SEYFARTH SHAW

2015

YEAR IN REVIEW

Trading Secrets

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

Trading Secrets

Dear Clients and Friends,

2015 was a year of great change and accolades for our Trading Secrets blog. In particular, LexBlog ranked Trading Secrets the #2 Intellectual Property Blog and Top 30 Am Law 200 blog in their *2015 Am Law 200 Blog Benchmark Report*. Since 2007, the blog has continued to grow in both readership and postings. Content from Trading Secrets has appeared on news sources such as *JD Supra, Mondaq, Lexology, Law360, IP Magazine, SHRM, 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 2015 Year in Review, which compiles our significant blog posts from 2015 and highlights our blog's authors. For a general overview of 2015, we again direct you to our Top 10 2015 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law blog entry as well as our 2015 Trade Secrets Webinar Series - Year in Review blog entry, which provide a summary of key cases and legislative developments in 2015, as well as practical advice on maintaining trade secret protections as well as other pertinent topics in this area.

As the specific blog entries 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, archived from 2011 to the present. In 2015, we offered video blog posts, audio podcasts, more special guest authors, a feature on international law, and provided an additional enhanced Resources page on the blog. We also continued our special feature tracking the proposed federal trade secret legislation. In 2016, we will also offer 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 2015, we hosted nine webinars, which are listed in this Review. For those who missed any of the programs in the 2015 webinar series, the webinars are available on the blog or CD upon request.

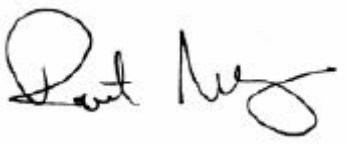
We are kicking-off the 2016 webinar series with a program entitled, "2015 National Year in Review: What You Need to Know About Recent Cases/Developments in Trade Secret, Non-Compete, and Computer Fraud Law." More information on our upcoming 2016 webinars is available in the program listing contained 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

2015 Trade Secrets Webinar Series

- 2014 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
  January 27, 2015
- Protecting Confidential Information and Client Relationships in the Financial Services Industry
  March 10, 2015
- International Trade Secrets and Non-Compete Law Update
  April 14, 2015
- Employee Social Networking: Protecting Your Trade Secrets in Social Media
  May 28, 2015
- How and Why California is Different When It Comes to Trade Secrets and Non-Competes
  June 23, 2015
- State Specific Non-Compete Oddities Employers Should Be Aware Of
  August 18, 2015
- So You Want an Injunction in a Non-Compete or Trade Secret Case?
  September 24, 2015
- Social Media Privacy Legislation Update
  October 27, 2015
- Enforcing Non-Compete Provisions in Franchise Agreements
  November 19, 2015

Trading Secrets

2016 Trade Secrets Webinar Lineup

- 2015 National Year in Review: What You Need to Know About the Recent Cases/ Developments in Trade Secrets, Non-Compete, and Computer Fraud
- The Defend Trade Secrets Act
- How Your Company May Fail to Protect Data
- Financial Services and Trade Secrets/Non-Compete Issues
- NLRB Issues: Addressing Trade Secret/Non-Compete Issues in Joint Employer Scenarios
- International Trade Secret and Non-Compete Legal Update
- Franchise and Trade Secret/Non-Compete Issues
- Trade Secret Protection Audit
- Criminal Trade Secret Issues
- Open Source Software as a Security Risk
- Proving-Up Trade Secret Misappropriation: Best Practices and Tales From the Trenches that Every Company Should Know

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.

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.

Trading Secrets

Christopher Baxter is a staff attorney in the Boston office and is located within the litigation department. Mr. Baxter is a registered patent attorney whose practice includes advising clients on various aspects of intellectual property law. Mr. Baxter has experience in trademark and patent prosecution as well as patent litigation. Mr. Baxter has also drafted and prosecuted numerous patent applications regarding technologies ranging from business methods to the chemical and mechanical arts. He also has experience in technology licensing.

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.

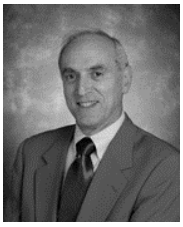
Enedina Cardenas is an associate in the Labor and Employment department of Seyfarth Shaw LLP. Ms. Cardenas defends employers against individual and multi-plaintiff claims of sexual harassment, wrongful termination, and wage & hour violations. She also represents employers on trade secret misappropriation, unfair competition, and other business tort claims.

