establish presumed reasonable terms for the duration, geographic scope, and activity restrictions of non-competes, such as a six month non-compete restriction, and limiting the employee only from taking a position with similar duties to previous position and within same geographic region he/she was in previously. Under current Massachusetts common law, while courts can *reform* overbroad agreements to be more limited, it is difficult at best for employers and employees to predict what will be deemed reasonable or not. Erhlich's proposal sets a "reasonableness" guidepost. Moreover, in a departure from current law, the proposal includes a *"red pencil"* provision for any non-compete restriction not presumed reasonable under the proposed legislative scheme. For example, if the enforcing company cannot demonstrate a legitimate business reason for exceeding a 6 month non-compete restriction,

Ehrlich's proposal requires a court to "red pencil" and strike the non-compete, rather than merely reduce it to a 6 month presumed reasonable time frame. The intent behind this part of the proposal is to incent employers to implement very tailored and narrow non-compete restrictions.

While it seems there is much less debate over the trade secrets provisions in HB4802, Erhlich also proposed some revisions relating to the UTSA, including expanding protections to licensees of trade secrets rather than just the owners; eliminating the need for owners of trade secrets that have been misappropriated to continue security protections while they pursue enforcement; and limiting the premature and breadth of disclosure of the trade secrets at issue in litigation to enforce UTSA protections.

As we had previously reported (link to previous blog), also still in play on non-compete and trade secret protection in Massachusetts are the House and Senate's pending economic development bills. The House economic development bill is notably silent on the issue of non-competes and adoption of the UTSA. The Senate economic bill, was also silent on the issue of non-competes, but would adopt the UTSA. Yesterday, while the Joint Committee hearing was underway, the Senate voted 32-7 in favor of a compromise approach offered by Senator William Brownsberger, an early proponent of banning non-competes. Here is a link to earlier blog entries on the bills. This compromise like Ehrlich's would limit the duration of non-compete restrictions to six months and prohibit their use with hourly employees. It is unclear what the House will do on the non-compete issue given the pending bill's silence on the issue. These differences will no doubt be addressed and perhaps settled later in the month when the Senate and House try to reconcile their economic development bills before the end of the legislative session on July 31.

In sum, it seems more likely now that Massachusetts will enact some form of legislation governing the use of non-competes and adopt some form of the Uniform Trade Secrets Act. The final form of such legislation remains to be seen, as well as whether it can be accomplished before the end of July. As we reported previously, there will be no more formal sessions of this legislature after July 31st. While informal sessions will still occur, typically those only address "non-controversial" legislation, such as the changing of a street name. Moreover, it is the last year of the two year legislative session, so unless the legislature acts on HB4802 or another standalone bill before the end of July, the legislation would have to be reintroduced into a new congress in January — with a new governor.

We will continue to monitor all the pending bills, as well as any others that may be filed, and report back.

No Massachusetts Non-Compete or Trade Secret Legislation This Year

By Erik Weibust, Katherine Perrelli, and Dawn Mertineit (July 21, 2014)

Although, as we have previously reported, the Massachusetts legislature arguably got closer to enacting a non-compete statute this year than ever before ─ which, if Governor Deval Patrick had his druthers, would have banned them outright ─ there will be no new legislation this year according to our sources. The legislative session ends today.

As we last reported, a compromise bill was overwhelmingly approved by the Massachusetts Senate in early July that would have required:

(a) that non-competes be in writing and signed by both the employee and the employer, and expressly state that the employee has the right to consult with counsel prior to signing;

(b) to the extent reasonably feasible, employees be given five business days' advance notice; and

(c) if entered into after commencement of employment (but not in connection with a separation agreement), non-competes must be supported by fair and reasonable consideration in addition to continued employment, and notice must be provided at least ten business days before the agreement is to be effective; and where the non-compete is part of a separation agreement, the employee must be given seven days to rescind acceptance.

The compromise bill also would have established presumptions of reasonableness with respect to duration (6 months), geographic reach (the area in which employee, during the last two years of employment, provided services, or had a material presence or influence), and the scope of proscribed activities (specific types of services provided by the employee during last two years of employment), and it would have banned the use of non-competes for workers classified as nonexempt under the FLSA (e.g., hourly workers).

Finally, the compromise bill would have permitted courts to reform (or "blue pencil") non-competes only where provision to be reformed was either presumptively reasonable (as described above) or where the employer made objectively reasonable efforts to draft the particular provision so that it would be presumptively reasonable.

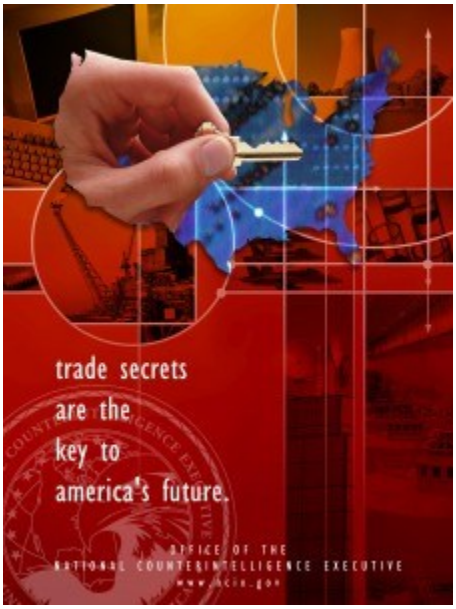
While this bill was supported in the Massachusetts Senate, it will not pass this year. Likewise, there will be no new legislation enacting the Uniform Trade Secrets Act.

Trading Secrets

Although non-compete legislation is dead in the water this year, we have no doubt that it will be a hot issue again next year, particularly with the election of a new governor this fall. We will keep you posted on any developments.

Push for Federal Trade Secret Legislation Gaining Momentum

By Robert Milligan (August 13, 2014)



Federal legislators introduced bills this year to create a civil cause of action for private litigants in federal court for trade secret misappropriation.

With the most recent bill introduced in the House by a bi-partisan coalition in late July, there appears to be surging momentum for the passage of federal trade secrets legislation this fall, particularly with several leading companies and business groups supporting the creation of a federal civil remedy.

The Economic Espionage Act, which provides criminal liability for trade secret misappropriation, currently only authorizes civil actions by the Attorney General but not by private parties. Accordingly, unless diversity jurisdiction exists, or there is some other hook such as a cause of action brought under the federal Computer Fraud and Abuse Act, there is currently no basis to bring a civil trade secret cause of action in federal court.

Instead, plaintiffs are left to bring trade secret claims in state court under various state statutory adoptions of the Uniform Trade Secrets Act. Massachusetts and New York have not adopted the UTSA and trade secret claims are brought under the common law in those jurisdictions.

There are inconsistencies and differences among some states concerning their specific adoption of the UTSA and some courts have differing interpretations regarding the key provisions of the UTSA. In sum, there are significant differences among some states concerning key issues such as recoverable damages/royalties, preemption, trade secret identification, reasonable secrecy measures, statute of limitations, and reverse engineering. Thus, companies who conduct business in the United States often must address differing and conflicting standards when trying to protect their trade secrets throughout the nation.

Senate Bill: *Defend Trade Secrets Act*

On April 29, 2014, Sens. Christopher Coons (D-Del.) and Orrin Hatch (R-Utah) introduced the Defend Trade Secrets Act of 2014. The bill amends the Economic Espionage Act to provide a civil cause of action to private litigants for violations of 18 U.S.C. § 1831(a) and 1832(a) of the EEA and for "misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce." According to the sponsors, the bill will provide uniform trade secrets protection and federal remedies across the United States. They also stated that there is a need for

legislative action with an estimated $160 to $480 billion lost to trade secrets theft in the United States and the ease of theft in the electronic age.

The bill marked the latest attempt in the past four years to create a private civil cause of action for trade secret misappropriation at the federal level. The following bills previously failed: Amendment to Currency Exchange Rate Oversight Reform Act of 2011, Protecting Trade Secrets and Innovation Act of 2012 ("PATSIA"), and Private Right of Action Against Theft of Trade Secrets Act of 2013 ("PRATSA").

The bill provides for a five year statute of limitations and provides uniform remedies for misappropriation of trade secrets. It provides for injunctive relief to prevent any actual or threatened misappropriation of trade secrets. It also allows for affirmative actions to be taken to protect trade secrets. With respect to damages, it provides damages for actual loss, unjust enrichment, and a reasonable royalty in certain scenarios. Additionally, in exceptional circumstances, royalties can be awarded for the use of trade secrets in lieu of a permanent injunction. In cases of willful or malicious misappropriation, the bill provides for exemplary damages of not more than three times the actual damages. It also provides for attorneys fees' and costs for willful and malicious misappropriation or for the pursuit of a trade secret cause of action in bad faith.

It also provides for *ex parte* orders for preservation of evidence and seizure of any property used, in any manner or part, to commit or facilitate a violation of the statute, using the procedure contained in the Lanham Act.

Lastly, the bill provides that nothing in the statute "shall be construed . . . to preempt any other provisions of law." Accordingly, the intent of the bill is not to preempt state UTSA claims. It is unclear whether state common law claims would also not be subject to preemption.

House Bill: *Trade Secrets Protection Act*

On July 29, 2014, a similar bill, entitled the Trade Secrets Protection Act of 2014, was introduced into the House, by a bi-partisan group led by George Holding (R-N.C) and Jerrold Nadler (D-NY).

"American businesses face relentless cybersecurity threats every day, costing our economy billions of dollars and tens of thousands of jobs each year," said Rep. George Holding in his press release in support of the bill.

"As a way to help create jobs, grow our economy and protect our businesses, I have introduced the Trade Secrets Protection Act of 2014. This bill will help supply American businesses, both large and small, with the tools needed to combat these destructive threats," he added.

"American businesses are global leaders in innovation and job creation, yet they are faced with increasing threats to valuable information. The current patchwork within state and federal statutes is not enough to keep pace with organized trade secret theft, resulting in a loss of nearly $100 billion which could mean 200,000 jobs, a recent report stated, " he remarked.

"By helping American businesses defend against these threats, we are not only protecting American interests, but helping recover the millions of dollars and thousands of jobs lost each year," Holding concluded.

The bill is co-sponsored by Holding, Howard Coble, R-N.C., Hakeem Jeffries, D-N.Y., Steve Chabot, R-Ohio and John Conyers, D-Mich.

Differences Between the Two Trade Secret Bills

The House bill largely tracks the Senate's Defend Trade Secrets Act but has three notable and significant modifications, which are tracked in this redline:

1) It only permits a civil claim for "misappropriation of a trade secrets that is related to a product or service use in, or intended for use in, interstate or foreign commerce." It does not permit a claim for a violation of 18 U.S.C. § 1831(a) and 1832(a).

2) It permits a seizure order on an *ex parte basis* to preserve evidence or to prevent the propagation or dissemination of the trade secret that is the subject of the action but it has certain precautions and limitations not found in the Senate bill.

3) It clarifies that it only covers misappropriation actions that occur on or after it is enacted.

With respect to the seizure order language, in order to obtain an *ex parte* order, the plaintiff must show, that (1) a temporary restraining order under Rule 65(b) would be inadequate because the defendant would evade, avoid, or otherwise not comply with such order; (2) an immediate and irreparable injury will occur if seizure is not ordered; (3) the harm to the plaintiff of denying the order outweighs the legitimate interests of defendant and substantially outweighs any harm to third parties; (4) the plaintiff is likely to succeed against the defendant in showing that the defendant misappropriated the trade secret and is in possession of the trade secret; (5) the plaintiff described with particularity the matter to be seized and the location where the matter is to be seized; (6) the defendant would destroy or make the property inaccessible to the court if the applicant were to proceed on notice; and (7) the plaintiff has not publicized the request.

Additionally, the court's order must (1) minimize any interruption of the business operations of third parties and the defendant that is unrelated to the trade secret that has allegedly been misappropriated; (2) protect the property from disclosure to plaintiff; (3) set a hearing date no later than seven days after the order is issued; and (4) require a security adequate to cover damages from a wrongful or excessive seizure. The court is required to take appropriate action to protect the defendant from publicity. The court is also required to take custody of the material ordered seized. Lastly, any person who suffers damage by reason of a wrongful or excessive seizure has a cause of action against the plaintiff.

In sum, the most significant difference between the bills is the clarification and refinement of the seizure order.

https://www.youtube.com/watch?v=QAZNmFeJ2gU

Analysis and Discussion of the Legislative Movement

According to sources, there may not be any significant opposition by the Senate sponsors to the House's version of the trade secret bill.

With some attention away from patent reform on the Hill, there may be an opportunity to get a trade secret bill done in the fall. Congress has shown an ability to pass amendments to the Economic Espionage Act in recent years. We expect that there will be activity on the bills in early September with possible votes taken in mid-to-late September.

There appears to be some very positive momentum for the bills, including bi-partisan support in both houses by high ranking legislators and likely support by the Obama Administration. Additionally, on the right, the Heritage Foundation recently wrote an article in support of a private right of action. On the left, Congresswoman Zoe Lofgren previously proposed creating a civil cause of action in federal court last year in the PRATSA bill. Also, a diverse set of companies and organizations have come out in favor of legislation or the concept of a federal civil cause of action, including Adobe, Boeing, Microsoft, IBM, Honda, DuPont, Eli Lilly, Broadcom, Caterpillar, NIKE, Qualcomm, General Electric, Michelin, 3M, United Technologies Corporation, AIPLA, ABA IP Section, National Association of Manufacturers, and the National Chamber of Commerce.

As indicated NAM supports the bill, noting that it marked "a critical step toward ensuring manufacturers can effectively and efficiently enforce their trade secrets at home and abroad." "[Trade secret] theft costs businesses in this country some $250 billion a year," the group said. "The Trade Secrets Protection Act would help to address this challenge by providing access to federal civil enforcement for trade secrets theft. Right now, businesses must go state by state to defend their rights."

Proponents of the bill cite the advantages of a federal cause of action, as among other things, a unified and harmonized body of law that addresses discrepancies under the existing law and provides companies a uniform standard for protecting its proprietary information. It may treat trade secrets on the same level as other IP and establish them as a national priority, address national security concerns, and create a demonstrative effect on major foreign jurisdictions. The bill may provide a complimentary measure to combat trade secret misappropriation by private industry in light of strained government resources. There are also service of process advantages, ease of conducting nationwide discovery, and additional remedies to aid victims, such as seizure.

Additionally, the former head of the Patent Office, David Kappos recently came out in favor of the bill on behalf of the Partnership of American Innovation stating, "Trade secrets are an increasingly important form of intellectual property, yet they are the only form of IP rights for which the protection of a federal private right of action is not available. The Trade Secrets Protection Act will address this void, and the PAI supports its swift enactment."

While no formal opposition has been organized yet, various attorneys skeptical of the legislation cite federalism concerns, legislation in search of a problem, the alleged over breadth of the seizure language, and the perceived burden on the federal courts.

We will carefully track the developments of these bills going forward this year. It is important to note that like the United States, the European Commission is considering a directive providing more uniform protection of trade secrets.

Massachusetts Governor Makes Last Ditch Effort to Pass Non-Compete Legislation Before His Term Ends

By Erik Weibust and Dawn Mertineit (August 25, 2014)

As you may recall, we recently reported that Massachusetts legislators' attempts to pass a bill altering the landscape of non-compete enforceability (including Governor Deval Patrick's bold push to ban non-compete agreements altogether) failed yet again. As has become a nearly perennial event in the Commonwealth, efforts to push legislation through by the close of the session were frenzied, but ultimately much ado about nothing.

Surprisingly, now that the formal legislative session has ended (and before a new one begins next January), Governor Patrick has reintroduced non-compete legislation, although tellingly, this version is much more measured than his previous proposal. Indeed, instead of proposing to ban non-compete agreements altogether, Governor Patrick's new proposal mirrors the most recent compromise bill introduced by Senator Will Brownsberger and Representative Lori Erlich, which was overwhelmingly approved in the Senate but failed to pass before the end of the session.

To wit, like the previous compromise bill, the newly introduced Patrick bill would require:

(a) that non-competes be in writing and signed by both the employee and the employer, and expressly state that the employee has the right to consult with counsel prior to signing;

(b) that to the extent reasonably feasible, employees be given five business days' advance notice; and

(c) that if entered into after commencement of employment (but not in connection with a separation agreement), non-competes must be supported by fair and reasonable consideration in addition to continued employment, and notice must be provided at least ten business days before the agreement is to be effective; and where the non-compete is part of a separation agreement, the employee must be given seven days to rescind acceptance.

The bill also creates presumptions of reasonableness as to duration (6 months), geographic reach (the area in which employee, during the last two years of employment, provided services, or had a material presence or influence), and the scope of proscribed activities (specific types of services provided by the employee during last two years of employment). It also bans the use of non-competes for workers classified as nonexempt under the Fair Labor Standards Act (i.e., hourly workers).

Finally, the bill allows courts to reform non-competes only where the provision to be altered is either presumptively reasonable as described above, or where the employer made "objectively reasonable efforts to draft the particular provision so that it would be presumptively reasonable".

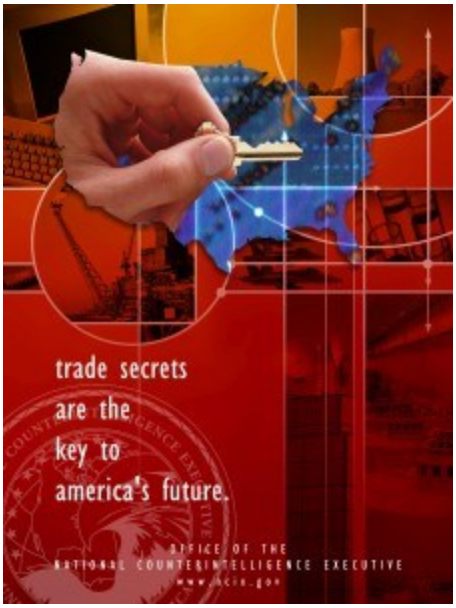
It's unclear what progress will be made on this bill, if any. Now that the formal legislative session has ended, many legislators are focused on their reelection campaigns. No votes will be taken on the bill until next year's formal session commences in January of 2015, when a whole new crop of legislators will be getting to work – along with a new governor, as Governor Patrick is not running for reelection this year.

Stay tuned for any new developments!

House Judiciary Committee to Consider Federal Trade Secret Legislation

By Robert Milligan and Joshua Salinas (September 9, 2014)

With increased activity regarding proposed federal trade secret legislation expected this month and for the remainder of the fall Congressional session, Seyfarth Shaw's dedicated Trade Secrets group has created a resource page on its Trading Secrets blog which summarizes the proposed legislation, outlines the arguments in favor of and against the legislation, and provides additional legislation resources for our readers' convenience.



The resource page will be continuously updated as we monitor and keep you apprised of the most recent developments, debate, and news regarding the proposed legislation.

While there was a mark up of the House Trade Secrets Protection Act of 2014 scheduled before the House Judiciary Committee on *September 10, 2014, at 10:00 a.m. EST,* ***it has been continued until next week.*** We will let you know when the date is announced and we will cover it all with live-tweeting on Twitter at @tradesecretslaw and @joshsalinas.

House Judiciary Committee Considers Federal Trade Secret Legislation

By Robert Milligan and Joshua Salinas (September 17, 2014)

With increased activity regarding proposed federal trade secret legislation expected this month and for the remainder of the fall Congressional session, Seyfarth Shaw's dedicated Trade Secrets group has created a resource page on its Trading Secrets blog which summarizes the proposed legislation, outlines the arguments in favor of and against the legislation, and provides additional legislation resources for our readers' convenience.