Jesse Coleman is a partner in the Litigation Department of Seyfarth Shaw LLP. His practice encompasses various types of civil litigation facing the health care industry, energy industry, and related industries. This includes representing managed care organizations, insurance companies, hospital systems, and physicians in matters involving contract disputes, peer review and credentialing proceedings, Medicaid bid protests, antitrust claims, defamation claims, EMTALA claims, ERISA claims, professional liability claims, and regulatory matters before state and federal agencies. He has also represented and counseled both health care and energy-sector clients in numerous trade secret disputes.

Trading Secrets

Matthew Christoff is an associate in the Commercial Litigation Practice Group of Seyfarth Shaw LLP. He focuses his practice on issues involving eDiscovery, including electronic document preservation, production, review, and spoliation. Mr. Christoff has a technical background that has included computer support, network administration, and programming.

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.

Lauren Gregory is an associate in the Litigation Department of Seyfarth Shaw LLP. Ms. Gregory's practice centers around the resolution of complex commercial disputes, including general business and contract disputes, unfair competition, misappropriation of trade secrets and other confidential information, and trademark, trade dress, and copyright infringement.

Trading Secrets

Justine Giuliani is an associate in the Melbourne office of Seyfarth Shaw Australia. She is a member of the firm's International Employment Law practice. Justine has experience across all aspects of employment and industrial relations law. She advises clients in relation to employment arrangements and industrial instruments, workplace policies, executive employment issues, termination of employment, enterprise bargaining, industrial action and workforce restructures.

Daniel Hart is a partner 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 more than 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.

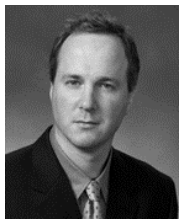
Trading Secrets

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.

Richard Lutkus is a partner in the San Francisco office of Seyfarth Shaw LLP. His practice is dedicated to complex information governance issues including information security, eDiscovery consulting and litigation response, digital forensics, data breach prevention and response, cyber-stalking mitigation, and information technology related policies and practices.

Andrew Masak is an attorney 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.

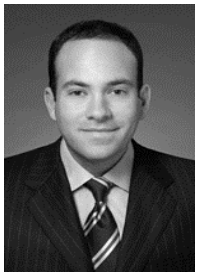
Georgina McAdam is an associate in the International Labor & Employment practice of Seyfarth Shaw (UK) LLP, based in the firm's London office. Her focus is on all areas of employment law, both contentious and non-contentious. Prior to joining Seyfarth Shaw, Ms. McAdam worked in one of London's top-tier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

Trading Secrets

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.

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.

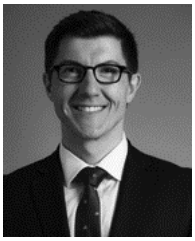
Joshua Salinas is an attorney in the Los Angeles office of Seyfarth Shaw LLP, practicing in the areas of trade secrets, restrictive covenants, computer fraud, and commercial litigation. Mr. Salinas' experience includes the prosecution and defense of trade secret misappropriation and unfair competition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

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.

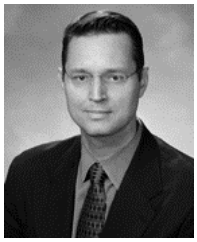


Michael Tamvakologos is a partner in the International Employment Law practice of Seyfarth Shaw Australia. Michael is an experienced litigator and adviser. Michael advises clients concerning all facets of industrial and employment law, including executive recruitment, remuneration and termination issues; bargaining, industrial action, industrial disputation, and breach of enterprise agreement claims; application for approval of enterprise agreements (including appearing in contested hearings); outsourcing and transfer of business; general protections and discrimination matters; breach of contract, wrongful and unfair dismissal, restraint of trade and unfair dismissal claims; and claims relying on the Australian Consumer Law.

Trading Secrets

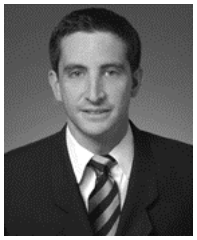
John Tomaszewski is senior counsel in the International Data Protection Practice Group of Seyfarth Shaw LLP. He has significant experience counseling companies regarding data protection and information security throughout the Americas, Europe and Asia. His clients have included a myriad of technology companies as well as financial services, pharmaceuticals, and e-commerce companies of all sizes. John has prepared privacy policy documentation for HR departments, cloud service providers, social media companies, and a host of both traditional "brick-and-mortar" and emerging technology clients.

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.



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.

Trading Secrets

Dallin Wilson is an associate in Seyfarth Shaw's Boston office and is a member of the Commercial Litigation, Construction, Consumer Financial Services Litigation, and Securities and Financial Litigation practice groups. Mr. Wilson represents clients in all manner of litigation matters in state and federal court. His clients include banking institutions, supermarkets, contractors, and privately held corporations. Mr. Wilson also has experience representing healthcare entities in government investigations related to violations of HIPAA, Anti-Kickback Statutes, and other state and federal regulations.

Rebecca Woods is a partner in the Atlanta office of Seyfarth Shaw LLP and co-chair of the firm's Commercial Litigation practice group. 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 senior counsel 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.

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

2015 Summary Posts

- Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2015
  By Robert Milligan and Paul Freehling (January 11, 2016)

- Best Practices Shared in Seyfarth Shaw's 2015 Trade Secrets Webinar Series Year in Review
  By Robert Milligan (December 16, 2015)

Trade Secrets Legislation

- Latest Updates on Federal Trade Secrets Legislation
  By Robert Milligan and Joshua Salinas

Trade Secrets

- Federal Circuit Reverses Lower Court's Ruling That Plaintiff's Trade Secret Misappropriation And Conspiracy Claims Were Untimely And Unprovable
  By Paul Freehling (January 12, 2015)

- Employer Can Be Found Liable For Misappropriating An Employee's Trade Secrets
  By Paul Freehling (March 10, 2015)

- Many Courts Are Reluctant To Permit Parties To Redact Filed Documents, Or To File Them Under Seal, Even When They Contain Trade Secrets
  By Paul Freehling (March 25, 2015)

- Webinar Recap! Protecting Confidential Information and Client Relationships in the Financial Services Industry
  By J. Scott Humphrey and James Yu (March 30, 2015)

- SEC Cracks Down On Confidentiality Agreements Chilling Employees' Rights to Report Potential Securities Law Violations
  By Ada Dolph, Christopher Robertson and Robert Milligan (April 1, 2015)

- Unsecured Networks More Susceptible to Data Theft
  By Richard Lutkus and Matthew Christoff (June 19, 2015)

- New Jersey Supreme Court Confirms Aspiring Whistleblowers Can't Help Themselves to Confidential Documents
  By Robert Szyba and Jade Wallace (June 24, 2015)

- How a Trade Secret Could Have Saved a Running Royalty From a Nearly Invincible Law
  By Michael Baniak (June 25, 2015)

Trading Secrets

- Webinar Recap! How and Why California is Different When it Comes to Trade Secrets and Non-Competes
  By Robert Milligan, James McNairy and D. Joshua Salinas (June 29, 2015)

- Sales Of $8,000 Stemming From Trade Secret Misappropriation Results In Liability For $1.3 Million
  By Paul Freehling (July 23, 2015)

- Trade Secret Protection: What are Reasonable Steps?
  By Guest Author of TradeSecretsLaw.com, Pamela Passman (July 31, 2015)

- Recent Developments on Copyright Preemption of Trade Secret Claims in the Fifth Circuit
  By Matthew Werber (August 5, 2015)

- Employer's Action for Misappropriation of Trade Secrets Against Former In-House Counsel Who Engaged in Competitive Activities Not Subject to Anti-SLAPP Motion
  By Enedina Cardenas (August 6, 2015)

- Inevitable Disclosure Doctrine Held Inapplicable To Failed Business Transaction
  By Paul Freehling (September 3, 2015)

- Trade Secrets or Patents – Why Software Presents No "One Size Fits All" Solution
  By Patrick Muffo (September 14, 2015)

- Frequently Asked Questions Regarding Trade Secret Disputes and Employment Risks Answered
  By Robert Milligan and Michael Wexler (September 18, 2015)