The resource page will be continuously updated as we monitor and keep you apprised of the most recent developments, debate, and news regarding the proposed legislation.

The mark up of the House Trade Secrets Protection Act of 2014 scheduled before the House Judiciary Committee is scheduled for Wednesday, September 17, 2014, at 1:00 p.m. EST. We will cover the it all with live-tweeting on Twitter at @tradesecretslawand @joshsalinas.

International

Chinese Espionage Latest Target: Correction Fluid

By Anthony Orler (March 11, 2014)

Spell check features in word processing programs sent correction fluid the way of the buggy whip. Walter Liew and Robert Maegerle, however, saw a $28 million dollar payout to sell the secrets to, among other things, typewriter correction fluid. It is doubtful that they can "white out" the bars of their new prison cells, though.

Liew, a California engineering consultant, and Maegerle, a former engineer, were convicted in what may be the first federal jury conviction under the Economic Espionage Act of 1996 for economic espionage, trade-secret theft, witness tampering, and making false statements.

What could be so incredibly secret and technical about correction fluid?

The white pigment in correction fluid is titanium dioxide. Titanium dioxide is used in hundreds of items, including paints, plastics, paper, rubber, cosmetic products, and food. Titanium dioxide is also used in electrical ceramics and semiconductor devices. The annual global sales of titanium dioxide are approximately $17 billion dollars.

Maegerle's former employer holds trade secrets on how to make titanium dioxide, and accounts for one-fifth of the annual global sales of the chemical. Liew received the trade secrets from Maegerle and sold them for $28 million to China-based Pangang Group. Allegedly a Chinese state-owned company, Pangang is building a new plant to produce titanium dioxide in China.

The stolen trade secrets included a drawing of a plant system, an internal report about a computer model for a chemical process, a plant flow sheet and a basic data document containing the process and equipment needed to design a titanium dioxide production line.

Each defendant now faces up to 15 years in federal prison and hundreds of thousands of dollars in fines. Pangang was also charged but did not face trial because prosecutors were unable to serve legal documents on the company in China.

Liew's wife Christina was also charged with economic espionage, trade secret theft and witness tampering. She will be tried separately.

Trading Secrets

With economic espionage statutes supplementing trade secret law, the government now has additional weapons against trade secret theft. Now, aggressive and determined efforts to steal U.S. intellectual property can be thwarted. Additional deterrents to would-be espionage targets are realized through larger penalties for conviction under both economic espionage and trade secret laws.

Liew and Maegerle understood that the simplicity of the underlying product covered by the trade secret does not detract from the trade secret's importance to competitors. Although appeals are planned, it is unlikely that the defendants will have access to trade secrets protecting other "simple" devices, such as the locks on their prison doors.

For more information on *U.S. v. Liew*, 3:11-cr-00573, (N. D. Cal., 2014), see the Bloomberg News article and the FBI press release.

Recent Decision Affirms Significant Protections for Confidential Information in United Kingdom

By Ming Henderson and Razia Begum (March 26, 2014)

With the increasing number of disputes and client queries regarding confidential information in the United Kingdom, the recent case of *Personnel Hygiene Services Ltd & ors v. Rentokil Initial UK Ltd* , EWCA Civ 29, 29 January 2014, serves as a useful reminder of the extensive protection of confidential information.

The Court of Appeal, considered whether the obligations under a confidentiality agreement continued to apply after the parties entered into a second agreement which contained no such express obligations. The court upheld the first instance decision, finding that the confidentiality obligations continued to apply to protect trade secrets (in this case, information relating to customers and services). Although not a landmark decision, this may seem a surprising judgment , particularly as the second agreement contained an entire agreement clause which would usually be interpreted as replacing all previous contractual arrangements. The court made no reference to this point in the judgment.

In this case, Rentokil (the party in receipt of the confidential information) appealed against an injunction preventing it from contacting customers of UK Hygiene (the provider of the confidential information). UK Hygiene had terminated the second agreement in order to deal directly with the ultimate customers. Following this, Rentokil directly approached UK Hygiene's customers with a goal to provide services to them using, in part, confidential information (about customers and services) under the first agreement.

Key takeaway messages:

- **Extensive protection:** Although we would always recommend inserting strong confidential information clauses that limit use after the term of the agreement or for other purposes, this decision provides comfort to those providing information to potential competitors that "confidential information" with a significant risk of misuse will be protected.

- **Prevention is better than cure:** Though the point was not specifically raised in this case, companies should, if they are not already doing so, physically protect their confidential information (e.g. by installing passwords, limiting access by other means, etc.) and seek to retain control of it. This can be a far more effective and less costly approach in the long-term than litigating over confidential information in the hands of third parties.

With international offices in London, Shanghai, Melbourne, and Sydney, Seyfarth Shaw's trade secrets, computer fraud, and non-competes practice group provides national and international coverage for companies seeking to protect their information assets, including trade secrets and confidential information, and key business relationships.

Australia Non-Compete Primer: Protecting Your Business Interests Post-Employment

By Justine Turnbull and Cassie Howman-Giles (March 31, 2014)

Given difficult economic times, protection of confidential information (including trade secrets) has become a greater priority for business in Australia. As a result, post-employment restraint litigation is increasingly common as employers attempt to protect their confidential information and restrain former employees from soliciting the business of their valued clients.

This note outlines the position in Australia regarding the legal enforceability of post-employment restrictions on conduct.

POST-EMPLOYMENT RESTRAINTS

Content

It is common in Australia for contracts of employment with executives and other key employees to contain terms restricting the activities of employees after the employment relationship ends, including prohibitions against:

- competition;
- solicitation of clients, customers or suppliers; and
- solicitation of employees or other workers.

The restraints are almost always limited to a defined restricted activity, a time period and an area of operation. These operational limitations are important when considering whether the restraints are legally enforceable.

'Garden leave' clauses, which allow an employer to instruct an employee serving their notice period to not attend work, are increasingly being viewed by courts as being equivalent to post-employment restraints.

Are Restraints Enforceable?

In Australia, post-employment restraints are generally unenforceable for public policy reasons unless they are reasonably necessary to protect the employer's (or principal's) legitimate business interests (usually confidential information or goodwill with customers or employees). There are two elements to be satisfied: firstly, the employer must have a legitimate interest in imposing the restraint and secondly, the scope of the restraint must be no wider than is reasonable necessary to protect that interest.

Legitimate business interests

Stifling competition from a former employee or preventing a valuable worker from being employed by someone else is not a legitimate interest. Recognised categories of legitimate interest include confidential information and customer or employee connections.

Reasonableness

In assessing the reasonableness of a restraint, a court will consider various factors including:

- types of activities restrained;
- duration of restraint;
- geographic coverage of restraint;
- seniority and role of employee; and
- whether consideration is provided in exchange for the restraint and, if so, the level of consideration.

Seniority and role of the employee are an important consideration when considering enforceability as they determine whether the employee:

- had access to confidential information of the employer and/or customers;
- were 'customer facing' and involved in building customer relationships; and
- were the 'human face' of the business.

Enforceability of a restraint is determined at the time the restraint was agreed to (that is, in most cases, the time the employment contract was entered into).

Drafting Restraints

Given the difficulty in determining whether a restraint will be found to be enforceable, 'cascading clauses' are often used to provide the court with a variety of options for the scope of the restrained activities, the period and the geographical coverage. Courts have a common law power to delete the options so that the resulting clause is reasonable and enforceable (the 'blue pencil test').

In New South Wales, legislation empowers the Supreme Court of New South Wales to read down otherwise invalid restraints. This power is much broader than the common law power to simply sever certain options and can generally be relied on to obtain at least partial enforcement of a restraint in New South Wales.

Enforcement

The usual remedy sought by an employer when enforcing a post-employment restraint is an injunction, that is, an order of the Court restraining the employees from performing particular activities. The employer may also seek damages for any loss caused by a breach of the restraint.

Trading Secrets

With international offices in London, Shanghai, Melbourne, and Sydney, Seyfarth Shaw's trade secrets, computer fraud, and non-competes practice group provides national and international coverage for companies seeking to protect their information assets, including trade secrets and confidential information, and key business relationships. For more information on international trade secret and non-compete issues, please see our previous webinars When Trade Secrets Cross International Borders and Trade Secret and Non-Compete Considerations In Asia. We are pleased to announce that we will have another international trade secrets and non-compete law update later this year with an Australia and EU focus. Follow the blog for more details.

European Commission Proposes Directive for Trade Secrets Protection in EU

By Daniel Hart, Razia Begum, and Andrew Masak (May 7, 2014)

Later this month, voters in the European Union's 28 Member States will cast their votes for representatives in the European Parliament. Regardless of the makeup of the European Parliament following the election, trade secret regulation is one of the many issues that members are likely to take up when the European Parliament reconvenes later this year following the election.

On November 28, 2013, the European Commission announced a proposal for a Directive on trade secrets. If passed by the European Parliament, the Directive will increase the trade secrets protections afforded to companies with operations in the EU and may greatly enhance cross-border certainty and uniformity across Europe.

A Patchwork of Protection

Currently, there is no uniform protection of trade secrets across the EU. Instead, a patchwork of uneven levels of protection and remedies exist among EU Member States. As detailed in a study prepared for the European Commission, Austria, Bulgaria, the Czech Republic, Estonia, Germany, Finland, Greece, Hungary, Italy, Latvia, Lithuania, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and Sweden have legislation on misappropriation of trade secrets, although some of them do not define trade secrets. In contrast, Belgium, France, Ireland, Luxembourg, Malta, the Netherlands, and the UK have no specific statutory provisions regarding protection of trade secrets but rely on judicial interpretation of general provisions on extra-contractual liability or (in common law countries) on traditional common law. In Cyprus, trade secrets are only protected by contract. In France, misappropriation by employees of certain types of trade secrets (namely, manufacturing secrets) are criminally punished.

Highlights of the Proposed Directive

At this stage in the legislative process, the Directive remains merely a proposal. However, several aspects of the Directive, if adopted, would substantially alter the existing legal landscape and create a more harmonized trade secret regime throughout the EU.

Three features of the Directive are particularly noteworthy.

First, the Directive provides a common definition of "trade secrets" and uniform rules about the acquisition, use, and disclosure of trade secrets. For example, in language that is similar to the definition of "trade secrets" in the Uniform Trade Secrets Act (which the vast majority of U.S. states have adopted), the proposed Directive defines a trade secret as "information which meets all the following requirements":

- "is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question";
- "has commercial value because it is a secret"; and
- "has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret."

The proposed Directive also provides that acquisition of a trade secret is unlawful "whenever carried out intentionally or with gross negligence by":

- unauthorized access to or copy of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;
- theft;
- bribery;
- deception;
- breach or inducement to breach a confidentiality agreement or any other duty to maintain secrecy; or
- any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

Second, the Directive establishes a common set of procedures and remedies for trade secret holders where there is unlawful acquisition, use, or disclosure of that trade secret, including a two-year statute of limitations for bringing claims for trade secret misappropriation. The Directive also includes rules on the preservation of trade secrets during litigation.

Third, the Directive provides for uniform remedies for civil law redress for trade secrets misappropriation across Member States, including injunctive and declaratory relief, damages, and sanctions for non-compliance. The Directive also includes various reporting provisions.

The Road Ahead

Because the proposed Directive was only recently published, and the parliamentary process is unlikely to start in earnest until at least until Autumn, 2014, it is unclear whether the Directive as currently written will be implemented, if at all. Certain groups – for example, the IP Federation (representing a number of major innovative UK companies) – have welcomed the Directive. Businesses have applauded there being greater certainty of protection consistently across all Member States, especially given the continuous rise in the misuse of trade secrets, which is escalated by growing technological advances. In contrast, others have been critical of the breadth of protection that the proposed Directive would afford trade secrets. For instance, the EU at this stage has decided not to harmonize criminal sanctions. In addition, as with countless other attempts to transcend European boundaries with international law and norms, some political parties and movements within Member States may oppose any Directive that could be viewed as taking away autonomy and sovereignty from Member States.

If the Directive does come into force, Member States will still need to implement the Directive within two years from the date of adoption of the Directive into their own national law. EU directives lay down certain end results that must be achieved in every Member State by a specific date. Individual Member States must adapt their laws to meet these goals, but are free to decide how to do so. For example, the European Scrutiny Committee in the UK Parliament has already indicated that existing common law and contract law in the UK adequately protects trade secrets consistent with the Directive. However, the Committee is considering whether the Directive nonetheless would require the UK to pass implementing legislation.

We will continue to monitor this proposed Directive as it is considered by the Council of Ministers and members of the European Parliament for adoption under the ordinary legislative procedure in the months ahead. Dan Hart will also be leading a discussion on this topic at the ITechLaw World Technology Conference next week in New York.

Seyfarth Attorneys Lead Discussion of Proposed EU Trade Secrets Directive at ITech Law World Technology Conference

By Daniel Hart (May 16th, 2014)

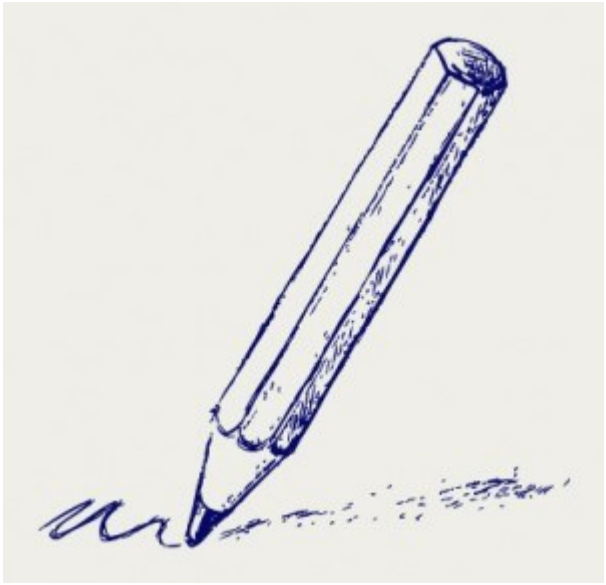
This week, at the ITech Law World Technology Conference in New York, Seyfarth attorney Dan Hart briefed members of the International Technology Law Association's Intellectual Property Committee about the European Commission's proposed Directive on trade secret protection. As we have written, the new Directive, if enacted, will substantially alter the legal landscape in Europe regarding trade secret protection and will enhance cross-border certainty within the EU. Dan's presentation generated lively discussion among lawyers from a wide variety of jurisdictions regarding the similarities and dissimilarities between European and US trade secret law and similar attempts in the US to federalize trade secret protection.

The ITech Law World Technology Conference concludes today. If you are attending the ITech Law World Technology Conference, please be sure stop by our table in the Vanderbilt Room of the Waldorf-Astoria Hotel.

Trading Secrets

Once You've Made Your Restrictive Covenant Bed You Must Lie Upon It…

By Ming Henderson and Razia Begum (July 30, 2014)



The traditional approach taken by the English Courts to restrictive covenants was confirmed in the decision of the Court of Appeal in *Prophet plc v Huggett [2014] EWCA Civ 1013*. The Court of Appeal overturned a High Court judge's decision that the words "or similar thereto" should be added to the relevant clause in order for it to make commercial sense and the injunction against the employee was disregarded.

Prophet is a software company which sells its software products to the fresh produce industry. Mr Huggett was a sales manager for Prophet. His contract contained (amongst other post-employment restrictions and obligations) a 12-month non-compete clause from selling Prophet software following the termination of his employment. Mr Huggett joined a competitor which sold competing software but, technically, not Prophet software. Therefore, on a literal interpretation, the non-compete provided no protection to Prophet and proved futile, as only Prophet sold Prophet software.

The Court of Appeal unanimously confirmed the position that restrictive covenants should be strictly interpreted unless the covenant is ambiguous and the literal meaning could lead to absurdity. Only in the latter case, could a restrictive covenant be subject to judicial reinterpretation to give effect to a commercially sensible solution which reflects the true intention of the parties. But this was not the case here – the restrictive covenant was simply poorly drafted and the draftsman (although professional) failed to consider the extent of any practical benefit which Prophet would derive from the restriction on competition.

This case serves as bold reminder that:

- **Careful thought and drafting:** Restrictive covenants should be carefully considered and drafted. The drafting and literal language should reflect the true intention of the employer. If it's not covered by the restrictive covenant itself it's not likely to be enforceable. In practical terms, employers should at the outset of the drafting process consider what competitive activities and eventualities it wants the employee to be prevented from engaging in following the termination of employment.

- **Once you've made your bed, you must lie in it:** The English Courts generally prefer not to interfere with and change private contracts agreed between parties. This case was an illustration of that very point. An employer therefore cannot general rely on the Court to rescue it from a badly drafted covenant and cure its bad deal. In the Court's words, "Prophet made its . . . bed and it must now lie upon it".

When Is The Possession of International Trade Secrets A Mistake Or Economic Espionage: Contrasting U.S. v. Yeh with U.S. v. Liew

By Timothy Hsieh (August 5, 2014)

The judgments rendered in two recent 2014 federal criminal cases reveal the inherent complexity in prosecuting international trade secret misappropriation claims.

In *U.S. v. Liew*, Judge White of the U.S. District Court for the Northern District of California sentenced defendant Walter Liew to 15 years in prison for misappropriating trade secrets from chemical giant DuPont and selling them to an overseas Chinese company known as the Pangang Group, based in Chengdu. It was proven during the trial that Liew and his company, ironically named USA Performance Technology, received over $27.8 million in compensation for selling DuPont's industrial trade secrets to Pangang, the trade secrets including technical blueprints belonging to DuPont related to the manufacturing of titanium dioxide, a white-colored pigment used in many commonplace consumer products such as paper and plastic. Thus, Liew's intent to misappropriate trade secrets was established beyond a reasonable doubt by U.S. Attorneys.

On the other hand, in *U.S. v. Yeh*, a Texas jury acquitted former Texas Instruments (TI) employee Ellen Yeh on all counts brought against her (including trade secret misappropriation) based on proprietary information she admitted downloading before leaving the U.S. to work for a semiconductor manufacturing company in China. In her testimony, which she submitted polygraph results for, Ms. Yeh stated that she had no idea such activity was illegal or unauthorized, was confused about what constituted a TI trade secret vs. non-trade secret, and merely downloaded the files only for safekeeping in case another job opportunity arose to work for TI in China. Therefore, after a nine-day jury trial, she was acquitted because she was not found to have the requisite intent to commit trade secret misappropriation or illegal copying.

Proving Intent to Misappropriate Trade Secrets Beyond A Reasonable Doubt

In the *Yeh* case, it was difficult to prove Ms. Yeh's intent to misappropriate trade secrets beyond a reasonable doubt, which is the standard used under the law, e.g., trade secrets misappropriation prohibited by the Economic Espionage Act and illegal copying prohibited by the National Information Infrastructure Act, a U.S. computer crime law passed in 1996. It is also harder to establish the commission of complex crimes such as criminal trade secret misappropriation because such claims require multiple elements to prove, such as the accused having to know what a trade secret is first (and why it would derive value from not being generally known to the public) and then knowingly, willfully misappropriating the trade secret once having this knowledge.

It may have been harder to prove intent in the *Yeh* case because it only involved the downloading of proprietary information. In the Liew case, not only was their possession of trade secrets (in the form of blueprints) but there were proven sales of that information made by Liew to the Pangang group. Liew also paid former DuPont engineers for trade secrets, so there were financial transactions Liew underwent to acquire the trade secrets in the first place. Therefore, the presence of commercial activity may make it easier to prove intent to misappropriate trade secrets, because it already establishes that the accused knows that the proprietary information he is selling or buying has high economic value.