- When E-Filing Goes Wrong: How to Protect Your Trade Secrets in the Event of Inadvertent Online Disclosure
  By Lauren Gregory (September 23, 2015)

- Financial Projections, Strategic Plans, And Customer Contract Proposals Can Be Trade Secrets
  By Paul Freehling (September 28, 2015)

- Getting Your Money Back: New Jersey Employers Can Disgorge A Disloyal Employee's Salary
  By Christopher Lowe and Robert Szyba (October 1, 2015)

- Webinar Recap! So You Want An Injunction in a Non-Compete or Trade Secret Case?
  By Justin Beyer, Eric Barton and Bob Stevens (October 2, 2015)

- Daily Trade Secret Theft for Daily Fantasy Sports?
  By Marcus Mintz (October 7, 2015)

- Dueling Dumpling Trade Secret Dispute Heads to District Court
  By Dawn Mertineit (October 14, 2015)

Trading Secrets

- Utah Supreme Court Lays Out Pro-Plaintiff Presumption of Harm Standard in Trade Secret Cases
  By Robert Milligan and Amy Abeloff (October 14, 2015)

- Poor Employer Onboarding and Departure Procedures Can Lead to Horrifying Results Including the Loss of Trade Secrets
  By Robert Milligan and D. Joshua Salinas (October 30, 2015)

- Protecting Intellectual Property Throughout Its Lifecycle
  By Guest Author for TradeSecretsLaw.com, Stroz Friedberg (November 5, 2015)

- "Reasonable Suspicion" of Trade Secret Misappropriation Isn't Always Enough
  By Lauren Gregory (November 6, 2015)

- Perspectives From the Bench: A Recap of the AIPLA Trade Secret Law Summit's Judicial Panel
  By Erik Weibust and Dawn Mertineit (November 13, 2015)

- Untrusted Advisor: How Your Law Firm May Fail to Protect Your Data
  By Richard Lutkus (December 4, 2015)

Computer Fraud and Abuse Act

- Satisfying the Computer Fraud and Abuse Act's Jurisdictional Requirements Can Be Complicated
  By Paul Freehling (April 27, 2015)

- CFAA and SCA Do Not Prohibit Creation Of A Fake Facebook Page
  By Paul Freehling (June 15, 2015)

- Corporate Espionage: Not Your Typical Sports-"Gate"
  By Erik Weibust (June 26, 2015)

- California Federal Courts Reiterate: Unless Computer Hacked, Computer Fraud and Abuse Act Permits Misuse Of Electronic Information
  By Paul Freehling (September 15, 2015)

- Michigan Federal Court Rejects As Dicta Sixth Circuit's Broad Computer Fraud and Abuse Act Interpretation
  By Paul Freehling (October 12, 2015)

- Nosal Update: Ninth Circuit Hears Oral Arguments on Password Sharing and Scope of Computer Fraud and Abuse Act
  By Robert Milligan and Amy Abeloff (October 28, 2015)

Trading Secrets

Non-Competes & Restrictive Covenants

- Appellate Court Holds That Non-Compete Agreement Assigned Pursuant to Bankruptcy Court Order is Enforceable by Assignee
  By Paul Freehling (January 20, 2015)

- Non-Solicitation Covenant That Is Silent As To Its Scope May Be Unenforceable
  By Paul Freehling (February 18, 2015)

- Geographically Overbroad Non-Competes Held To Be Unenforceable
  By Paul Freehling (February 26, 2015)

- Beware of the Delaware Choice of Law in Non-Compete Agreements
  By Justin Beyer and Matthew Hafter (March 2, 2015)

- Ninth Circuit Jeopardizes Broad "No Re-Hire" Clauses in California
  By Robert Milligan and Carrie Price (April 13, 2015)

- Forum Selection Clause in Non-Compete Agreement Unenforceable
  By Paul Freehling (April 20, 2015)

- Aggressive SEC Enforcement Efforts Regarding Confidentiality Agreements Will Continue
  By Ada Dolph (April 22, 2015)

- Court, Applying Pennsylvania And California Law, Declines To Enjoin Alleged Violation Of Worldwide Non-Compete
  By Paul Freehling (May 5, 2015)

- Court Affirms California Attorney General's Demand for Confidential Donor List
  By Ofer Lion, Douglas Mancino and Christian Canas (June 1, 2015)

- Texas Don't Hold 'Em: Forum Selection Clause Is Unenforceable
  By Joshua Rodine and Jonathan Brophy (June 10, 2015)

- Non-Compete That Grants An Employer The Right To Seek Injunctive Relief No Guarantee That Injunction Will Issue
  By Paul Freehling (June 12, 2015)

- Is An Offer Of At-Will Employment Adequate Consideration For A Non-Compete? Recent Court Rulings Split Three Ways
  By Paul Freehling (June 30, 2015)

- Non-Compete Injunction Denied, Ninth Circuit Remands For Reconsideration, But District Court Denies It Again, Declines Equitable Tolling
  By Paul Freehling (July 10, 2015)

Trading Secrets

- 50 State Non-Compete and Trade Secret Desktop Reference
  By Robert Milligan (July 22, 2015)

- No Economic Recovery Available For Breach Of A Non-Compete Set Forth In A Distributorship Agreement Which Bars Damages Awards
  By Robert Milligan and Paul Freehling (July 27, 2015)

- Court Decries Ambiguity Of Terminology Used In Non-Compete Agreement And Injunction
  By Paul Freehling (August 10, 2015)

- Effective Carve-Outs to Seek Injunctive Relief from the Court in Arbitration Provisions
  By Alex Meier (August 12, 2015)

- Webinar Recap! State Specific Non-Compete Oddities Employers Should Be Aware Of
  By Michael Baniak and Paul Freehling (August 20, 2015)

- Trend In The Courts: It's Getting Harder To Obtain Preliminary Injunctions In Restrictive Covenant Cases
  By Paul Freehling (November 19, 2015)

- Do Non-Competes Really Stifle Tech Innovation?
  By Dawn Mertineit and Dallin Wilson (November 20, 2015)

- Pennsylvania Supreme Court Rules That Continued Employment Is Not Sufficient Consideration for Non-Competes Entered Into After the Employment Relationship Has Begun
  By Paul Freehling and Robert Milligan (November 20, 2015)

- Webinar Recap! Enforcing Non-Compete Provisions in Franchise Agreements
  By Erik Weibust (November 25, 2015)

- Texas Federal Court Rules "Anti-Competitive" Employment Covenants Do Not Raise Federal Antitrust Question
  By Jesse Coleman (November 30, 2015)

- Non-Disclosure Agreement Enforceable Although Unlimited In Time And Area
  By Paul Freehling (December 1, 2015)

Legislation

- Don't Tweet On Me! Montana and Virginia Become Latest States to Pass Social Media Privacy Legislation
  By Adam Vergne and Chuck Walters (May 21, 2015)

- Connecticut Governor Signs New Social Media Privacy Legislation
  By Daniel Hart (May 29, 2015)

Trading Secrets

- The Sounds of Silence: Non-Compete Reform Efforts Largely Absent in Massachusetts Legislature
  By Katherine Perrelli, Erik Weibust and Dawn Mertineit (June 5, 2015)

- Democratic Senators Propose Federal Legislation to Ban Use of Non-Compete Agreements with Low-Wage Employees and to Require Advance Notice to Potential Employees of Requirement to Sign Non-Compete
  By Robert Milligan (June 8, 2015)

- Video Interview: Discussing the MOVE Act with LXBN TV
  By Robert Milligan (June 18, 2015)

- Hawaii Bans Non-Compete and Non-Solicit Agreements with Technology Workers
  By Robert Milligan (July 6, 2015)

- Alabama Revises Non-Compete Statute In Effort to Provide Additional Clarity
  By Eric Barton (July 14, 2015)

- U.S. Congress To Again Consider Private Right of Action for Trade Secret Misappropriation
  By Marcus Mintz (July 30, 2015)

- Latest Update on Federal Trade Secrets Legislation
  By Robert Milligan and Amy Abeloff (August 26, 2015)

- U.S. Senate To Hold Hearing On Impact of Trade Secret Theft
  By Robert Milligan and Amy Abeloff (December 1, 2015)

- Update on the Senate Judiciary Committee's Hearing on the Protection of Trade Secrets
  By Robert Milligan and Amy Abeloff (December 2, 2015)