Knowledge of What Constitutes a Trade Secret v. A Non Trade Secret

In the *Yeh* case, Ms. Yeh asserted that she was confused about what constituted a TI trade secret versus non-trade secret proprietary information. It may be difficult to discern a highly valuable trade secret from information that is already proprietary. Therefore, the burden is on the trade secret holder to educate their employees properly about company information, or to have stricter protection protocols under company policies for information clearly constituting trade secrets. The easier it is to establish that an accused party knows what a trade secret is, the easier it will be to establish the intent of that accused party to misappropriate trade secrets. For example, in addition to being found guilty of paying former DuPont employees to provide him with company trade secrets, Liew was also found guilty of filing false tax returns, making false statements, and witness/evidence tampering. Therefore, it might be clearer in Liew's case that he knew what trade secrets were and also knew their true value – which is why he went to such extents to acquire them and sell them to the Pangang Group.

Limited Time for Prosecution

Having a smaller window of time to pursue remedies for trade secret misappropriation allows a higher likelihood of success. As does ensuring the defendant does not leave the country. Ms. Yeh departed TI over nine years ago. In 2005, because she had been living in China for a while already, the prosecution was stalled for over five years, and even after the grand jury indictment in 2008, she still continued to live overseas in China. Not until August of 2013 did Yeh finally return to the U.S. to face trial after she was detained at the South Korean border in response to a "Red Notice" issued by Interpol at the U.S. government's request. The process would have been much better for the prosecution, strategically as well as time-wise, if the defendant stayed in the United States, like the Liew case.

The Defendant Need Not Actually Use The Trade Secrets

Liew's attorney, Stuart Gasner from Keker & Van Nest, argued that Liew received the trade secrets from a former DuPont engineer who had kept them sitting in his closet for 14 years. He further stated that there was no proof that Liew actually used those secrets to hurt DuPont. Assistant U.S. Attorney John Hemann quickly responded that Gasner's argument that the trade secrets weren't used was "the most insulting thing that has been suggested" and that there was still misappropriation and the sale of such highly confidential, proprietary information.

Takeaways

There are a number of factors, as discussed above, that need to be taken into consideration when prosecuting a trade secret misappropriation claim in a federal criminal case. For a crime as complex as trade secret misappropriation, the more details and facts that can be established about the defendant's state of mind, the stronger the case will be.

United Kingdom Update on Contractual Notice Periods and Restrictive Covenants

By Ming Henderson and Georgina McAdam (August 7, 2014)

An employee cannot 'walk out' and refuse to work to avoid their notice period and the restrictive covenants contained in their contract of employment.

In *Sunrise Brokers LLP v Rodgers [2014] EWHC 2633* the High Court held that an employer does not have to accept that a 'walk out' by an employee will terminate the contractual relationship. The employer has the option to accept the employee's repudiatory breach or to affirm the contract. In addition, although a court cannot order an employee to work, it can grant an injunction ordering an employee to observe the other terms of his contract during his notice period and his post-termination restrictive covenants.

Background

Mr Rodgers was employed by Sunrise on a fixed term contract until 22 September 2014, terminable on 12 months' notice. His contract contained a valid set of restrictive covenants.

At the beginning of March 2014 Mr Rodgers signed another contract with a competitor to commence work on 1 January 2015. On 27 March 2014 Mr Rodgers told Sunrise that he was leaving immediately, which he confirmed in writing in April 2014. Sunrise stopped paying him at the end of March 2014 and confirmed payment would recommence if he returned to work.

Decision

Following Mr Rodgers' resignation with immediate effect, Sunrise had the option to accept his repudiatory breach or to affirm the contract. The Court ruled Sunrise did not lose its right to affirm the contract by its decision to cease payment to Mr Rodgers who refused to work, as the employee must be ready and willing to work in exchange for wages and vice versa. Failure of either of these mutual obligations did not mean the contract ceased to exist. In effect, only one obligation (pay) is suspended until the other obligation (work) is performed.

Mr Rodgers was not entitled to payment irrespective of work, as the price of the restrictions and other terms to which he was bound under his contract (analogous to garden leave). His entitlement to payment depended on his readiness and willingness to work. It was held Mr Rodgers remained employed until 16 October 2014 (a reduced notice period offered by Sunrise).

The Court agreed that it was forbidden to enforce the terms of Mr Rodgers' contract, if this would compel Mr Rodgers into "forced labour". However, it was appropriate to grant an injunction ordering Mr Rodgers to observe the other terms of his contract (e.g. not working for a competitor and not contacting his former clients), until 16 October 2014.

The post-termination restrictive covenants were reasonable when entered into and could be enforced. Given the fact the contract indicated that the maximum period of restraint required by Sunrise was 6 months from the last client contact and that an employee would usually spend approximately 4 months handing over his/her job, the Court concluded it would be reasonable to enforce the post-termination covenants for 10 months from the last client contact. Therefore, it was held that the restrictive covenants would be upheld until 26 January 2015.

Takeaways

1. Although the courts cannot force an employee to work, they are willing to grant an order requiring an employee to comply with the other terms of his contract, therefore it is essential to have a well drafted and up to date employment contract.

2. During garden leave an employee is entitled to receive pay whilst being asked not to work by the employer but the same does not apply where the employee refuses to work. An employee cannot demand that he/she is put on garden leave. It is the employer's choice.

3. Employers should carefully consider the short and long term impacts of an employee resigning in breach of contract and seek legal advice on immediate actions to be taken. Beyond the restrictive covenant issues, the business may also want to consider how to safeguard confidential information, trade secrets and client contacts.

Kansas Federal Court Denies Preliminary Injunction For Alleged Violation Of Confidentiality And Non-Compete Covenants under Canadian Law

By Paul Freehling (August 11, 2014)

\The plaintiff corporation — now a Delaware LLC based in Kansas — was headquartered in Alberta, Canada at the time its employees signed agreements containing confidentiality and non-compete covenants. The agreements designated the applicable law to be that of Alberta. When its ex-employees allegedly violated the covenants, the plaintiff sued them and their new employer in a Kansas federal court. Relying largely on Alberta law, that court recently denied the plaintiff's motion for entry of a preliminary injunction.

Summary of the Case

The court denied the injunction with respect to the covenant of confidentiality, holding that the evidence did not show a substantial likelihood of trade secrets misappropriation. The non-compete prohibited ex-employees from servicing any competitor or customer in any capacity anywhere in the world. No Canadian case was located which enforced such a broad prohibition. The court concluded that neither the balance of harms nor the public interest warranted issuance of the requested injunction. *AgJunction LLC v. Agrian Inc.*, Case No. 14-CV-2069-DDC-KGS (D.Kan., July 23, 2014).

The Corporate and Individual Parties

Plaintiff AgJunction makes and sells "precision" agronomy hardware and software. In November 2012, AgJunction moved its corporate headquarters from Alberta, Canada, to Kansas. Before AgJunction left Canada, its employees signed non-compete and confidentiality covenants governed by Alberta law.

The corporate defendant, Agrian, is a California corporation which, historically, made and sold "compliance" agronomy software. In December 2012, AgJunction licensed Agrian to access the former's software for the purpose of reselling or sublicensing it to specified companies. The license contained a confidentiality provision. In early April 2013, Agrian began developing "precision" agronomy software. One by one during the period August-December 2013, five employees of AgJunction resigned and went to work for Agrian. They also were named as defendants (subsequently, the cases against two of the individuals were dismissed for lack of personal jurisdiction over them in Kansas).

AgJunction's Complaint

AgJunction's largest customer was Crop Production Services (CPS). When AgJunction was informed by CPS of its intent to move its "precision" business to Agrian, AgJunction filed a multi-count complaint against Agrian and the five ex-employees. The complaint alleged trade secret misappropriation, breach of contract, and other wrongs.

"Last peaceable uncontested status"

AgJunction moved to enjoin the defendants from competing. Reviewing Kansas law, the court stated that a preliminary injunction should not be issued unless it restores the "last peaceable uncontested status existing between the parties before the dispute developed." To warrant an injunction, AgJunction was required to make a "strong showing" that it was likely to succeed on the merits. But Agrian began the process of creating "precision" products prior to the time any of the five employees left AgJunction, and so the court concluded that an injunction would "disturb the status quo and is disfavored."

Canadian Law Governing Misappropriation of Trade Secrets

A Canadian employer alleging trade secrets misappropriation must demonstrate that particularized "know how" was taken, not just "general skills and knowledge." AgJunction showed only the latter.

Canadian Law Governing Non-Compete Covenants

The court concluded that "AgJunction has produced some evidence suggesting that defendants, at best, acted in an underhanded manner in their departure from and dealings with AgJunction" but not the requisite "strong showing" that it would prevail at trial. Reviewing Alberta law, the court observed that "Because there is generally an imbalance in power between employer and employee, restrictive covenants in employment contracts receive rigorous scrutiny in Canada." Further, Canadian courts enforce non-compete clauses "only in exceptional circumstances."

Geographically broad non-compete clauses have been upheld in Canada, for example, an assets sale agreement restraining competition in the entire country, but no case was located that supports a global provision. The court stated that Canadian jurists are not likely to enforce an employment agreement covenant prohibiting "a nearly unbounded scope of work with no geographical limitation." Finally, regarding balancing harms and the public interest, the court said that "the harm the injunction would cause defendants is certain, while the evidence that they stole AgJunction's confidential and proprietary information is not."

Takeaways

The opinion in *AgJunction v. Agrian* should be consulted when Canadian law may apply to restrictive covenants. The opinion contains an extensive discussion restrictive covenant disfavor by Canadian courts. Interestingly, AgJunction did not rewrite the choice of law provision in its covenants, to take advantage of the greater likelihood of enforceability, after moving its headquarters to Kansas (*see, e.g., Wichita Clinic, P.A. v. Louis*, 185 P.3d 946, 951-55 (Kans. App. 2008) (emphasizing the sanctity of contracts in enforcing reasonable restrictions, even in employment agreements). However, a preliminary injunction against Agrian might also have been denied under Kansas law unless the expansive breadth of the territorial and prohibited activities provisions in AgJunction's covenants was narrowed.

The French Answer To Flexible Working: The Right To Privacy and To Limit Work After Business Hours

By Ming Henderson (August 19, 2014)

The French Answer to Flexible Working

Ever since the first laws on the 35-hour week were enacted over fifteen years ago, monitoring working time has been a headache for employers in France. With the introduction of new technology and mobile devices, the situation has worsened. The French approach to flexible working is to reaffirm that employees have the right to privacy and in some sectors the obligation to disconnect, as recently shown by the CNIL, the French Data Privacy Watchdog and theSYNTEC Federation.

SYNTEC Agreement: An obligation for employees to disconnect

SYNTEC, the National Federation covering many employers in the IT sector and consultancy firms, recently signed a new collective bargaining agreement on working time limiting work after business hours, due to concerns expressed by Unions about employees' work overload and burn-outs. Rather than a new law banning work after 6pm as was incorrectly reported in several newspapers, effective 4 January 2015, the agreement (which has been extended by law to all employees in this sector, one of the biggest in France) will impose on employees not just a right but an actual obligation to disconnect during daily and weekly rests. Employers will, for their part, be required to carefully manage employee workloads so that minimum rest times can effectively be taken. There is not an opt-out process for employees in the relevant job categories.

CNIL's first official opinion on BYOD

The CNIL's main duties are to inform individuals and corporations about their data privacy rights and obligations, as well as to provide guidelines and regulations on data privacy issues, but it may also impose financial penalties of up to 150,000 Euros per breach.

Where the so-called Bring Your Own Device or BYOD practice exists, employees have access to their professional emails, and the company's data from their mobile phone, personal laptop or tablet. The CNIL, recently published its first official opinion on such practice in its latest newsletter . Rather than fighting it back, the CNIL embraces BYOD but emphasises the need to find a balance between the company's data confidentiality and the protection of the employee's privacy.

To ensure company held data and confidential information are secure, the CNIL recommends companies adopt certain good practices such as: (1) installing software (MDM-Mobile Device Management and MAM-Mobile Application Management for example) that enables employers to encrypt devices and remotely destroy data on employees' devices if needed, (2) classifying data and better managing access rights, (3) storing employees' personal or private data separately from

company data, and (4) finally, adopting an IT policy which defines the company's internal compliance rules.

The CNIL acknowledges that BYOD bears some risks but these are not dissimilar to issues raised by homeworking employees for which there is specific regulation, particularly on costs and working time. Similar to homeworking rules, employer monitoring of employees' devices must not interfere with their right to privacy and must not become a tool to control the employee's activity.

Takeaways

CNIL's implicit approval is good news but employers should ensure the practical recommendations, particularly around monitoring and the right to privacy, are effectively implemented to avoid employee claims, Health and Safety Issues and the intervention of the CNIL.

BYOD also raises many other legal issues not addressed by the CNIL or in the recent SYNTEC agreement, in particular:

- Are mobile devices working tools or personal items? This question is relevant for payroll tax purposes for example and to assess how data is recovered at the end of the employment;
- Is the company at risk for not consulting with the Works Council or the Health and Safety Committee before implementing a BYOD practice?
- How can working time effectively be measured due to the blurred lines between working and non-working times and how far should monitoring of working hours go?

It may be appropriate to include the CNIL's recommendations and to have clear policies in the company Internal Rules ("Règlement Intérieur"), to ensure employees meet their obligations and that a right balance is found so business needs can be met.

Shanghai Courts Provide Additional Relief to Employers for Breach of Non-Compete Agreements

By Wan Li (August 20, 2014)

Non-compete agreements are widely used by employers in certain industry sectors in China to protect their trade secrets and confidential information.

In China, employers may require the employee to continue to perform the non-compete obligation and pay liquidated damages in accordance with the non-compete agreement after breach occurs.

In the past, however, the following uncertainties could impede the employer from obtaining effective remedies against the departing employee.

First, although it is clear that an employee breaching a non-compete agreement must continue to perform his/her obligations under the agreement regardless of whether he/she has paid liquidated damages, it was unclear whether the courts would provide for **mandatory enforcement** when the employee refuses to perform such obligation.

Second, although the employer is entitled to liquidated damages from the employee breaching the non-compete agreement, courts tend to adjust the amount of the liquidated damages by considering the actual loss of the employer, and the salary as well as the non-compete compensation received by the employee. In many cases, employers may not receive the full amount of the agreed liquidated damages.

Two recent Shanghai cases demonstrate that employers may now obtain more complete remedies for breach of non-compete agreements.

In the first case, the Shanghai Labor Dispute Arbitration Committee issued an arbitration award requiring the employee to continue to perform the agreed non-compete obligation owed to the former employer. However, the employee refused to perform such obligation after the arbitration award took effect. Upon the request of the former employer, the People's Court of Pudong District in Shanghai issued an order to mandatorily enforce the arbitration award, which forced the employee to terminate employment with the new employer, which is a competitor.

In the second case, the People's Court of Xuhui District in Shanghai found in favor of the employer on its claim for the agreed liquidated damages (RMB 150,000) to be paid by the former employee for her breach of the non-compete duty. Compared with the salary and non-compete compensation of the employee, the employee's agreed liquidated damages was much higher. In other cases, courts have lower the agreed liquidated damages based on the principle of equality and fairness. However, in this case, the court held that since the actual loss to the employer was difficult to calculate, the liquidated damages should be paid in accordance with the amount agreed by both parties. In principle, employees are obliged to continue to perform the non-compete agreement regardless of whether liquidated damages are payable. In this case, since the non-compete agreement had expired, the employee was only obliged to pay the agreed liquidated damages.

Trading Secrets

These two recent Shanghai decisions provide employers with authority for more effective remedies for breach of non-compete agreements. The first case demonstrates that injunctive relief for breach of non-compete agreements is available. The second case demonstrates that the court will support the liquidated damages agreed by the two parties. In addition to liquidated damages, the employee is obliged to continue to perform his/her non-compete obligation until the agreed term expires. We will keep a close eye on other significant non-compete and trade secrets cases in China.

What You Need to Know About Non-Compete Covenants in India

By Guest Authors Sajai Singh and Soumya Patnaik (August 21, 2014)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry about non-compete covenants in India by technology and corporate attorneys Sajai Singh and Soumya Patnaik of J. Sagar Associates in Bengaluru, India. Sajai serves as the President of ITechLaw, a leading technology law organization. This entry is part one of a two part series on non-competes and trade secrets in India.

-Robert Milligan, Editor of Trading Secrets

A non-compete covenant is a contract, or a clause in a contract, limiting a party from competing with the business or trade of another party. Most commonly such covenants are entered into between employers and their employees, or between companies during a transaction involving transfer of business or goodwill.

Legal Status of Non-Compete Covenants

Section 27 of the Indian Contract Act, 1872 ("ICA") provides the test for determining the legality of non-compete covenants in India. Section 27 of the ICA states that "every agreement by which any one is retrained from exercising a lawful profession, trade or business of any kind, is to that extent, void." The only statutory exception to this is an agreement not to carry on business, of which goodwill is sold.

An agreement in restraint of trade has been identified as one in which a party agrees with any other party to restrict his liberty in the future to carry on trade, business or profession, with other persons who are not parties to the contract in such a manner as he chooses. Non-compete clauses have therefore, time and again, been regarded by courts in India, as restrictive clauses, which undermine a party's freedom to engage in trade. A literal interpretation, of Section 27 invalidates all non-compete covenants, irrespective of their reasonableness, or consideration paid for such covenants. In an employment situation however, such clauses are usually held to be valid during the period of employment, but invalid post-termination.

In *Krishan Murgai v. Superintendance Company of India*[1], the Delhi High Court deliberated over whether a contract of employment, entered into by the appellant with the respondent, which prohibited him from engaging in similar business as that of the respondent, during his employment, and for a further period of 2 years after the termination of his employment was violative of Section 27 of the ICA. The court held that Section 27 does not distinguish between reasonable or unreasonable restraint of trade and therefore any restraint imposed on the employee after the term of employment, would *prima facie* be void and unenforceable.

In *Star India Pvt. Ltd. v. Laxmiraj Seetharam Nayak & Anr*[2], the Bombay High Court had to determine whether an injunction could be granted in furtherance of a negative stipulation, in the nature of a non-compete clause, in an employment agreement. The Bombay High Court held that the injunctive relief sought would not be granted where its effect would be to compel the employee to continue in the services of the employer, against his will.

In *Taprogge Gesellschaft MBH v. IAEC India Ltd*[3], the Bombay High Court held that a restraint operating after termination of the contract to secure freedom from competition from a person, who no longer worked within the contract, was void. The court refused to enforce the negative covenant and held that, even if such a covenant was valid under German law, it could not be enforced in India.

Exceptions to the Rule

Restraint imposed on freedom of trade and business, has been recognised as valid in certain circumstances.

Exception 1

The first of such circumstances is contained in the statutory exception to Section 27, which provides that, if a party sells the goodwill of his business to another he can agree with the buyer that he will not carry on a similar business within the specified local limits. As per Section 27, "one who sells the goodwill of a business may agree with the buyer to refrain from carrying on a similar business, within specified local limits; so long as the buyer, or any person deriving title to the goodwill from him, carries on a like business therein, provided that such limits appear to the Court reasonable, regarding being had to the nature of the business."

In such cases, courts will generally grant suitable injunctive remedies, to prevent a contracting party from carrying on a trade or business, the goodwill of which has been transferred by him for good consideration.

Second Exception

The second exception has been carved out by courts, by subjecting Section 27 to a less literal construction, and pertains to employment relationships. In the case of *Niranjan Shankar Golikari v. Century Spinning & Mfg. Co.*[4], the Supreme Court held that restrictions that are to operate only while the employee is contractually bound to serve his employer are never regarded as being in restraint of trade, at common law, or under Section 27. Therefore, where a clause imposes a partial restraint, prohibiting the employee from performing services in the same area of business, as that of the employer, during the stipulated period of the agreement, such restraint would not violate Section 27.

As far as post-termination employment restraints are concerned, it has been reiterated time and again, that in order to restrain an employee from joining a competitor, the onus would be on the employer to prove that there is actual theft of confidential and proprietary information, and that the loss of trade secrets, or the disclosure of trade secrets to the competitor has caused or is likely to cause damage/loss to the employer. Even in this case, it is likely that courts would only restrain the employee from disclosing any confidential/proprietary information to the competitor, but may not necessarily prohibit him from joining the competing organisation. In any event, the burden of proof in such cases is on the employer, and is very high.

Third Exception

The third exception relates to the restrictions on a franchisee's right to deal with competing products during the subsistence of the franchise agreement. In *M/S Gujarat Bottling Co. Ltd. v. The Coca Cola Co.*[5], the Supreme Court held that some terms of commercial contracts have passed into the accepted currency of contractual or conveyancing relations, and aim at promoting trade and business. Such terms due to their nature and purpose cannot be said to enter into the field of restraint of trade. In this case, the Supreme Court held that a negative stipulation in a franchising agreement, restraining the

franchisee from dealing with competing goods, during the subsistence of the franchising agreement, could not be regarded as restraint of the franchisee's right to trade.

The Need for Change

Although the need to protect contractual autonomy and liberty has been repeatedly expounded by Indian courts, non-compete clauses have been consistently held to be invalid, by virtue of Section 27 of the ICA. Under the present statutory framework, a company is almost paralyzed in terms of preventing an employee with access to confidential information and intimate knowledge of its trade secrets, from moving to a competitor.

---

[1] AIR 1979 Del 232

[2]2003 (3) Bom CR 563

[3] AIR 1988 Bom 157

[4] AIR 1976 SC 1098

[5] AIR 1995 SC 2372

What You Need to Know About Trade Secrets in India

By Guest Authors Sajai Singh and Soumya Patnaik (August 22, 2014)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry about trade secrets in India by technology and corporate attorneys Sajai Singh and Soumya Patnaik of J. Sagar Associates in Bengaluru, India. Sajai serves as the President of ITechLaw, a leading technology law organization. This entry is part two of a two part series on non-competes and trade secrets in India.

-Robert Milligan, Editor of Trading Secrets

Of all the intellectual property generated by a company, its trade secrets are perhaps the most important. However, unfortunately, in India, they are also the most neglected and vulnerable. This vulnerability is due to the fact that India offers no statutory recognition to an establishment's trade secrets. Unlike other jurisdictions, trade secrets are not covered within the purview of Intellectual Property law in India. Companies therefore, have to rely on contractual and common law mechanisms to protect and prevent their proprietary information from falling into the hands of third parties, especially, competitors. Recognising the intrinsic value and vulnerability of trade secrets, courts in India, have generally upheld trade secret protection. This note sketches the broad outline of trade secret protection law existing in India, and examines some of the principles laid down by Indian courts in that regard.

Protection of Trade Secrets in India

The law protecting a company's trade secrets is derived from principles of the law of torts, restitution, agency, quasi-contract, property and contracts. In the absence of statutory regulation, companies have sought protection for their confidential information under two main heads, contractual obligations and equitable/implied confidentiality obligations.

a. Contractual Protection

Non-disclosure agreements remain the primary mechanism for protection of proprietary information in India. Indian courts have recognised the right of an employer to prevent disclosure of classified information by an employee or ex-employee, through covenants in the employment agreement. In one case[1], the Bombay High Court, while considering a confidentiality clause in an agreement, stated that if such clause prevents the employee from divulging any secret information of a specific nature after termination of his service, an injunction in accordance with the terms of such clause, would be reasonable and justified in law.

Similarly, courts have also upheld the validity of restrictive clauses in agreements such as technology transfer agreements, which impose negative covenants on parties, not to disclose or use the information received under the agreement, for any purpose other than that agreed to.

b. Equitable protection

Courts of law in India have not restricted the ambit of trade secret protection to relationships governed by contracts. In the case of *John Richard Brady v. Chemical Process Equipments P.* Ltd.[2] the Delhi High Court invoked a wider equitable jurisdiction, and awarded an injunction even in the absence of a contract, based on an implied obligation to maintain confidentiality on the part of the employee. Similarly, in the Homag India case [3], the Karnataka High Court held that the non-existence of an actionable right would not be assumed, merely due to the absence of a contract between the parties, as long as the petitioner could establish the wrongful disclosure of its proprietary information by the defendant.

Need for Legislation

In India's increasingly competitive environment the protection of proprietary information often foretells the success or failure of a business. Indian companies are keen on protecting their intellectual property under the label of trade secrets rather than patents, as it affords them greater autonomy and secrecy. Therefore, there is a pressing need for a concrete legislation recognising and protecting trade secrets in India. In 2008, the Ministry of Science and Technology, published a draft legislation titled the National Innovation Act, 2008 ('Innovation Bill') that sought to codify and consolidate the law of confidentiality and aid in protecting confidential information, trade secrets and innovation. However, the Parliament, till date, has not directed its attention to the Innovation Bill, and consequently, trade secrets in India, remain unregulated.

---

[1] VN Deshpande v. Arvind Mills AIR 1946 Bom 423

[2] AIR 1987 Delhi 372

[3] Homag India Pvt. Ltd. vs. Mr. Ulfath Ali Khan and IMA AG Asia Pacific PTE. Ltd MANU/KA/1569/2012

Seyfarth Attorneys Facilitate Discussion On Trade Secret Protections and Legislative Developments in US and EU at ITechLaw 2014 European Conference

By Robert Milligan and Ming Henderson (October 17, 2014)

Seyfarth IP, International and Trade Secret Attorneys are participating in the ITechLaw 2014 European Conference in Paris, France this week.

ITechLaw is a not-for-profit organization established to inform and educate lawyers about the unique legal issues arising from the evolution, production, marketing, acquisition and use of information and communications technology.

Seyfarth partner Robert Milligan, an ITechLaw Member of the Board of Directors, will facilitate a discussion with some of the over 300 international attorneys in attendance on "Trade Secret Protections and Legislative Developments in the US and EU," on Friday, October 17th.

Trade secrets and proprietary information are an often overlooked form of intellectual property in some countries or not considered intellectual property in others. Nevertheless, many companies derive tremendous value from such information, and litigation often ensues when misappropriation or breach occurs. Additionally, advances in technology continue to facilitate and encourage the proliferation of information.

The discussion will cover the latest developments in the United States and EU to enhance trade secret protections, including the proposed federal legislation to create a civil cause of action for trade secret misappropriation in federal court and the EU Directive to increase the trade secrets protections afforded to companies with operations in the EU which may greatly enhance cross-border certainty and uniformity across Europe.

The IP workshop will discuss the proposed legislation, the various interests involved, and the pros and cons of such legislation, its chances of success, and it will facilitate a lively discussion of the basic principles any legislation should contain. The discussion will also address whether increase protections for trade secrets will stifle creativity and employee mobility.

The outcome of the discussion will provide a critical assessment of trade secrets, how they are presently protected, and how the United States and Europe are proposing to increase protections for trade secrets, as well as a greater insight on the pros and cons of providing greater protections for trade secrets, while still promoting creativity and innovation.

For reference, please find a discussion paper prepared on these issues for the presentation.

Seyfarth will have a staffed table at the event, Seyfarth attorneys Ilan Barzilay, Ming Henderson, and Robert Milligan are scheduled to attend and participate. For more information, please click here.

French Court Rules That A Confidentiality Clause Does Not Require Any Financial Compensation to Be Lawful

By Ming Henderson (November 20, 2014)

As many readers will know, non-compete clauses in employment contracts are only valid in France if, among other conditions, an employee receives a financial consideration of 40 to 60% salary depending on the sector and the role for the duration of the restriction. But do confidentiality clauses need to be subject to the same treatment?

The recently published decision of the High Court (SNC Adex v/ MD dated 15 October 2014) confirming that a confidentiality clause does not require any financial compensation will be met with a sigh of relief by employers employing staff in France.

"A confidentiality clause does not prevent an employee from finding another job"

This decision, though not entirely surprising, is important firstly because rulings by the High court on confidentiality clauses are rare and can be quoted by employers as authority for cases before other courts. Secondly, the circumstances of the employee were particularly interesting: the employee had argued that following his redundancy as Marketing Director (industrial explosive division), the confidentiality clause in his employment contract effectively prevented him from finding another role because he had always worked in the same niche sector where his skills are rare. He also claimed the confidentiality clause was particularly restrictive as it was neither limited in time nor geographical scope. All these circumstances, the employee argued, meant he was prevented from working for a competitor, and therefore in the same way that a non-compete clause operates, the contractual restrictions imposed on him should only be enforceable if he received an adequate financial compensation.

Not so. The high court disagreed with the employee's reasoning and declared that the clause did not prevent the employee from finding another job, it just imposed on the employee a duty to keep confidential the restricted information he held regarding the company.

Key Takeaways – Confidentiality clauses are a must-have

The decision of the High court is good news for employers, particularly given the facts at stake. Employers should therefore be encouraged to include a robust confidentiality clause in the employee's contract in France and ensure the confidentiality obligations are reconfirmed at the time of termination. Even though there is an implied duty to keep information confidential during the employment contract, this duty falls when the employment contract expires, and the confidentiality clause which needs to be

expressly agreed by the employee prior to the termination will be helpful to protect the employers interests when parting with the employee.

Currently only non-compete clauses are subject to a financial compensation in an employment contract. It will be interesting to see whether, like confidentiality clauses, non-solicitation clauses that apply post termination also continue to be exempt from any financial compensation.

Proposed New Rules on Trade Secrets in Europe – the European Commission Proposal on the Protection of Know-How

By Guest Author Bartosz Sujecki (December 1, 2014)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry by Bartosz Sujecki, an attorney from Bavelaar Advocaten in the Netherlands, on the European Commission's proposed Directive to provide harmonized trade secret protections in Europe.

-Robert Milligan, Editor of Trading Secrets

The protection of trade secrets is very important for every company. At the beginning of a patent, a design or a copyright, there is an idea. The idea must be kept secret in order to enjoy the later protection. Therefore, the protection of know-how is as well essential for the protection of intellectual property rights. In the European Union, the protection level of know-how differs in the Member States. Some Member States do not have any rules regarding the protection of know-how. In only few Member States, the national laws define the term trade secrets or protect trade secrets. Additionally, the national laws of all Member States do not have the opportunity to file for a cease and desist order against infringers of trade secrets. Besides that, the rules on the calculation of damages for the infringement of intellectual property rights are inadequate for the infringement of trade secrets. In addition, the national rules do not have criminal sanctions in cases of infringement or even theft of trade secrets. Another problem of the national laws of the Member States is that they do not have any rules regarding the protections of trade secrets during litigation.

Due to the divergences in protection of trade secrets in the different national laws of the Member States, companies in the European Union have called for the introduction of harmonized rules for the protection of trade secrets within the European Union. The absence of rules regarding the protection of trade secrets is having negative effect of the Internal Market in the European Union.

On 28th November 2013, the European Commission has therefore introduced a Proposal for a Directive on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013), 813 final. With the introduction of these measures, the European Commission aims to improve the effectiveness of legal protection of trade secrets in the European Union and ensure the competitiveness of European business and research bodies.

In its first Chapter, the proposal defines the scope of application as well as the meaning of trade secrets. According to article 2 of the proposal, trade secrets must have three elements in order to gain protection: First, the information must be confidential. Second, the information must be of commercial

value due to the confidential character. Third, the trade secret holder should have made reasonable efforts to keep the information secret. The definition is based on the definition of "undisclosed information" as laid down in the TRIPS Agreement.

In Chapter II, the circumstances and requirements are set out under which the acquisition, the use and the disclosure of trade secrets is considered to be unlawful, see article 3 of the proposal. If these requirements are fulfilled, the holder of the trade secrets is entitled to seek the application of the measures and remedies as laid down in the proposed directive. The key requirement in this context is the absence of consent of the trade secret holder. In addition, article 3 of the proposal also determines that the use of trade secrets by a third party is as well unlawful, if that third party was aware, should have been aware, or was given notice of the unlawful act.

Chapter III of the proposal establishes the measures, procedures and remedies that the Member States shall make available to the holder of trade secrets in case of unlawful acquisition, use and disclosure of these trade secrets by a third party. Section 1 of Chapter III contains the general principles applicable to the civil enforcement instruments in order to prevent and repress acts of trade secret misappropriation, namely effectiveness, fairness and proportionality, see article 5. Article 6 of the proposal safeguards to prevent abusive litigation. An interesting provision is article 7 of the proposal, which introduces a period of limitation according to which actions for the application of the measures, procedure and remedies must be brought within at least one year but no more than two years after the date on which the applicant became aware, or had reasons to become aware, of the last fact giving rise to the action. Article 8 of the proposal aims to safeguard confidentiality of trade secrets in case of discloser within court proceedings. Section 2 provides for provisional and precautionary measures in the form of interlocutory injunctions or precautionary seizures of infringing goods.

Finally, Sections 3 of Chapter III (articles 11-14 of the proposal) provides for the measures that may be ordered with the decision of the merits of the case. Article 11 of the proposal provides for the prohibition of the use or the disclosure of the trade secrets, the prohibition to make, offer, place on the market or use infringing goods and corrective measure. The corrective measures request the infringer to destroy or deliver to the holder of the trade secrets all information he holds with regard to the unlawfully acquired, used or disclosed trade secrets. The rules regarding the compensation of damages are set out in article 13 of the proposal. The calculation of the damages is based on all the relevant factors, such as the negative economic consequences, which the injured party has suffered. However, in certain cases other than economic factors, such as the moral prejudice caused to the trade secret holder, can be taken into consideration in the calculation of the damage.

With these proposed rules, the European Commission introduced a new framework of protection of trade secrets. In general, these new instruments can be seen as an appropriate solution for the protection of trade secrets in the European Union. On aspect of the proposal needs, however, still to be adjusted. One of the key issues of the enforcement of intellectual property rights as well as trade secrets is evidence. This proposal does not contain any rules with respect to the facilitation of the burden of proof. Therefore, this proposal should be adjusted on this point.

Bartosz Sujecki, PhD, partner Bavelaar Advocaten, Amsterdam, the Netherlands.

As previously reported here, the EU Council issued its position on the directive in the spring of 2014. In general, the Council supports the Directive with some minor changes: a) the Council proposes a six–year limitation period on suing over trade secrets compared to the two years proposed by the Commission; b) the Council's version clarifies that national laws may provide greater protection for trade secrets than that set out in the directive; and c) and the Commission's draft required a trade secret holder to show that an alleged infringer had acted 'intentionally' or with 'gross negligence' and

the Council has removed this requirement. The Council has also requested changes to allow the restricted disclosures of trade secrets during and after trade secret litigation which are broader than permitted in the Commission's proposal.

The Directive is currently being reviewed by the EU Parliament's Legal Affairs, Internal Market, and Industry Committees and their decisions have not been released yet. While the Parliament has not yet voted on the proposal, it is expected that the matter will be scheduled for a first reading in the Parliament during the first half of 2015.

First United Kingdom Decision on Tweeting in Workplace

By Ming Henderson and Razia Begum (December 22, 2014)

Season's Tweetings

In the first UK high court decision on tweeting, the Employment Appeal Tribunal has held that dismissal of an employee for offensive posts on his private twitter account could potentially justify termination under the UK's unfair dismissal rules.

The employee was dismissed after a colleague raised an anonymous complaint about the content of his tweets. The Court held that termination of an employee for offensive comments on his social media account could fall within the 'range of reasonable responses' open to employers. The employee's right to freedom of expression needs to be balanced against the employer's concern to protect its reputation.

To decide whether termination was justified, UK Employment Tribunals will look at the entire picture, including:

- Was the twitter account relevant to the employee's role? In this case, the employee used the twitter account in his role as an internal investigator, to monitor the posts of other employees.
- Was the twitter account genuinely private? If it linked the employee to the employer, or was followed by a number of work colleagues or customers, it may not be seen as private.
- Did the employer's social media policy or disciplinary rules make clear that offensive twitter posts could result in discipline, up to and including termination?
- Is there evidence of actual damage to the employer's reputation, such as complaints from customers or wider publicity?

This case extends the principles already applied to Facebook comments, as in the case of *Apple v Crisp* where termination was justified for an employee who criticized Apple's products on Facebook in breach of a clear internal policy.

[*Game Retail Ltd v Laws*]

Social Media and Privacy

Tips For Protecting Trade Secrets In The Social Media Age

By Erik Weibust (February 4, 2014)

Social media clearly has numerous uses and benefits, as hundreds of millions of users worldwide can attest. From connecting with a long lost friend, to marketing a new product or service, to organizing a high school reunion or even an uprising in the Middle East, social media has become a ubiquitous part of our lives. But its rapid proliferation comes with risks.

In addition to the hazards to individuals on which the media regularly reports — invasion of privacy, harassment, bullying and the like — the increased risks to employers are just as compelling, albeit perhaps not as sensational. Most employers today have implemented social media policies that govern such things as if and when employees may access social media during the workday and appropriate uses thereof, but many companies fall short in protecting their trade secrets and customer relationships or goodwill.

Employees, especially younger ones, may unwittingly put their employers at risk simply by connecting with customers and/or vendors on LinkedIn, or by boasting about their latest achievements on Facebook or Twitter. Or they may be using social media intentionally to solicit customers or employees after termination.

As the line between business and personal information becomes increasingly blurred, employers must be cognizant of the risks inherent with the increased use of social media and take affirmative steps to protect their trade secrets and customer relationships before it is too late. Once a trade secret has been disclosed, its protections cannot be recovered; and once a customer leaves, he or she may never return.

Setting Expectations

The most basic step that any employer should take to protect itself is to set expectations for its employees. In addition to creating the kind of culture where employees want to be protective of their employer, this can be accomplished by implementing policies that limit what employees are permitted to post on social media, and the security or privacy measures that must be put in place if they do so.

For instance, subject to the strictures of the National Labor Relations Act, employees should not be permitted to comment publicly on confidential projects or issues, even if they believe it is only to their "small" group of friends. While this is universally true, any policy should explicitly reference social media. Moreover, if employees are permitted to connect with customers and vendors on LinkedIn, their list of contacts should be set to private so that other LinkedIn users cannot view them. This type of policy is the building block for all others, and it isn't enough simply to have such a policy in place; it must clearly and repeatedly be explained to employees, and perhaps even be the subject of an annual training.

While most employers have confidentiality and nondisclosure policies and agreements in place, they oftentimes do not specify that customer contact information, preferences, and the like that are maintained on LinkedIn and other social media sites fall within the strictures thereof. These policies and agreements should require that such information be deleted immediately from the employees' accounts if they leave the company for any reason (just as hard copy customer lists must be returned or destroyed).