International

- Opposition Emerges to EU Trade Secrets Directive
  By Daniel Hart (February 23, 2015)

- Webinar Recap! International Trade Secret and Non-Compete Law Update
  By Daniel Hart, Ming Henderson and Wan Li (April 23, 2015)

- Update on Trans Pacific Partnership's Potential Impact on Trade Secret Law
  By Eric Barton (October 16, 2015)

- Proposed US and EU Trade Secrets Laws Progress but Unlikely to be Enacted This Year
  By Daniel Hart (October 30, 2015)

Trading Secrets

- Australia Non-Compete Update: the Difference Between Winning and Losing Restraint Litigation is Often Good Housekeeping
  By Michael Tamvakologos and Justine Giuliani (December 11, 2015)

- What does the Trans Pacific Partnership mean for IP in Australia?
  By Justine Turnbull and Cassie Howman-Giles (December 15, 2015)

- Leveraging Employment Restraints to Protect Business Assets
  By Michael Tamvakologos (December 18, 2015)

- Proposed EU Trade Secrets Directive Crosses Another Hurdle with "Provisional Agreement" Between Council and Parliament
  By Daniel Hart (December 21, 2015)

- Drafting and Litigating Post-Employment Restrictive Covenants in Australia – Tailoring Your Restraint to Ensure the Right Fit
  By Michael Tamvakologos and Justine Turnbull (December 22, 2015)

- Restraint Payments in Australia – Compliance Issues
  By Michael Tamvakologos and Justine Turnbull (December 28, 2015)

Social Media and Privacy

- Privacy & Security Are Back on the Agenda in DC
  By John Tomaszewski (January 14, 2015)

- How Far Does the "Internet of Things" Reach?
  By John Tomaszewski (February 5, 2015)

- Aspects of Private Social Media Groups May Be Protectable Under Illinois Trade Secret Law
  By Christopher Baxter (May 28, 2015)

- Webinar Recap! Employee Social Networking: Protecting Your Trade Secrets in Social Media
  By John Tomaszewski, Eric Barton and D. Joshua Salinas (June 9, 2015)

- Inside Views: The Intersection Of Trade Secret Law And Social Media Privacy Legislation
  By Eric Barton (August 25, 2015)

- 2015-2016 Edition of the Social Media Privacy Legislation Desktop Reference Now Available
  By Robert Milligan and Daniel Hart (September 9, 2015)

- Information Security Policies and Data Breach Response Plans Webinar Now Available!
  By Karla Grossenbacher and John Tomaszewski (October 5, 2015)

Trading Secrets

- Eric Barton on What Employers Should Know About Where Social Media Password Laws and Trade Secrets Intersect
  By Eric Barton (November 2, 2015)

- Webinar Recap! Social Media Privacy Legislation Update
  By Robert Milligan, Daniel Hart and D. Joshua Salinas (November 4, 2015)

2015 Summary Posts

Trading Secrets

Top 10 Developments/Headlines in Trade Secret, Computer Fraud, and Non-Compete Law in 2015

By Robert Milligan and Paul Freehling (January 11, 2016)

Continuing our tradition of presenting annually our thoughts concerning the top 10 developments/headlines this past year in trade secret, computer fraud, and non-compete law, here—in no particular order—is our listing for 2015 and a few predictions for 2016. Please join us for our first webinar of the New Year on January 29, 2016 discussing these developments/headlines.

1) Enactment of federal trade secret legislation moves closer, while federal non-compete bill gains no traction. In last year's Top 10 listing, and in several blog posts from 2015, we described the ongoing effort of a large bipartisan group of U.S. Senators and Representatives to create a federal civil cause of action for trade secret misappropriation (according to govtrack.us, as of January 11, 2016 there were 22 cosponsors of such legislation in the Senate and 107 in the House). The proposed bill is entitled "The Defend Trade Secrets Act of 2015" ("DTSA"). On December 2, 2015, the Senate Judiciary Committee held a hearing on the DTSA and it received a positive reaction from the Committee. We expect that the DTSA will be voted on by Congress in the spring of 2016.