Although potentially difficult to enforce on their own, absent evidence of misappropriation or improper solicitation, policies such as this can influence a court's opinion of a noncompliant former employee and add support to a request for injunctive relief should litigation be initiated. Of course, one purpose of these policies is to set clear expectations so as to avoid the need for litigation in the first place.

Who "Owns" Social Media?

Once employee expectations are established, the next thing an employer should do is assert an ownership interest over social media accounts and content, even if that content is already identified as confidential and must be deleted when the employment relationship ends. Few courts have addressed the issue of who "owns" social media. It is a difficult issue because accounts are often free and employees have already joined at the time of hire. Employers should, at the very least, have policies in place that inform employees that the company owns any content that was developed on the job or using the employer's resources or confidential information.

For instance, the policy should be clear that customer information and goodwill are the company's property even if posted on an employee's LinkedIn account. (This policy must go hand in hand with the confidentiality policies discussed above or it will be ineffective.) There will always be disputes over whose goodwill it actually is, and social media ownership policies will certainly not be enforced by every court under every set of circumstances, but it is better to implement such a policy than face the risks of not doing so.

Last year, in Eagle v. Morgan, a federal court in Pennsylvania ruled that a company could not assume its former CEO's LinkedIn account after she was terminated because although the company had expressed "an intense interest in the issue involving ownership of LinkedIn accounts," it was clear that on the date the CEO was terminated "no policy had been adopted to inform the employees that their LinkedIn accounts were the property of the employer." Had the company implemented such a policy, the outcome may have been different.

On the flip side, in Ardis Health LLC v. Nankivell, a federal court in New York ruled that a former employee must turn over the login, password and other access information to several websites, blogs, and social media pages that she had created and maintained for her former employer, because the employee had signed an agreement at the outset of her employment that all work created or developed by her "shall be the sole and exclusive property of [the employer], in whatever stage of development or completion," and that she must return all confidential information upon request. The existence of such an agreement in this instance protected the company.

Where there is no policy or agreement, a court may leave the question of ownership to a jury, which is not a good result for employers, as jurors will not want to believe that their employers can appropriate or monitor their social media accounts. InPhoneDog v. Kravitz, a federal court in California denied a former employee's motion to dismiss claims by his employer, alleging that the former employee unlawfully continued using the company's Twitter account after he quit. There was no policy or agreement in place in this case, and the ultimate outcome will necessarily turn on who actually owns the Twitter account.

Similarly, in Christou v. Beatport LLC, the plaintiff claimed that a former employee misappropriated its trade secrets, including login information for profiles on MySpace and lists of MySpace "friends." The defendants argued that a list of MySpace friends "is broadcast to the public via the Internet and thus cannot be considered a trade secret." A federal court in Colorado denied the defendant's motion to dismiss, holding that whether the information was a trade secret is a factual issue, but opined that:

Social networking sites enable companies … to acquire hundreds and even thousands of "friends." These "friends" are more than simple lists of names of potential customers. "Friending" a business or individual grants that business or individual access to some of one's personal information, information about his or her interests and preferences, and perhaps most importantly for a business, contact information and a built-in means of contact. Even assuming that employees generally knew the names of all of the "friends" on [the former employer's] MySpace pages, it is highly unlikely, if not impossible, that employees knew the contact information and preferences of all those on the "friends" list from general experience.

This is an evolving area of law, and information that was protectable 10 years ago may not necessarily be protectable today.

In Sasqua Group Inc. v. Courtney, a federal court in New York ruled that LinkedIn connections and Facebook relationships with clients cultivated by a former employee were not trade secrets belonging to the firm because although that information "may well have been a protectable trade secret in the early years of [the company's] existence when greater time, energy and resources may have been necessary to acquire the level of detailed information to build and retain the business relationships at issue … for good or bad, the exponential proliferation of information made available through full-blown use of the Internet and the powerful tools it provides to access such information [now] is a very different story."

While this case is a classic example of bad facts making bad law, having policies in place at the very least sets expectations for employees, and at best it could carry the day in court.

Beware of Overreach

When implementing policies and agreements related to social media, employers must beware not to infringe upon employees' rights under state or federal law, including the National Labor Relations Act, which safeguards employees' right to engage in "protected concerted activities," Additionally, many states have now enacted or proposed some form of social media privacy laws, some of which prohibit employers from requiring employees or applicants to disclose login information to social media accounts and retaliating against those who refuse to do so.

Employers must also ensure that their own conduct does not run afoul of any laws, including the federal Stored Communications Act, which prohibits the unauthorized access of electronic communications and has been applied to social media. Earlier this year, in Ehling v. Monmouth-Ocean Hospital Service Corp., a federal court in New Jersey held that an employee's Facebook posts were protected by the Act because she had configured her privacy settings to restrict posts to her "friends" (but found that the employer had not violated the act by viewing the employee's wall, because a co-worker, who was one of her Facebook friends, showed the post to their employer).

Similarly, in Maremont v. Susan Fredman Design Group Ltd., a federal court in Illinois refused to grant summary judgment to an employer on claims brought by an employee alleging that it had illegally accessed her Twitter and Facebook accounts while she was on medical leave, finding that there were factual disputes as to whether the employer exceeded its authority in accessing those accounts.

Legal issues aside, most employers do not want to create a culture where their employees are constantly in fear of being monitored, which will harm morale and decrease loyalty. This can have the exact opposite effect of what the policies are intended to promote, as disgruntled or disloyal employees are the most likely to take actions harmful to the company.

What Constitutes Solicitation on Social Media?

Regardless of what policies and agreements are implemented, employers must typically still establish that a former employee misappropriated trade secrets and/or improperly solicited customers or employees to obtain relief. The lines are not as clear as they were in the past, however. Does "friending" a customer on Facebook constitute solicitation? Updating one's LinkedIn account to identify a new employer? Tweeting how great a new employer's product or service is? These questions largely remain open and have not been addressed in most jurisdictions.

In fact, recent research has uncovered no published decisions in the employment context regarding what constitutes improper solicitation using LinkedIn, the most prolific business-centric social media site that has more than 225 million users worldwide.

However just last month, a Massachusetts court issued an unreported decision in KNF&T Staffing Inc. v. Muller, holding that updating a LinkedIn account to identify one's new employer and to list generic skills does not constitute solicitation. In this rather narrow decision, the court did not address whether a LinkedIn post could ever violate a restrictive covenant, and several other cases involving this issue settled before it could be resolved.

Outside of the employment context, the Court of Appeals of Indiana, in Enhanced Network Solutions Group Inc. v. Hypersonic Technologies Corp., held that a nonsolicitation agreement between a company and its vendor was not violated when the vendor posted a job publicly on LinkedIn and an employee of the company applied and was hired for the position, because all major steps that led to the employment were initiated by the employee.

In the context of Facebook, a Massachusetts court ruled in Invidia LLC v. DiFonzo that a hairstylist did not violate her nonsolicitation provision by "friending" her former employer's customers on Facebook because "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."

Likewise, in Pre-Paid Legal Services Inc. v. Cahill, a former employee posted information about his new employer on his Facebook page "touting both the benefits of [its] products and his professional satisfaction with [it]" and sent general requests to his former co-employees to join Twitter. A federal court in Oklahoma denied his former employer's request for a preliminary injunction, holding that communications were neither solicitations nor impermissible conduct under the terms of his restrictive covenants.

In sum, common sense continues to reign supreme in determining what constitutes solicitation in the age of social media, and if it looks, tastes and smells like solicitation, it probably is. Nevertheless, it is imperative that employers protect their trade secrets and goodwill by setting clear expectations and implementing policies and agreements that clearly express those expectations and provide a means by which to enforce them if necessary.

Big Data and IP Business Strategy

By Guest Author Joren De Wachter (March 19, 2014)

As a special feature of our blog –special guest postings by experts, clients, and other professionals –please enjoy this blog entry about the big data and IP business strategy by technology lawyer and IP strategist Joren De Wachter. Joren serves as a Co 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 and for more on Big Data, please see our webinar on the Big Data Revolution.

-Robert Milligan, Editor of Trading Secrets

Big Data is an important technological change happening around us.

How should businesses react? What is the right business strategy? And, as part of such business strategy, what is the right Intellectual Property Strategy?

It can be the difference between success and failure.

1. What is Big Data?

"Big Data" is the revolution happening around us in the creation, collection, communication and use of digital data.

In the last couple of years, humanity's capacity to create data, to communicate and to process them, has increased manifold.

According to IBM, we produced 2.5 Exabyte (that's 2,500,000,000,000,000,000 or 2.5×1018 bytes) of data every day in 2012.

But the total amount of data, already beyond easy intuitive grasp, is not the key characteristic of Big Data. Its key characteristic is the continued exponential growth of those data.

While 90% of all data in existence today was created in the last two years (which means that, in less than 18 months, we create more data than has been created since the beginning of humanity, roughly 150,000 years ago), the most important point is this: those 90% created in the last two years, that what we consider to be enormous amounts of data today, will be dwarfed into complete insignificance in a couple of years' time.

Humans are not very good at really understanding exponential mathematics, or at grasping its impact. This blogpost will give an insight into how technology businesses and their investors should plan and prepare for the Big Data Tsunami that is heading their way. And not just today, but for the foreseeable future. For there is no indication that this doubling of computational power (Moore's law), the doubling of storage capacity or the doubling of communication capability – each occurring in 18 months or less – is about to slow down in the next couple of years.

This presents every business with a serious challenge: how will the emergence of Big Data affect the way the business uses its intangible assets? As we know, most assets these days are intangibles, also known as Intellectual Capital or Intellectual Property.

Arguably, Intellectual Capital is at the heart of any innovative business. Using it better will be the recipe for future business success. And failing to use it better will be a recipe for failure.

2. Framing the discussion around Big Data and Intellectual Capital Strategy.

a) What do we mean by "data", and what is the difference with "information" and "intelligence"?

Data is a very wide concept. Everything created digitally is covered. From every document on your desktop to any picture posted by any user of social media. But it's much more than that. It also means that, e.g. all the 150 million sensors of the Large Hadron Collider in Geneva, delivering data 40 million times per second, are included in the concept of data. If all of those data would be recorded, they would exceed 500 Exabyte per day – 200 times more than the world creation of data per day according to IBM as referred to above. However, those data are not actually produced, recorded or processed – before that happens, massive filtering takes place. In reality, the LHC produces a mere 25 Petabyte per year of data (a Petabyte is 1×1015, so 1/1000th of an Exabyte).

The implication is that there are enormous potential amounts of data that will be created and processed, once our computing and communication capability allow for it.

But "data" means more than that. It also includes everything created by any kind of sensor, but also by any camera, the input of any user, any person operating a computing device (PC, mobile, tablet, etc). Any project, any plan, any invention, any communication is also included.

And all of those data increase exponentially, roughly every year or so.

What is the relation between "data" and "information"? In essence, they are the same. Every bit of data has information. The nature of that information and its potential value are determined by analyzing it. This is where we start talking about the meaning of data, and the intelligence that can be extracted from them.

However, while many definitions and approaches are possible in respect of how information becomes useful, and about the value of analysis and intelligence, a simple observation will be sufficient for the purpose of this blogpost.

That observation is that any subset of data, such as useful data, or intelligent data, or structured data, will grow in a similar, exponential fashion.

The implication of this observation is that it is not only "data" that grows exponentially, but also, by necessary implication, "knowledge" or "useful data". So, we need to assess Intellectual Property strategies in a world where the amount of knowledge grows exponentially.

b) The importance of algorithms

The analysis of data, or indeed pretty much any meaningful way of using data, is done through using algorithms.

Trading Secrets

An algorithm describes a process for calculation, processing or reasoning, and allows to extract meaning and understanding from data. This, in turn, increases the value of the data – algorithms make the data speak to us.

This is where data turn into intelligence; it is through applying algorithms that data start to make sense, and can give us additional information.

One of the great potentials of Big Data is the capability to recombine data from different sources, and compare and analyze them. This allows finding new correlations – something that will help us understand how society works, and how one phenomenon works on another.

For example, analysis of the raw data of drug prescription in the National Health Service in England and Wales, allows to find correlation with certain hospital visits for conditions that are indirectly caused by certain drugs, which have not been noticed by the clinical trials (or which the drug companies have kept hidden from publishing).

The potential value of Big Data, and the use thereof, is enormous. McKinsey, the consultancy, estimates that Open Data would add between $3tn and $5tn to the world economy – that's an economy with a size somewhere between Germany and Japan.

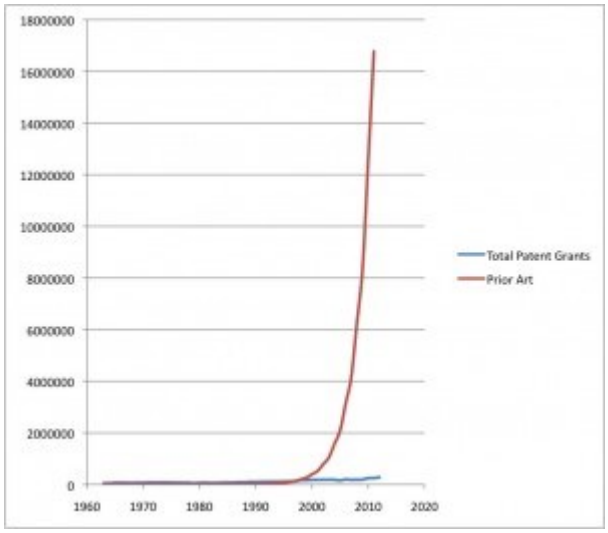
And algorithms are the key to unlocking this value of Big Data; hence they will be key in any IP Strategy.

c) What is Intellectual Property Strategy?

Intellectual Property Strategy means that business understands what their Intellectual Capital consists of, and uses it in the most optimal way to support the business strategy. It looks at a lot more than just patents or copyrights, the technical aspects of IP rights, but considers the whole range of Intellectual Capital.

Key aspects of IP Strategy consist of recognizing and understanding Intellectual Capital, assessing how they are used to support the business model and keeping the right balance between an open approach and using protection techniques (such as patents or copyright), by taking into consideration the impact of Open Innovation and Open Source.

In essence, it is the tool to bring innovation to market, and to scale innovation to new markets.



<u>3. Impact of Big Data on IP Strategy.</u>

This blogpost will look at how Big Data will impact IP Strategy from five angles. These five are 1) patent strategy 2) ownership of data 3) copyright 4) secrecy/know-how and 5) IP value and strategy of algorithms.
They are all essential parts of an IP Strategy.

a) Patent strategy.

Patent strategies can be quite different from one

industry to another.

However, there are some common elements to consider, and they can be summed up in two observations. The observations are that both obtaining and using patents will become much harder. As a consequence, the business value of patents is likely to drop significantly.

Obtaining patents will become much harder

The observation is straightforward, but very important: if the amount of available information doubles every 18 months, the amount of prior art also doubles every 18 months.big data and patents linear prior art.

Patents are exclusive rights, granted on novel and non-obvious technical inventions. The granting of patents is based on the assumption that the patent offices will know existing technology at the time of the patent application, and refuse the application if the technology described is not “novel”.

However, if the amount of existing information grows exponentially, this means that in principle, the rejection rate of patents must also grow exponentially, to the point where it will reach 100%.

The reason is simple: the number of patents does not double very fast – in the last 50 years, it has doubled only twice in the US. The exponential growth of prior art (remember – this is a phenomenon humans intuitively struggle to understand) means that the amount of information that would disallow the granting of a patent – and that is any patent – also grows exponentially.

So, unless the granting of patents also grows exponentially, the area of technology that is patentable will shrink accordingly. Since patents are granted by human operators (patent examiners), and the number of patent examiners cannot grow exponentially (within a couple of years, most of the workforce would have to consist of patent examiners, which would be absurd), the number of patents will fall behind. On an exponential basis.

More importantly, if the patent offices would do their job properly, and only grant patents on technology that is actually new, the rejection rate would soar, and would reach very high levels (up to 100%), within a relative short time span.

This means that the risk of having a patent rejected two or three years through the application process, will rise significantly.

However, this phenomenon is not very visible yet. One of the key reasons why the impact of the Big Data explosion of accessible information is not very visible at the moment in the way patents are being granted, is because the patent offices don’t actually look at prior art in a way that takes into account the exponential growth of non-patented technology information.

Most patent examination processes review existing patent databases, and will establish novelty against existing patents rather than the actual state of technology. This made sense in a world where the speed of information creation was not an issue, or ran generally parallel to the rate of technology patenting. However, as non-patented technology (and, more particularly, information thereon) doubles every 18 months, the relevance of patent databases to establish whether something is new, takes a significant nosedive.

It is not clear to me whether patent offices realize the exponentially growing insignificance of their traditional data-approach. Once they do, though, they only have two options. The first is to reject most,

if not all, patent applications. The second option is to ignore reality, and grant patents on non-novel inventions. However, this will (and arguably, already does) create huge problems in enforcing or using patents, as explained further below.

Either way, from a purely theoretical level, a novelty-based patent system is unsustainable in an environment of exponentially growing prior art or publicly available information.

From an IP Strategy point of view, this means that businesses will have to become much more selective and knowledgeable in their decision process on what to patent, and how to patent it.

This will affect both the scope of patents (which, in order to remain effective, is likely to become much more narrow), and the rate of success/failure of patent applications, both of which will have a significant impact on the return on investment in patent exclusive rights being sought and used by a business and its investors.

Use of Patents

A similar problem affects the potential use of patents as part of an IP Strategy. There are a number of ways in which patents can be used, but the core function of a patent is to act as an exclusive right – a monopoly – on the production or distribution of a product or service.

This means that "using" a patent effectively means suing a competitor to have them blocked access to market, or charge them a license for allowing them to sell.

However, depending on the specifics of the legal system involved, when a patent holder wishes to enforce a patent, the defendant often can invoke that the patent should not have been granted, because there was prior art at the time the patent was granted.

And, while patent offices do not seem to have a clear incentive to take into account actual reality, including the exponentially available information created by Big Data, when reviewing the application, the situation is very different for a defendant in a patent lawsuit.

They will have every incentive to establish that the patent should never have been granted, because there was pre-existing prior art, and the information in the patent was not new at the time of application.

And one important consequence of Big Data will be that the information available to defendants in this respect, will also grow exponentially.

This means that, again, from a theoretical level, the probability of being able to defend against a patent claim on the basis of prior art, will grow significantly. Because of the lag of time between patent applications and their use in court (it takes several years for an application to be granted, and it may take more time before a court decides on it), the effect of the recent explosion of information as a result of Big Data is not very visible in the patent courts yet. But this is a ticking time-bomb, and, if and to the extent procedural rules do not interfere with the possibility of invoking prior art to invalidate a patent, there is a high likelihood we will see the rates of invalidation in courts increase steeply.

From an IP Strategy point of view, this means that an offensive IP Strategy, consisting of suing competitors or others based on your patent portfolio, becomes more risky. While the costs will continue to rise, the potential of a negative outcome will also increase significantly.

There is a second important issue around use of patents that needs to be addressed here as well. It relates to the algorithmic aspect of patents.

A patent is, of itself, an algorithm. It describes the process of a technical invention – how it works (at least, that's what a patent is theoretically supposed to be doing).

It is therefore quite possible that a lot of algorithms around analysis of Big Data will become patented themselves. It could be argued that this will act as a counterweight against the declining value and potential of patents described above. However, I do not believe that the effect will be anything more than marginal.

The reasons for my opinion are the three challenges affecting the potential value of a patent on algorithms analyzing Big Data.

The first is that many of these algorithms are, in fact, not technical inventions. They are theoretical structures or methods, and could therefore easily fall into the area of non-patentable matter.

The second is that algorithmic patents are particularly vulnerable to the ability by others to "innovate" around them. It is quite unlikely that a data analysis algorithm would be unique, or even necessary from a technical point of view. Most data analysis algorithms are a particular way of doing similar things, such as search, clever search, and pattern recognition. There is, in actual fact, a commoditization process going on in respect of search and analytical algorithms.

As a general rule, in order to become patentable, such algorithms must be quite specific and focused. The broader they are described, the higher the likelihood of rejection because of the existence of prior art. However, this reduces their impact from the perspective of using them to block others access to market. A slightly different algorithm, yielding sufficiently similar analytical intelligence, but outside the scope of the first patent, will often (in my experience almost always) be available. This is due to the generic nature of the different aspects of most data analytical algorithms – it's basically always a combination of checking, calculating, filtering and compressing information (sometimes with visualization or tagging and creation of metadata added); but the potential ways in which these can be combined quickly becomes unlimited.

In practice, it means that a patent around data analysis can almost always be circumvented with relative ease.

But the third challenge is the most important one.

Patents are "frozen" algorithms. The elements of the algorithm described in a patent are fixed. In order to have a new version of the algorithm also protected, the patent will either have to be written very vague (which seriously increases the risk of rejection or invalidity) or will have to be followed up by a new patent, every time the algorithm is adapted.

And the key observation around Big Data algorithms is that, in order to have continued business value, they must be adapted continuously. This is because the data, their volume, sources and behavior, change continuously.
Compare it to the core search algorithms of Google. These algorithms are continuously modified and updated. Indeed, in order to stay relevant, Google must continuously change its search algorithms – if they didn't do so, they would drop behind the competition very quickly, and become irrelevant in a very short time.

The consequence is that, even if a business manages to successfully patent Big Data analytical algorithms, and avoids the pitfalls described above, such patent will lose its value very quickly. The reason is simple: the actual algorithms used in the product or service will quickly evolve away from the ones described in the patent. Again, the only potential answer to this is writing very broad, vague claims – an approach that does not work very well at all.

In other words: the technology development cycles of algorithms applied to Big Data analytics and intelligence are much too short to be accommodated by patents as they exist today.

Therefore, the use of patents will decline significantly; their value for business needs to be continuously re-assessed to address this observation.

From an overall IP Strategy point of view, this means that businesses will have to become much more selective in applying for and using patents. Conversely, investors will have to re-assess their view on the value that patents add to a business.

b) Ownership of data

Data ownership is an interesting, and developing area of law. In most countries, it is theoretically possible to "own" data under the law. The legal principle applied will differ, but is typically based on some kind of protection of the effort to create or gather the data, and will allow to block or charge for access or use.

However, there are a number of challenges related to ownership of data.

These challenges are based on the fact that Big Data is typically described by three characteristics: Volume, Velocity and Variety.

Volume stands for the ever growing number of data, as explained above. Velocity stands for the speed required to gain access to and use data, and Variety stands for the fact that data sources and formats multiply and change constantly.

From an ownership perspective, these charactistics lead us to two ways in which the traditional concept of data ownership is challenged by Big Data.

The first is the simple observation that data are a non-rivalrous commodity. That means that one person's use of data does not necessarily prohibit or reduce the value of use of those data by another person, or by another 10,000 persons.

From a technical perspective, re-use of data is the most common, and obvious, way of approaching data.

But the challenge is neither technical nor legal; it is based on business models and interests.

And those business models and interests point us to two very relevant facts: a) most data are generated by someone else, and b) the value of data increases by their use, not the restriction on their use.

Trading Secrets

The first fact is obvious, but its relevance is underestimated. Most of the business value in Big Data lies in combining data from different sources. Moreover, the actual source of data is often unknown, or derives from different levels of communication. Data from customers will be combined with data from suppliers. Data from government agencies will be combined with data from machines. Internal data need to be compared with external data. Etc. Etc.

Therefore, there is a clear push towards opening up and combining data flows – this is the most efficient and best way to create business value.

And while it is true that from a legal and risk management perspective, many people will indicate the risks related to opening up data flows (and those risks are real), it is my perspective that those risks, and the costs related to tackling them, will drown in the flood of business value creation generated by opening up and combining data flows.

Add in the observation that many governments are currently considering how much of their data will become open. The likely trend is for much, much more public data to be made available either for free, or for a nominal access fee. This, in turn, will increase the potential of re-usability and recombination of these data, pushing in turn businesses to open up, at least partly, their own data flows.

And this leads to the second fact. The value of data is in its flow, not its sources.

Big Data can be compared to new river systems springing up everywhere. And the value of a river is in having access to the flow, not control over the sources. Of course, the sources have some relevance, and control over specific forms or aspects of data can be valuable for certain applications.

But the general rule is, or will be, that gaining and providing access to data will be much more valuable than preventing access to data.

As a result, the question of “ownership” of data is probably not the right question to ask. It does not matter so much who “owns” the data, but who can use them, and for what purpose.

And, as the number of sources and the amount of data grows, it is the potential of recombining those aspects, that will lead to exponential growth in how we use and approach data.

The river analogy comes in handy again: as the number of sources and data grows, the number of river systems also grows – and they will be virtually adjacent to each other. If you can’t use one, you jump to another one; the variety on offer will make control or ownership in practice virtually impossible to operate.

The conclusion on ownership is again best illustrated by our river analogy: we should not focus on who owns the land that is alongside the river; we should focus on being able to use the flow, and extract value from that.

From a practical perspective, it means that “ownership” of data should be looked at from a different angle: businesses should not focus on acquiring ownership of data, but on expanding different ways of using data, regardless of their source.

c) Copyright

Copyright is a remarkably inept system for the Information Society. Its nominal goal is to reward authors and other creators. In real life, it mainly benefits content distributors.

Originally, copyright was typically granted for the expression of creative activity: writing a book or a blog, creating or playing music, making a film, etc.

However, copyright also applies to software code, based on the observation that code is like language, and therefore subject to copyright. As such, copyright covers the code, but not the software functionality expressed through the code.

But does copyright apply to Big Data? And if so, does it have business value?

Data is information. Copyright does not apply to the semantic content or meaning of text written by human authors. In other words, it is not the message that is covered, but the way the message is formulated. If only one formulation is possible, then there is no copyright protection, because there is no creative choice possible. That is, very abridged, what copyright theory states.

Logically, this means that most data will fall outside of copyright. Any data generated by machines or sensors will not be covered by copyright. Any statistical or mathematical data is, as such, not covered by copyright.

That means that a very large subset of Big Data will not be covered by copyright. This legal observation will not stop many businesses from claiming copyright. Claiming copyright is easy: there is no registration system, and there is no sanction attached to wrongfully claiming copyright or claiming copyright on something that cannot be covered by copyright (e.g. machine-generated data).

Another large subset of Big Data is, in theory, covered by copyright, but in practice, the copyright approach does not work. This subset relates to all user generated data. Any picture, video or other creation posted by any social media user online is, in theory, covered by copyright. But that copyright is never actually used.

Users will not be allowed to claim copyright protection against the social media platform (the terms of use will always include extremely liberal licenses, allowing the social media platform to do pretty much what they want with the content).

More importantly, the value of all that user generated content lies in using it in ways that copyright is structurally unable of handling. User generated content, in order to have value, must be freely available to copy and paste, tag, adapt, create derivatives of, and, fundamentally, share without limitation. It is the opposite of what copyright tries to achieve (a system of limited and controlled distribution and copying).

Again, the analysis points to the inappropriate nature of our Intellectual Property system.

Most business value in using Big Data will be in open breach of copyright, typically by ignoring it or, at best, pay some lip service to it (as e.g. Facebook or other large social media do), or will be dealing with

data that are not under copyright, but have not necessarily been recognized yet as such by the court system.

As a result, the copyright aspect of any IP strategy in Big Data will first and foremost have to make the analysis of a) whether copyright applies, and b) whether it adds any business value.

Since the applicability of copyright on machine or user generated content is partly in legal limbo, an appropriate solution for some businesses may be to use the creative commons approach. It helps to ensure that data are shared and re-used, hence increasing their value, and allows, from a practical perspective, to ignore the question whether or not copyright applies. If it applies, the creative commons license solves the problem. If it does not apply, and the data can be freely used, the end result will be, from a business perspective, similar.

A final point on database rights, a subset of copyright for a specific purpose, developed in the European Union.

While database rights may look as a system specifically designed for Big Data, reality shows otherwise.

Database rights don't protect the actual data, they protect the way in which data are organized or represented.

In a typical Big Data situation, they would apply to the structured result of an algorithmic analysis of a dataset. Or they could apply to a relational database model, the way in which an application will sort data that is delivered to it, before specific functionality is applied to it.

While these have potentially quite a lot of value, the concept of protecting them through a copyright-related system suffers from the same weaknesses of copyright itself.

The value of such databases directly derives from a) access to the underlying data and b) the algorithmic process of selecting and manipulating the data, both of which are not covered by database rights. The end result of the exercise, as a snapshot, is covered by database rights. But the logic of importing, selecting and other functions on them, are not.

In other words, it's another Intellectual Property Right that does not focus on the business value of Big Data – which is why nobody really talks about it.

d) Secrecy/know-how

Secrecy and know-how protection can be a very valuable asset of businesses. The most classic example is of course the secret formula of Coca-Cola. It's not actually protected by a formal Intellectual Property Right (anyone is free to copy e.g. cooking recipes), but it has significant business value, and it is protected by other legal instruments. Typically, contract law, with confidentiality agreements, will play a big role in protecting business secrets and know-how, and most legal systems allow businesses to bring legal claims against competitors, business partners or employees who disclose or use secret information in unauthorized ways.

By and large, this approach is used by many businesses. Often, the strategy around protecting Intellectual Capital will consist of understanding what the business secrets are, and building appropriate procedures of protection or disclosure.

Yet, a key consideration for this part of any IP and business strategy is the word "secret."

Secrecy has a major downside: it means you can't talk about, use or disclose whatever is secret in a way that allows others to find out about it. The challenge here is that a lot of the value of Big Data depends, as we have seen repeatedly, on the ability to have access, and preferably open or free access, to as much data as possible.

This means that there is a natural market-driven pressure to businesses, in a Big Data environment, to prefer the use (and therefore an open approach) to data, rather than to limit or restrict use. While it is true that access to certain data can be very valuable, this approach is typically based on the assumption that one knows the data available, and understands at least the most important value considerations in respect of these data.

This is where Big Data presents an important shift: not only does it become much harder to know who owns or generates which data, or what is in those data, it also becomes much riskier not to grant relatively free access to data. This is because there is a lot of relevant, but not necessarily obviously visible, value in the data. A lot of value in Big Data comes from recombining data from different sources, or approaching data in a different way (e. g. compressing data in a visual or topographic way in order to discover new patterns).

As a result, businesses that open up their data are more likely to retrieve value from those data, and those that do, will retrieve more value from the data that is most open and accessible.

These developments will change habits within businesses, who will be pushed by market forces and the need to be more efficient, to open up more and more data sets and data sources. Inevitably, this will clash with strategies to keep information secret.

While it is, in theory, uncertain which way this conflict will play out, we need to be reminded again of the exponential growth of Big Data. The logical consequence of this exponential growth is that the pressure to open up is likely to be much stronger, and yield more direct benefit, than the longer term strategy to keep things secret because one day that may yield an additional benefit.

In other words, it will become much harder for businesses to keep things secret, and there will be growing pressure to open up data streams.

From an IP Strategy point of view, this means that understanding and selecting those intangible assets that have more value as a secret than as an open, accessible intangible asset will become more difficult, but, arguably, also more important. On the other hand, businesses that reject the knee-jerk reaction to keep as much as possible hidden or secret, may find that they evolve faster and generate more new business opportunities. It is not a coincidence that Open Innovation has become such a tremendous success. Big Data is likely to reinforce that evolution.

e) Intellectual Property and value of algorithms.

A point that has been touched upon repeatedly is the value of algorithms in a world of Big Data.

Algorithms are the essential tools enabling businesses to make sense of, and create value out of, Big Data.

Yet algorithms are not, as such, protectable under formal Intellectual Property Rights.

Is this a problem for an IP Strategy? Not necessarily.

After all, an IP Strategy is not just about protecting or restricting access to Intellectual Capital, it is also about positive use of that Intellectual Capital to serve the strategic and operational needs of the business concerned.

The financial services industry has used complex algorithms for many years, particularly in the mathematical structures known as “quants” – the formulae used to operate in and track the highly complex mathematical environments of derivatives, online trading or future markets (not to mention the toxic products that are one of the causes of the crash of 2007-2008).

Yet, many of these systems do not enjoy any formal Intellectual Property Protection. No patents are used, no copyright applies. Secrecy does apply, of course, but the market data themselves are very open and visible; indeed, most of the algorithms depend on liquidity, if not of financial assets, then certainly of financial data.
The pattern is similar for algorithms around Big Data. While some secrecy can be tremendously important for specific parts of algorithmic use of Big Data, the liquidity and open nature of the data themselves will often be at least as, if not more, important.

To that needs to be added the need of continuous change and adaptation of such algorithms – in order to have business value, algorithms need to be “alive”. And in order to be alive, they need to be fed those huge amounts of data for which they have been created.

The analogy with bio- or ecosystems is not a coincidence. Just like biosystems thrive on resources that are freely available as a result of ecological circumstances (the energy of the sun, the oxygen in the air, etc), Big Data ecosystems are emerging and evolving, based on free(ish) availability of data and data streams.

As a result, an IP Strategy towards algorithms will have to take into account their almost biological-like behavior. Clever strategies will therefore allow for processes of evolution and selection to occur – and it is likely that those processes that allow free access to data will outperform, through the force of evolutionary pressure, those that do not allow such free access.

It will be therefore key for any IP Strategy to look at the core algorithms that are at the heart of any business dealing with or affected by Big Data. That will be almost everybody, by the way. And such an IP Strategy will have to consider the benefits to be gained from an open approach, to the risks suffered from closing down access to that new lifeblood of the Big Data Information Age: the flow of data itself.

4. Conclusion

A recurring theme throughout this article has been that the traditional view on data and their use is being challenged.

That traditional view is based on making data and information artificially scarce, and trying to charge for it. Intellectual Property Rights are the most obvious ways of making non-rivalrous commodities such as ideas, technology and data artificially scarce.

Yet, as an inescapable consequence of the exponential growth of Big Data, that approach is now at risk of causing more damage to businesses, rather than providing benefits.

Big Data is like a river system. The value of Big Data is not in its many sources, but in gaining access to the flow, and using it for the strategic purposes of your business.

A traditional IP Strategy, focusing on ownership, is in our analogy akin to focusing on claiming land a couple of miles from the river. It is looking in the wrong direction, and misses most of the value of Big Data. While some ownership of a bit of river banks (the algorithms) may have value, our Big Data River is more complex than a simple estuary – it is like the Delta of the Nile – overflowing regularly, where riverbanks and plots of land all of a sudden disappear or get flooded. And a new Delta comes into existence every 18 months.

Therefore, as a conclusion, IP Strategies around Big Data should focus on the instruments to access and use the flow of data, rather than using outdated models of artificial scarcity that will be overtaken by the exponential growth of Big Data.

California Attorney General Provides Some Guidance on Cybersecurity

By John Tomaszewski (March 27, 2014)

Cross-Posted from The Global Privacy Watch

With all the high-profile cybersecurity breaches that seem to be in the news lately, there is a plethora of "guidance" on cybersecurity. The Attorney General of California has decided to add to this library of guidance with her "Cybersecurity in the Golden State" offering. Cybersecurity is a pretty mature knowledge domain, so I am not quite sure why General Harris has determined that there needs to be additional guidance put in place. However, it is a good reminder of the things that regulators will look for when assessing whether or not "reasonable security" was implemented in the aftermath of a breach. And while there isn't anything new in the guidance, what is informative is what is *not* there.

General Harris' guidance does a good job of turning an oftimes technical topic into something most small to medium business owners can understand. Considering the vector for attacking large companies is the smaller vendor of the big company, this is a quite laudable goal (think Target's HVAC vendor).

The elevation of the "first principles" of 1) Assume You are a Target, 2) Lead by Example (for the CEO), 3) Map Your Data, 4) Encrypt Your Data, 5) Bank Securely, 6) Defend Yourself, 7) Educate Employees, 8) Be Password Wise, 9) Operate Securely, and 10) Plan for the Worst are all good foundations to work from. Unfortunately, these principles are a floor, and a somewhat incomplete floor at that.

Risk-Based Security

The most glaring "first principle" that seems to be missing from General Harris' guidance is "Understand Your Risk." While concepts of risk-assessment methodology are sprinkled throughout the document's text, this foundational principle isn't really called out. Applying "reasonable security" must start with an understanding of what is reasonable. While the data mapping exercise recommended by General Harris is a good start, merely knowing where your data is doesn't actually describe the complete risk profile. What kind of data is present? Where did it come from? How is it used? Where does it go (vendors, or end-of-life)? These are all things that are critical in determining which of the security measures you deploy.

All of the other cybersecurity models start with a risk analysis. NIST and the FISMA frameworks are all risk based. So is theFFIEC's guidance for the financial industry. This is a foundational element that needs to be called out as a "first principle" in and of itself.

Ecosystem Security

In the highly networked environment which is the modern age of service delivery, no business is an island. General Harris' guidance seems to be mostly internally focused – what can the business do to protect itself. As we have seen with the Target hack, one of the additional foundational principles of good cybersecurity is understanding where one sits within the larger ecosystem. The HVAC vendor needs to understand that they have a duty to those clients upstream, but also that they have a risk from *their* vendors downstream. This is also part of the risk-based security approach described above. You can't just look to your own systems, you have to look at the systems in both directions of the supply-chain.

All in all, General Harris' guidance is a good start, but it is missing two highly-critical principles which a number of other cybersecurity frameworks rely on for their foundation. These principles of risk-based security, and a holistic point of view are going to be critical for anyone who wants to avoid having the General look closely at their cybersecurity program because of a breach which effects Californians.

Scott Schaefers Discussing Employee Social Media Privacy – How Employers Can Strike the Necessary Balance

By Scott Schaefers (April 18, 2014)

https://www.youtube.com/watch?v=MDkHChi3-hc

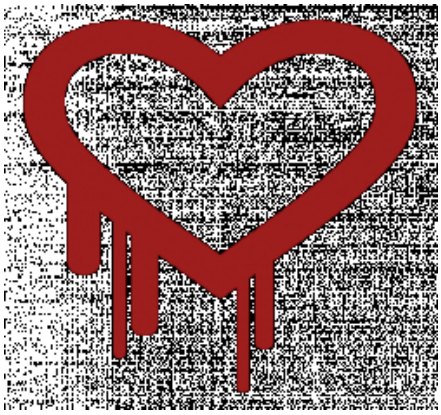
On April 16th, Scott Schaefers spoke with LexBlog's Colin O'Keefe in a live online interview about what employers need to know about the social networking privacy legislation passed by thirteen states in the last two years. Scott discussed Seyfarth's soon-to-be-published survey of that legislation, as well as some ideas of what employers can do to protect its proprietary assets. Those interested in more detail can attend our upcoming April 24th webinar, in which we will present the various features of the new laws, as well as what to expect in the courts.