Many industry representatives who have written or spoken on the subject support the DTSA. They cite such reasons as: (a) it will provide uniform statutory provisions in contrast to the "Uniform Trade Secrets Act" ("UTSA")—adopted by every state except New York and Massachusetts—but which contains some significant state variations; (b) rather than litigate in state courts, some attorneys and companies prefer federal courts, particularly because of federal bench experience with patent, trademark, and copyright cases; (c) personal jurisdiction over defendants may be easier to obtain in a federal court than in a state court with respect to individuals or businesses charged with claims involving overseas trade secret misappropriation or computer fraud and discovery of parties and non-parties may be easier to conduct in federal court; and (d) the statute of limitations in the proposed DTSA is longer, and the maximum amount that can be awarded as punitive damages is higher than the amount available under the UTSA.

A number of academics oppose adoption of the DTSA. They suggest that the expense of litigating in federal court often exceeds the cost of handling a case in a state court. Some also take issue with, among other sections, the *ex parte* seizure provisions in the DTSA (although proponents cite those provisions as advantages). Opponents of the DTSA mention that the UTSA has had years of judicial interpretation that provides some measure of predictability. Opponents have also voiced concern with respect to some potentially ambiguous terms in the proposed DTSA.

We also reported on proposed federal legislation to ban enforcement of non-competes against low wage employees and to require employers to disclose in advance that employees must sign non-competes. The Senate bill is called "Mobility and Opportunity for Vulnerable Employees" ("MOVE"). At present, MOVE has few sponsors and does not appear to be gaining any traction.

Trading Secrets

Please see our dedicated page for the latest updates on the proposed federal trade secret legislation. As discussed below, we expect regulators and employees to continue to challenge the necessity and breadth and scope of non-compete agreements in certain industries.

2) Watch for challenges to (a) confidentiality covenants interpreted as discouraging cooperation with government agency investigations or chilling Section 7 rights and (b) "do-not-hire" agreements. In 2015, federal government agencies such as the SEC took aim at confidentiality clauses seemingly intended to dissuade employees from whistleblowing with respect to alleged employer misconduct. Additionally, the NLRB continued its crusade of striking employer confidentiality agreements/policies that may chill employees from exercising their rights under the National Labor Relations Act. Accordingly, we expect that non-disclosure provisions that interfere with government investigations or chill Section 7 rights will continue to be scrutinized in 2016. Further, the government previously challenged agreements among competitors that prohibited them from hiring their competitors' employees. Plaintiffs' attorneys have attempted to capitalize on such efforts by bringing class actions for alleged unlawful "do-not-hire" arrangements between competitors and some cases have resulted in large settlements. We expect to see more such cases in 2016.

3) The Ninth Circuit's narrow interpretation of the Computer Fraud and Abuse Act ("CFAA") was supported by some courts in other circuits, but rejected by others, and other computer hacking issues continue to percolate. The CFAA states that one who "intentionally accesses a computer without authorization or exceeds authorized access" commits a crime. 18 U.S.C. § 1030. In 2012, in *U.S. v. Nosal*, the Ninth Circuit Court of Appeals (in a divided *en banc* decision) adopted the narrow interpretation that the only intended targets of the law were hackers who "break into" a computer and that the statute does not criminalize the unauthorized *use* of computerized data by misguided employees. 676 F.2d 854. The same court reiterated that view in *U.S. v. Christensen*, Nos. 08-50531, *et al.* (Aug. 28, 2015). The court added, however, that California Penal Code § 502, which prohibits unauthorized taking or using information on a computer, does not require unauthorized access and, therefore, is markedly unlike 18 U.S.C. § 1030.

In decisions announced before 2015, the Fourth Circuit concurred with *Nosal*, but the First, Fifth, Seventh, and Eleventh disagreed. Judicial decisions in 2015 supported each position and, therefore, further muddied the waters.

In *U.S. v. Valle*, Nos. 14-2710-cr and 14-4396-cr (2d Cir., Dec. 3, 2015) (2-1 decision), the majority concluded that there is equal merit to the narrow statutory interpretation announced in *Nosal*, and the diametrically opposed, broader interpretation set forth by courts disagreeing with *Nosal*. Based solely on the doctrine of lenity, the Second Circuit adopted the narrow view.