Though the specific components of the laws vary from state to state, generally speaking they prohibit employers from requiring or requesting employees to provide access to their personal social networking accounts (Facebook, LinkedIn, Twitter, etc.). The penalties for violations also differ depending on the state, and range from mere slaps on the wrist (i.e. New Jersey) to much heavier civil liability, including payment of employees' attorneys' fees (i.e. Oregon). Employers enjoy a number of exemptions and immunities under many of the statutes, including the right to demand access for employer-related accounts, to demand access upon reasonable suspicion of information theft, and to conduct appropriate network and system monitoring.

Some gaps in the new laws will have to be filled in by the courts, including how the laws will impact employers' rights to its trade secrets; the discoverability of social networking account content in litigation now that the content has been given an added measure of privacy; and which state's law will apply in disputes involving multi-state employers. Employers are encouraged to consult with counsel versed in the new legislation to anticipate the effect on their businesses.

Heartache from Heartbleed – The Security of Open Source

By John Tomaszewski (April 25, 2014)



Much has been written about Heartbleed and the significant impact it has on the security infrastructure of the internet. Articles and blog postings have taken both the "sky is falling" and "it's not so bad" points of view. However, there is a more fundamental issue which has raised its ugly head – is the use of open source "commercially reasonable" in a security framework?

- A little history first.

The Heartbeat Extension for the Transport Layer Security (TLS) protocol is a proposed standard which can be found in RFC 6520. Back in 2011, In Robin Seggelmann, who was a Ph.D. student at the University of Duisburg-Essen at that point in time, developed the Heartbeat Extension for OpenSSL. Dr. Seggelmann then requested that the result of his work be integrated into OpenSSL. His code was reviewed by Stephen N. Henson, one of OpenSSL's four core developers. Mr. Henson apparently missed the fact that when a server sends a Heartbeat request to another server, a misformed request can return 64k more data than is appropriate. Simply put, the reviewer missed validating a variable containing a length parameter.

This sounds like a simple mistake which should not have been made in the first place. However, it raises two questions: 1) how was the mistake made in the first place, and 2) why wasn't it caught?

- Open Source – How it Works

Open source code is created and managed by a community of developers. This community isn't a company, or a government standards body. It is merely a group of folks who are doing the work in their spare time. Some money gets donated to these projects, but it is usually very little. The OpenSSL project has received a total of $841 in funding. That is hardly enough money to effectively incentivize folks to engage in the project, much less spend large amounts of time reviewing and auditing the effectiveness of the code.

One of the benefits of the open source movement which is often touted is that with the code out in the open, lots of people have the opportunity to review and evaluate the code independently. Unfortunately, unless those developers are independently wealthy, they have no motivation to so such a review.

It is this lack of funding which can be pointed to as a root cause of both problems – why the mistake was made and why it wasn't caught. Which, of course, brings us to the legal question. Businesses have an obligation to manage their systems in a resilient and reliable way. I won't rehash all the different reasons that mandate good security practices. Much ink has been spilled on that topic already. So, is the use of open source then consistent with this obligation?

- Commercially Reasonable Security

One really cannot paint the open source initiatives with a generalized “this is good” or “this is bad”. Each project has different levels of involvement and different levels of funding. What will be important for businesses to do is treat open source applications the same way that they treat commercial off-the-shelf products. Evaluate the functionality and test the applications before deployment. Some companies have a general prohibition against using open source inside their infrastructure. However, this is usually associated with the need to protect intellectual property of the company. Consequently, the policy isn’t applied to non-IP related environments. While it isn’t completely necessary to prohibit open source solutions in the security infrastructure, companies need to be cognizant that they should be putting the same level of scrutiny toward the security applications they use as the intellectual property they want to protect.

Trading Secrets is on Twitter, Facebook, Google+, Tumblr, YouTube, and LinkedIn

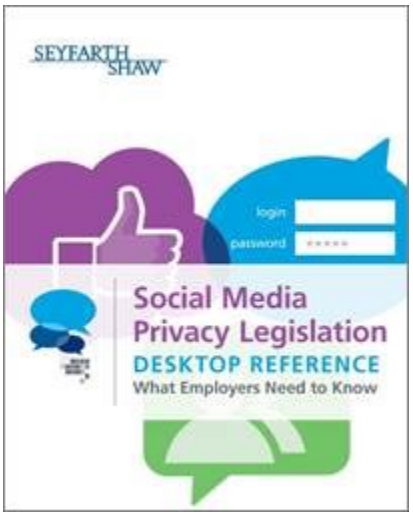
By Robert Milligan (April 29, 2014)

As the social media landscape continues to evolve rapidly, Trading Secrets is committed to keeping pace with this evolution in order to provide the most value for our readers. Regular blog contributors Erik Weibust and Dawn Mertineit, both attorneys in Seyfarth's Trade Secrets Practice, serve as the Trading Secrets "social media directors" and will be actively monitoring the social media outlets for the blog, including Twitter, Facebook, Google+, Tumblr,YouTube, and LinkedIn.

We will continue to educate about news and legislation relating to trade secrets, non-competes, computer fraud, privacy and social media. Through our social media accounts, Erik and Dawn engage directly with influencers in our industry/area of expertise, share content with them, and stay active in conversations through various social media platforms — all with a focus on sharing items that are of value to our audience. We encourage our readers to engage in the conversation as well!

Seyfarth Shaw's Social Media Privacy Legislation Desktop Reference

By Robert Milligan (April 30, 2014)



We are pleased to provide you with our Social Media Privacy Legislation Desktop Reference.

There is no denying that social media is an ever-present issue in the workplace and in our personal lives. Since April 2012, a growing number of states have passed some form of social media privacy legislation. Nearly all other state legislatures, as well as Congress, considered, or are considering, some version of legislation affecting employee privacy and social media. Consequently, employers, HR professionals and in-house counsel are faced with daily situations requiring guidance.

Seyfarth's Social Media Practice Group has prepared an easy-to-use "Social Media Privacy Legislation Desktop Reference," as a starting point to formulating guidance when these issues arise. The Desktop Reference:

- Describes the content and purpose of the various states' new social media privacy laws.
- Delivers a detailed state-by-state description of each law, listing a general overview, what is prohibited, what is allowed, the remedies for violations, and special notes for each statute.
- Provides an easy-to-use chart listing on one axis the states that have enacted social media privacy legislation, and on the other, whether each state's law contains one or more key features.
- Offers our thoughts on the implications of this legislation in other areas, including technological advances in the workplace, trade secret misappropriation, bring your own device issues and concerns, social media discovery, federal law implications, and conflicts of laws.
- Concludes with some best practices to assist companies in navigating this challenging area.

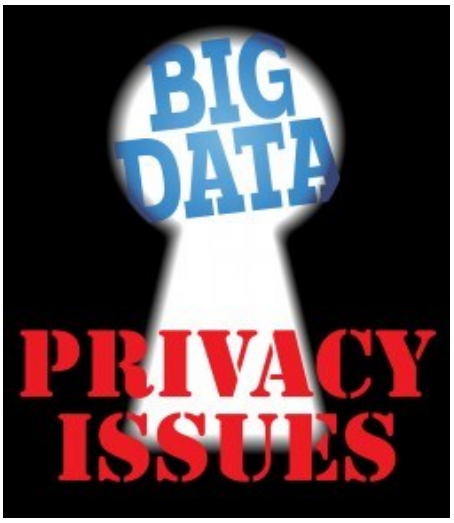
We hope that you find its content useful.

If you would like a hard copy of the Desktop Reference, please contact Robert Milligan at rmilligan@seyfarth.com.

Talking About Big Data: A Framework

By John Tomaszewski (May 7, 2014)

Cross Posted from Global Privacy Watch



The White House released a set of reports this month on Big Data and the privacy implications of Big Data. While a number of folks have been discussing the President's Council of Advisors on Science & Technology ("PCAST") report, I would offer that the Office of Science and Technology Policy ("OSTP") report needs to be read in conjunction with the PCAST report. They do two different things. One is a report on the technical state of affairs, and the other is more of a policy direction piece, which is driven by the technologically-oriented findings. Various points-of-view have been put forth as to the relative merits of each report, but there seems to be an important element missing from both reports. Both reports discuss the need for policy decisions to be based on context and on desired outcomes. Unfortunately, neither report really gives a good taxonomy around the informatics ecosystem to allow for a clear path forward on "context" and "desired outcomes". What I mean by this is best summed up in the comment in the PCAST report which states: "In this report, PCAST usually does not distinguish between "data" and "information".". "Data" and "Information" are very different things, and one really can't have a coherent policy discussion unless the distinction between the two is recognized and managed.

Informatics Ecosystem

The importance of having a clear taxonomy around the informatics lifecycle cannot be overstated. In fact, the challenges of most privacy system implementations reflect this circumstance. For example, attempting to classify "personal information" is not an easy thing. Is a first/last name combination with ZIP personal information? If the name is John Smith and the ZIP is 11004, likely not. However, if the name is John Tomaszewski and the ZIP is 77002, it absolutely is personally identifiable – there is only one of me. Consequently, we need a better way of describing the different relative elements of the taxonomy.

- *Data*

Often, we hear Data and Information used interchangeably. This most certainly not the case. Data, by itself is a representation, or token, of a fact. For example, data is 77002. It is a ZIP code. By itself, data isn't very useful. You can't action raw data. This is the foundational state for the taxonomy. It is also rather rare in the real world.

- *Information*

Information is the next transformative state of Data. It is Data used within a context. The context or "metadata" is what gives value to the Data. To go back to the name and ZIP example, the context that

the last name is Polish and the ZIP is in Houston, transforms two simple data points into Information. You now have an identity of a unique individual.

- *Knowledge*

Knowledge is the next transformative state of Information (a pattern emerges). Not only is Knowledge actionable, it can be used to evaluate and identify past patterns. Instead of only action, Knowledge provides the capability of Understanding.

- *Wisdom*

The final transformative state in this taxonomy is Wisdom (You can call it whatever you want, but this seems to fit). Wisdom is enough Knowledge to be able to start to predict future states.

Each of the states gets triggered by a critical mass of the prior state being fused together. This continued fusion of Data with more and more Data is what makes Big Data useful – you can finally get to Wisdom.

The challenge that the two White House reports have, is that they discuss the risks associated with Big Data without describing which level in the taxonomy they are concerned with. Each level of the taxonomy has a greater and greater potential for impact (both good and bad). Consequently, if you are looking for context-based, outcome-driven policy, you need to know which layer you are in the taxonomy. Neither report does this in an effective manner. As a result, whether you think the reports are a good thing, or "too little, too late" there is still going to be a deficiency in having the policy conversation until those at the table start using the same structure.

Massachusetts Social Media Privacy Bill Hits A (Small) Bump In The Road

By Erik Weibust (July 1, 2014)

Not as widely covered as a bill currently pending before the Massachusetts legislature that would ban employee non-competes in the Commonwealth is a lesser known bill, entitled "An Act Relative to Social Media Privacy Protection" (S.2118), that would prohibit employers from requiring employees or applicants to hand over their social media log-in information, or requiring employees to accept invitations to connect on social media. We first reported on a previous version of this bill in 2012.

Although the social media bill was recently added as an amendment to the Massachusetts Senate's proposed budget, it did not make it into the final budget that the House and Senate are expected to pass. The bill may, however, still pass this legislative session. According to the *Boston Globe*, a spokesperson for the bill's lead sponsor, Senator Cynthia S. Creem, said that her office will work to advance the bill before the session closes on July 31.

As we have previously reported, at least a dozen other states have passed similar social media legislation. Regardless of whether your state has passed or is considering such legislation, all employers should be cognizant of how to protect their trade secrets in the age of social media without running afoul of state social media laws or the NLRA. More on that here.

We will continue to monitor the status of this legislation and report back with any developments.

And speaking of social media, don't forget to follow us on Twitter, Facebook, Google+, Tumblr, YouTube, and LinkedIn, and download our Social Media Privacy Legislation Desktop Reference.

John Tomaszewski Explains the Supreme Court's Riley v. California Decision and What It Means for Consumer Privacy Going Forward

By John Tomaszewski (July 7, 2014)

https://www.youtube.com/watch?v=hzPtTfjJCMw

While the Supreme Court has taken some heat in the past for seeming to misunderstand technology and how it impacts the normal person's life, with *Riley v. California* the Court demonstrated not only an unexpected fluency with how mobile phone technology has evolved, but also with how it has caused our daily sphere of privacy expectations to evolve. Just like when the police want to rifle through your house, when they want to go through your phone, the Chief Justice makes it very simple – get a warrant.

Time to Party Like It's 1999… Again: Information Technology Returns to Center Stage

By Matthew Hafter (July 8, 2014)

With the Securities and Exchange Commission's attention again returning to cybersecurity issues, many registrants are recalling the Commission's intense focus on "Year 2000" issues over a decade ago.

Commissioner Luis Aguilar, in remarks at the SEC's cybersecurity roundtable held on March 26, 2014, made a special point of discussing the SEC's growing concerns about cybersecurity and observed that cyber-attacks have wide-ranging and potentially devastating effects on the economy, individual consumers and on markets and investors. In an April 2, 2014 speech, Commissioner Aguilarstated that the SEC's Office of Compliance Inspections and Examinations will be making cybersecurity an exam priority, warning that the industry should expect that SEC examiners will be reviewing whether asset managers have policies and procedures in place to prevent and detect cyber-attacks and whether they are properly safeguarding their systems against security risks.

These concerns are not limited to those operating in the retail side of the securities markets. All companies subject to reporting obligations under the Securities Exchange Act of 1934 must be aware of how cybersecurity issues should be disclosed. The SEC identified several key areas of potential disclosure in CF Disclosure Guidance: Topic No. 2 .

Risk Factors

The SEC expects registrants to disclose risks related to cyber incidents if those risks make an investment in the company speculative or risky. As with other risk factors, disclosure must be tailored to the registrant's specific circumstances, and include such matters as areas of business or operations that give rise to material cybersecurity risks, and the potential costs and consequences. Companies that outsource must consider cybersecurity risks related to that aspect of their business and how those risks are addressed, including detection of incidents and potential insurance coverage.

Management's Discussion and Analysis

Cybersecurity risks and incidents may result in costs or other consequences that are reportable as a material event, trend or uncertainty that could have a significant impact on a registrant's operations, financial condition and results. Such disclosure could include the impact of increased expenses for data and system security, or the consequences of theft of valuable intellectual property from a cyber-attack.

Description of Business

Registrants must disclose any material effects of cyber incidents on products, relationships with business partners, or competitive conditions.

Legal Proceedings

Cyber incidents may result in litigation or government investigations that meet the disclosure requirements of Item 103 of Regulation S-K. In particular, Instruction 2 requires aggregation and disclosure of "any proceeding [that] presents in large degree the same legal and factual issues as other proceedings." In this way, individual claims related to cyber security incidents may point to a larger disclosure issue – both in terms of meeting the dollar threshold of Item 103 and a failure of internal controls (discussed below) – even if each claim by itself is not material.

Financial Statement Disclosure

There are many ways cybersecurity risks and incidents may affect a registrant's financial statements. These include:

- Costs to maintain system and data security and to prevent cyber incidents.
- Costs to remediate the effects of any data breaches (such as customer loyalty or incentive programs, or providing free credit reports).
- Expenses and losses resulting from claims asserted by customers for product returns, breach of warranty, or breach of contract, or claims from counterparties for their own remediation efforts, as well as the costs of regulatory investigations and potential litigation. The financial statements must deal with accrual and/or disclosure for both asserted and threatened claims; and, in addition, cyber incidents are one of the relatively rare instances where unasserted possible claims are so likely and could be so material that they must be dealt with under the loss contingency rubric.

Disclosure Controls and Procedures

Cyber incidents pose multiple risks to the registrant's ability to control its own data and other assets and to its ability to accurately record and report information required in SEC filings. This may the most painful disclosure of any listed, because it requires the registrant to at least skirt around the edges of information about vulnerabilities it would not want any hacker to know about.

The SEC's Disclosure Guidance on cybersecurity did not present mandatory rules for disclosure, but merely guidance. However, given the SEC's increasing attention to this hot-button issue it is likely that the Commission will be pressing registrants to provide greater attention and detail to these challenges. Privately held companies should also be mindful of the disclosure obligations identified by the SEC when issuing securities in private transactions. We also expect cybersecurity issues to become increasingly prominent in the broader realm of corporate governance as directors are likely to face greater scrutiny under the standards of *In re Caremark International, Inc. Derivative Litigation*, 698 A.2d 959 (Del. Ch. 1996) to assure that the company has adequate information and reporting systems to assure compliance with applicable legal requirements related to data security and privacy.

NLRB Rules That "Liking" A Facebook Comment Is Protected Activity

By Jeffrey Berman and Candice Zee (August 27, 2014)

The National Labor Relation Board ("Board") issued its latest decision on social media issues on August 22, 2014. In*Triple Play Sports Bar & Grille*, 361 NLRB No. 31 (2014), the Board ruled that a Facebook discussion regarding an employer's tax withholding calculations and an employee's "like" of the discussion constituted concerted activities protected by the National Labor Relations Act ("Act"). The Board also held that the employer's internet and blogging policy violated the Act.

The employer, Triple Play Sports Bar and Grille, is a bar and restaurant. In 2011, at least two employees discovered that they owed more in state income taxes than they expected. Employees discussed the situation at work and complained to Triple Play, which had planned a staff meeting to discuss the employees' concerns. Prior to the meeting, a former employee posted the following "status update" to her Facebook page:

Maybe someone should do the owners of Triple Play a favor and buy it from them. They can't even do the tax paperwork correctly!!! Now I OWE money…Wtf!!!

Several Facebook friends posted comments in response to the status update, including two of Triple Play's employees. One employee commented, "I owe too. Such an asshole." A second employee "Liked" the former employee's status update, but posted no comment. When Triple Play discovered that two of its employees had participated in the Facebook discussion, it terminated their employment for disloyalty.

The Board held that Triple Play violated the Act by terminating the employees' for engaging in activities protected by the NLRA. In its analysis, the Board first determined that the Facebook discussion at issue should not be analyzed under the*Atlantic Steel Co*., 245 NLRB 814 (1979) standard. To determine whether an employee loses the Act's protection under*Atlantic Steel*, the Board balances four factors: (1) the place of the discussion; (2) the subject matter of the discussion; (3) the nature of the employee's outburst; and (4) whether the outburst was provoked by the employer's unfair labor practices. The Board noted that the first factor alone supported its conclusion that *Atlantic Steel's* framework is tailored for workplace confrontations with the employer, and not for the type of employee activities in this case.

Instead, the Board applied the standards set forth by the US Supreme Court in the *Jefferson Standard* and *Linn* cases. In*Jefferson Standard*, the Court upheld the discharge of employees who publicly attacked the quality of their employer's product and business practices without relating their criticisms to a labor controversy. *NLRB v. Electrical Workers Local 1229 (Jefferson Standard),* 346 US 464 (1953). In *Linn*, the Court limited state-law remedies for defamation in the course of a union-organizing campaign to instances where the complainant could show that "the defamatory statements

were circulated with malice" and caused damage. *Linn v. Plant Guards Local 114*, 383 US 53, 64-65 (1966).

Applying *Jefferson Standard* and *Linn* to the facts of the case, the Board determined that both the employees' comments and "like" in response to the Facebook post constituted a dialogue among employees about working conditions that was protected by the Act. The Board determined that the evidence did not establish that the discussion was directed to the general public. Although the record did not establish the former employee's privacy settings on Facebook, the Board noted that the comments were posted on an individual's personal page rather than a company page providing information on its products or services. The Board concluded that the employees' comments were not "so disloyal as to lose the Act's protection" because they did not disparage their employers products or services, or undermine its reputation. The Board also held that the comments were not defamatory, but simply a statement of a negative personal opinion of Respondent's owner.

The Board also found that the Triple Play's Internet/Blogging policy in the employee handbook violated Section 8(a)(1) of the Act. The policy warned that "engaging in inappropriate discussions about the company, management, and/or co-workers, the employee may be violating the law and is subject to disciplinary action, up to and including termination of employment."

The Board held that the policy was overly broad and unlawfully chilled employees in the exercise of their Section 7 rights. It further noted that Triple Play's subsequent termination of the employees who engaged in the Facebook discussion further demonstrated the employer's improper prohibition of Section 7 activity. The Board ordered Triple Play to discontinue using the policy.

In his dissent, Member Miscimarra agreed with his colleagues that Triple Play unlawfully discharged the employees and questioned them about their Facebook activity. He disagreed, however with the finding that the Internet/Blogging policy violated the Act. Member Miscrimarra noted that the language of the policy did not expressly or implicitly restrict Section 7 activity, and was not applied to restrict protected activity. Specifically, Triple Play did not apply or refer to the policy when it discharged the employees.

What does this mean for employers? Employers must tread lightly before disciplining employees for social media comments that might appear to be critical of their employer. Employers should also review their social media policies to make sure that they are not in violation of the Act. Remember, the employees in this case were not a part of any union or labor organization.

Security Breach Liability – It's Complicated

By John Tomaszewski (October 6, 2014)

The security breach news cycle continues. There remains a deluge of news stories about point-of-sale terminals being compromised, the ease of magnetic stripes being cloned, and the need for Chip and PIN technology being deployed on credit cards. The legal ramifications of all these events is just starting to become apparent – and it's complicated. Individual liability is beginning to develop.

Security Life-Cycle

Before addressing legal issues, the question (mostly as a result of the Wyndham case) as to what constitutes "reasonable security" should be addressed. Fortunately, the law doesn't require perfect information security. To do that would be to encase your computers and data in a block of amber and toss them to the bottom of the Marianas Trench – which makes them useless. So, for the rest of us who actually want to do business, the question is what do you do to have "reasonable security"?

The FTC has spent a pretty good amount of time going through what they consider "reasonable security". Unfortunately, it isn't a laundry list of "…do this and everything will be all right.' One of the major take-aways of the Wyndham case is that the variable nature of the security threats which are out there demands that the FTC have the ability to evaluate reasonable security on a case-by-case basis. Practically this means you need to have a three-pronged strategy: 1) Risk Assessment (and you have to do this regularly – not just once, and think you are done); 2) implementation of controls to mitigate the threats identified in the first step (not just the ones that the media, or your vendor says you need to use); and 3) incident response protocols.

In general, the usual cause of a breach is a failure to do the first step. If you don't know what your actual risk is (or how it has changed – remember, this isn't a static environment), it won't matter what you do in the control phase as you won't cover all the actual risks that are there.

Legal Implications

With a breach, the default approach of *res ipsa loquitor* is rearing its ugly head. In other words, the plaintiff's bar would have the mere existence of the breach be a violation of a duty. Interestingly enough, much like other res ipsa cases, determining who is the culpable party is just as difficult. Who was responsible for the breach? Who has standing to sue? Which part of an organization had the obligation to protect against breaches?

If a large company has a breach, someone is going to sue them. Either the people who had their data compromised, or the shareholders who have stock that has gone down in price. As I have commented in other posts, officers and directors have a duty of care they must adhere to. However, the usual cause of action which can affect the individual manager has been limited to the data subject, or the

shareholder as the plaintiff. While this remains true, there is an additional party who is starting to prosecute individuals – the FTC.

In February of this year, the 4th Circuit upheld a $163 million judgment against an individual executive at a company accused of defrauding consumers via a "scareware" scheme. While not directly the same as a security breach, the defendant's argument in this case centered around a challenge to the legal standard the lower court applied in finding individual liability under the FTC Act. Specifically, that a person could be held individually liable if the FTC proves that the individual participated directly in the deceptive practices or had authority to control them, and had knowledge of the deceptive conduct.

This standard comes from securities fraud jurisprudence and requires proof of an individual's authority to control the alleged deceptive practices, coupled with a "failure to act within such control authority while aware of apparent fraud." This proposed standard would permit the commission to pursue individuals only when they had actual awareness of specific deceptive practices and failed to act to stop the deception, i.e., a specific intent/subjective knowledge requirement".

However, the 4th Circuit said this standard would effectively leave the FTC with the "futile gesture" of obtaining "an order directed to the lifeless entity of a corporation while exempting from its operation the living individuals who were responsible for the illegal practices" in the first place.

While the 4th Circuit's holding is related to a very obvious fraud scheme, the usual cause of action the FTC asserts against a company for a security breach is under the "deceptiveness" prong of Section 5, liability for a security breach is starting to creep outward to those who are actually responsible for the security posture of a company.

Cybersecurity: Coming to an Office Near You

By Anthony Orler (October 20, 2014)

Way back in the 1980's, there was a very simple way to keep computer information from being stolen. Every disk containing confidential information was locked in a Sargent and Greenleaf safe.

Of course, even then, there were problems: 22,000 or so 3.5 inch "microfloppy" disks hold the same amount of data as a 32 GB thumb drive can hold today. The safe got a bit full, and it was difficult to find your disk in that haystack.

Now there is the internet, and tablets that are fully-functioning computers, and cellular telephones the size of…tablets. Cell phones can take pictures, record conversations, and send data anywhere in the world.

For example, Stephen Ward of Owensboro, Kentucky sold a digital copy of a confidential manual for the RQ-21A Blackjack drone aircraft to an FBI undercover agent. For more on Mr. Ward's conviction, see the Yakima Herald article. Of course, some people just give electronic copies of government secrets away, like Edward Snowden and Bradley Manning.

The insider threat to data security, also called "cybersecurity" is no longer somebody else's problem, nor merely an information technology (IT) problem. Cyber crimes are everyone's problem. And everyone at your company needs to be part of the solution.

This does not mean that everyone must be subjected to lie detector tests or threatened with waterboarding if they accidentally lose their cell phone. It does mean that everyone must use a little common sense about their use of company resources, and it also means the company should have reasonable IT safeguards.

Many people use workplace-provided laptop computers to do their jobs from somewhere other than the office. That alone isn't a problem, but having open access to sensitive corporate data via the coffee house wi-fi, or allowing wireless access to proprietary data, might be. Some employees absolutely must have the latest and greatest devices to be more productive. These next-generation devices may also have…the ability to access confidential data without leaving a trace. Then there are personnel that just leave devices lying around unattended. All of these situations must be addressed.

Because not all data is proprietary, a good place to start is determining what data needs protection. For example, if your company stores or works with Protected Health Information (PHI), that data probably needs to be secured. Although this step may seem somewhat obvious, in July 2013, four million people had their PHI and social security numbers compromised, and another breach in 2011 affected 4.9 million people.

Trading Secrets

Once the confidential data is identified, secured storage for that data may be appropriate. Separate storage that is only accessible by certain employees, or other limitations on access may provide your proprietary data with additional protection. To ensure your secrets remain secret, you may want to do what the CIA and NSA do: encrypt your data.

No matter how safe the computer systems are, if you have inexperienced or untrained personnel, you have a big hole in your security system. Training your employees how to maintain data security on an ongoing basis should help maintain their awareness that the data is important and needs to be protected. Update your security training and your security system if new projects or data needs additional protection.

When you disseminate proprietary information, just because the data is no longer in your control doesn't mean you shouldn't take steps to protect it. Secure all data, and record the dissemination that is outside of normal avenues of access.

In other words, have a cybersecurity program that fits your business. Keep your employees aware of how to maintain security of the data in your systems. And every now and then, make sure that your confidential data cannot be retrieved by a teenager using their newest cell phone.

Or you can go back to the floppy disks and a safe. Kind of difficult to drag that into a business meeting, though.

Seyfarth Attorneys Facilitate Discussion On Cybersecurity and Protecting Valuable Trade Secrets at the 39th Annual Intellectual Property Institute Conference

By Robert Milligan (November 4, 2014)

Seyfarth Intellectual Property, Trade Secret and Privacy attorneys are participating in the 39th Annual Intellectual Property Institute Conference in Garden Grove, California this week.

The IP Institute brings together preeminent speakers from leading companies and law firms to share tips "from the trenches." The Institute covers a great array of topics affecting our clients, such as trademarks, copyrights, licensing, litigation, entertainment law, right of publicity, trade secrets, sweepstakes, social media, ADR, privacy, and technology law, as well as a separate patent law track.

Los Angeles Partner Robert B. Milligan will be moderating a panel on "Cybersecurity and Protecting Valuable Trade Secrets and Confidential Information While Balancing Innovation and Employee Mobility," and Sacramento Partner James D. McNairy will be presenting "Hot Topics in California Trade Secrets Law," on Thursday, November 6, 2014.

Seyfarth will have a staffed table at the event, Seyfarth attorneys Yandi Fashu-Kanu, Alan M. Lenkin, James D. McNairy, Robert B. Milligan, Puya Partow-Navid, Joshua Salinas, Eugene Suh and Kenneth L. Wilton are scheduled to attend and participate.

For more information, please click here

Connecticut Supreme Court Grants Private Action for HIPAA Breach

By Adam Laughton (November 11, 2014)

This week, the Connecticut Supreme Court issued an opinion which upheld a state common law negligence action against a healthcare provider for violation of privacy and confidentiality laws and regulations using as evidence of the standard of care the Health Information Portability and Accountability Act (HIPAA) and its accompanying regulations. The court denied defense arguments that HIPAA, which expressly does not provide a private right of action, preempts such state law negligence claims.

The plaintiff was a patient of the defendant and had been provided with a copy of defendant's privacy policy, which provided that protected health information would not be released or disclosed without the patient's authorization. Shortly thereafter, the plaintiff's ex-boyfriend filed suit against the plaintiff and served defendant with a subpoena requesting patient's medical records. Defendant responded to the subpoena by filing the plaintiff's medical record with the court, but did not notify the plaintiff. The plaintiff alleged that, as a result of this disclosure, she suffered harassment and extortion from her ex-boyfriend. The trial court initially ruled for the defendants, stating that HIPAA preempted any state statutory or common law claims related to HIPAA violations.

While acknowledging that it was "well settled" law that HIPAA creates no private right of action, the Connecticut Supreme Court reversed the trial court's decision, noting that the plaintiff was not asserting a statutory right or a private right of action under HIPAA, but rather was making a common-law negligence claim with HIPAA informing the standard of care. The court, in reviewing HIPAA's preemption provisions, which apply to "contrary" provisions of state law and exempt "more stringent" state laws, concluded that HIPAA did not preempt a state common law theory of negligence. the court found that HIPAA was appropriately used to inform the standard of care applicable to such a negligence theory on the basis that HIPAA now sets standards for health information privacy and confidentiality among health care providers,. The court was able to identify multiple decisions in both federal and state courts throughout the country which came to similar conclusions regarding HIPAA's failure to preempt common law claims of negligence.

This is an important decision that reflects how HIPAA non-compliance or breach can be used to establish claims of negligence based on breach of applicable standards of care extending to not only "covered entities" such as health care providers, insurers or clearinghouses, but also those organizations that do business with Covered Entities as Business Associates. Based on the Connecticut decision and other similar cases throughout the country, there is a likelihood we will see an increased number of claims using state common law negligence actions based on unauthorized release or disclosure of the plaintiff's protected health information, or even an inadvertent breach, if appropriate physical and technological safeguards were not in place as required by federal and state privacy laws.

The case is Emily Byrne v. Avery Center for Obstetrics and Gynecology, P.C. (SC 18904).

Union Files NLRB Complaint Regarding the USPS' Handling of Security Breach Involving Employee Personal Information

By Bart Lazar (November 19, 2014)

A company faced with a security breach has a lengthy "to do" list, things to accomplish with respect to its incident response plan. It must, among other things, determine the root cause of the vulnerability or breach, investigate and eliminate the vulnerability or breach, determine the full nature and extent of the breach, determine who to notify and finalize the notifications.

If the American Postal Workers Union (APWU) has its way, a unionized employer facing a security breach involving employee personal information would have yet another responsibility – bargaining over the impact of or response to the security breach.

The asserting that the United States Postal Service sent notice of the breach to employees on November 10, 2014, and offered the employees free credit monitoring for 1 year, but "did not give the Union advance notice that would enable it to negotiate over the impact and effects of the data breach on employees." The Union's complaint further states that by providing free credit monitoring, the USPS made a unilateral change in wages, hours and working conditions. Under the various state database security notification laws and the HiTech provisions of HIPAA, employers that encounter a breach of personal information regarding employees, must, absent certain exceptions, notify the affected employees (or for a HIPAA breach, plan participants), as well as potentially notify regulators and others.

There is no legal requirement in the United States that companies must consult with their employees regarding the investigation and/or impact of a security breach involving employee data. In fact, it is important that information concerning potential security incidents be maintained confidential so that the investigation is not compromised. Therefore, the APWU is taking a novel, unprecedented stance in claiming that the USPS had an obligation to be at the table and bargain over what actions USPS would take with respect to investigating and/or remediating a breach.

Although it will be several months (at the earliest) before the NLRB issues any type of ruling or guidance on this matter, employers should consider this type of communication should a data breach occur. In other words, while not legally required, it is certainly important and prudent for a company to consider all stakeholders in determining how to respond to a security breach. The goodwill of a company, and its relationships with employees and customers are extremely valuable.

Since the wrong internal or external communications concerning a breach can have a significant impact on how actual and potential customers and employees, as well as shareholders, perceive the company we recommend that every incident response plan include a company's public relations and communications experts in order to make sure that the proper groups are properly informed as to the status of a security incident and the measures a company is taking to protect affected individuals.

NLRB "Deletes" Employer Email Rule

By Jeffrey Berman and Nick Clements (December 15, 2014)

Until December 11, employers thought that they owned their email systems and could limit their use to company business. On that day, a divided National Labor Relations Board ("NLRB") ruled "not so." In *Purple Communications*, 361 NLRB No. 126 (Dec. 11, 2014), the NLRB ruled that employees who have access to an employer's email system as part of their job generally may, during non-working time, use the email system to communicate about wages, hours, working conditions and union issues. The NLRB reached this conclusion notwithstanding the fact that Purple Communications has a rule providing that its email system was to be used for "business purposes only." It is expected that the NLRB's ruling will be challenged in the federal courts.

Specifically, the NLRB ruled that employees with access to company email can use company email systems for union organization and Section 7 protected activities. The ruling overturned the NLRB's 2007 decision in *Guard Publishing v. NLRB*, (571 F.3d 53 (D.C. Cir. 2009)) ("*Register Guard*") which held, in relevant part, that employees have no statutory rights to use their employer's email systems for labor organization purposes or discussions about wages or other workplace issues. The *Purple Communications* ruling is the result of a case brought by the Communications Workers of America union ("the Union") after it failed in its attempt to organize employees of a company that provides interpreting services for the deaf and hard of hearing. The Company, for its part, had an "Internet, Intranet, Voicemail, and Electronic Communication Policy" that allowed the use of company owned electronic equipment and systems, including its email system, for "business purposes only." The Company claimed that its "business purposes only" restrictions for company email use were aimed at reducing workplace distraction. The Union argued, on the contrary, that the Company's prohibition of its employees' use of company email for non-business purposes and on behalf of organizations not associated with the company interfered with the Company's employees' Section 7 rights.

As anticipated, the NLRB sided 3-2 with the Union; the three Democratic appointees voting in favor of what many will view as an unprecedented taking of private, employer property. The two Republican appointees filed vigorous dissents. The NLRB held that Section 7 statutorily protected communications (*e.g.*, communications about labor organizations, wages or other workplace issues) between employees on nonworking time must be permitted by employers that have chosen to provide employees email accounts hosted on the employer's email servers. In the ruling, the NLRB stated that *Register Guard* initially got the issue wrong because it undervalued employees' Section 7 rights and placed too much emphasis on employers' property rights. Additionally, the majority opined, Register Guard incorrectly analogized company email to company-related equipment (e.g., bulletin boards, copy machines, public address systems, etc.). The NLRB previously determined in an unrelated case that employers could place restrictions on company-related equipment, given its physical size and content limitations. But, for purposes of the current case, the NLRB concluded that this analogy "inexplicably failed to perceive the importance of email as a means by which employees engage in protected communications." Moreover, the majority noted that since *Register Guard* was decided seven years ago, the importance of email as a means for communication has only increased, further intensifying the error of the *Register Guard* decision.

The *Purple Communications* ruling, of course, turns *Register Guard*, on its head. However, the NLRB attempted to make its ruling seem more palatable by proffering several caveats in its general repudiation of *Register Guard*. First, the *Purple Communication* ruling applies only to employees who already have been granted access to an employer's email system in the course of their work. Accordingly, the ruling does not require employers to provide employees access to the employer's email system in the first place. Second, employers can still ban all non-work-related use of email—including Section 7 email use on nonworking time—if the employers can demonstrate that special circumstances make the ban necessary to maintain "production or discipline." Additionally, absent justification for a total ban of non-work related email on non-working time, employers may still limit employees' use of the employer's email system as long as the limitations are applied uniformly and are necessary to maintain "production and discipline." Unfortunately, the NLRB stated that the circumstances in which a ban would be justifiable would be "rare."

In a further effort to attempt to placate the anticipated employer reaction to the decision, the majority also stated that its ruling did not apply to non-employees, and that employers could lawfully monitor employee email use as long as doing so fell within the ordinary scope of its email system monitoring polices. This effectively means that employers may not increase its monitoring during a labor "organizational campaign" or "focus its monitoring efforts on protected conduct or union activists" or otherwise enhance their monitoring efforts to stymie protected activity. But, employers may continue to tell their employees that it monitors, or at least reserves the right to monitor, computer and email use for legitimate business reasons. Further, the ruling does not change the general rule that employees have no expectation of privacy when they utilize their employer's email systems. Thus, even though employees' use of their employer's email systems for Section 7 purposes is now protected, employers can still monitor their employees' use of the email system and also advise employees' that they are doing just that.

Finally, regardless of the far reaching impact of its decision, the NLRB did note that its *Purple Communications* decision would not prevent an employer from establishing uniform and consistently enforced restrictions. These restrictions could include, for example, prohibitions on large attachments or audio/ video segments, if the employer could demonstrate that, left unregulated, the employee actions would interfere with the email system's efficient functioning.

The upshot of the *Purple Communications* ruling is that employers should review their email system policies. In some cases, employers may want to eliminate email system usage by employees whose jobs do not require the use of email. Otherwise, employers need to ensure they apply their email system policies, including monitoring, uniformly and consistently. Finally, it never hurts to very clearly remind employees that they have no expectation of privacy when they use company email systems—even if they are engaging in Section 7 protected activities.

While some employers may modify their rules that the email system is to be used for business purposes only to read that "With the exception of communications regarding wages, hours, working conditions and unions, our email system may be used only for business purposes," other employers may wait to see if the federal appellate courts embrace this departure from decades of NLRB and judicial precedent.

Trading Secrets

Acknowledgments:

Special thanks to Lauren Leibovitch, Nicole Bandemer and Bridget Rabb for their work in putting together this year in review.

SEYFARTH SHAW

Atlanta
Boston
Chicago
Houston
London
Los Angeles
Melbourne
New York
Sacramento
San Francisco
Shanghai
Sydney
Washington, D.C.

www.seyfarth.com