Two judges in the Middle District of Florida reached opposite conclusions regarding *Cf. Nosal* (*Allied Portables v. Youmans*, 2015 WL 6813669 (June 15, 2015) (following *Nosal*), *with Enhanced Recovery Co. v. Frady,* No. 13-cv-1262-J-34JBT (Mar. 31, 2015) (rejecting *Nosal*)). The federal court in Utah adopted the broader interpretation in 2015. *Giles Construction, LLC v. Tooele Inventory Solution, Inc.*, No. 12-cv-37 (June 2, 2015). A judge in the Western District of Michigan followed *Nosal*. *Experian Marketing Solutions, Inc. v. Lehman*, No. 15-cv-476 (W.D. Mich., Sept. 25, 2015). A judge in the Eastern District of Michigan wrote a lengthy criticism of *Nosal*, and a prediction that the Sixth Circuit would not follow the Ninth, but the judge ultimately decided that the complaint before him stated a cause of action regardless of which statutory interpretation was intended. *American Furukawa, Inc. v. Hossain*, No. 14-cv-13633 (May 6, 2015). These widely disparate rulings will leave many employers without a clear path to follow.

Moreover, one Assistant U.S. Attorney told Congress in 2015 that the CFAA should be amended to clarify which of the two conflicting views Congress intended. We predict that, unless the statute is amended, the U.S. Supreme Court will have to resolve the circuit court split.

Additionally, we expect that the Ninth Circuit will issue another decision in the *U.S. v. Nosal* case this year to address whether password sharing to obtain access to a protected computer is actionable under the CFAA. Additionally, we expect to see more Penal Code section 502 claims in California based upon the alleged misuse of company information "without permission."

4) Security breaches continue to plague owners of confidential data. Hackers, nation states, competitors, and disgruntled employees are among those responsible for the breach and dissemination of confidential data. Following the Ashley Madison incident and some other highly publicized incidents, we expect to see more data breaches and resulting litigation in 2016, particularly in those jurisdictions where courts have been willing to soften the standing requirements for maintaining such suits. To guard against this risk, it is essential that companies have comprehensive information security policies and solid data breach response plans in place.

Sometimes the breach benefits only a single individual or entity, such as when an employee transfers employers and provides proprietary information belonging to the former employer to the new employer. However, the more serious consequences occur when, without the owner's authorization, such data is published on-line for all the world to see. To make matters worse, social media privacy legislation and other privacy laws can often frustrate efforts to identify the thief and to abort the publication.

In connection with a recent New York Supreme Court—New York's trial court—injunction hearing, a party accidentally filed its trade secrets on the New York State Courts Electronic Filing system. The adversary insisted, over the vehement objection of the party that made the inadvertent filing, that this act constituted a posting on the Internet that rendered the information publicly available. The court has delayed making a definitive ruling. On the other coast, the Northern District of California recognized that the issue occurring in New York could arise in California. The court, proactively, promulgated guidelines on its website for the prompt and effective removal of erroneous e-filings.

5) Employers' attempts to enforce non-compete and non-solicitation covenants against lower level employees troubles courts and legislators. At one time, courts normally appeared sympathetic to the principle espoused by employers that parties' non-competition and non-solicitation covenants were contracts that should be enforced. In 2015, although some courts enforced restrictive covenants, a number of judges refused to grant preliminary injunctions sought by former employers against ex-employees. *See, e.g.*, *Great Lakes Home Health Services Inc. v. Crissman*, No. 15-cv-11053 (E.D. Mich., Nov. 2, 2015); *Evans v. Generic Solutions Engineering*, No. 5D15-578 (Fla. App., Oct. 30, 2015); *Burleigh v. Center Point Contractors*, 2015 Ark. App. 615 (Oct. 28, 2015). Each of these courts concluded that the employers had not demonstrated the requisite extreme need for injunctive relief and protection. We expect courts to continue to make it difficult on employers to obtain injunctive relief in 2016, particularly where the employee is lower level and there is no clear evidence of imminent harm. We also saw some efforts (though not successful) in Michigan, Washington, Iowa, and Massachusetts to ban or otherwise limit non-competes.

6) Enforcement of restrictive covenants against franchisees gains traction. The NLRB signaled in 2015 its view that a franchisor's control over the business practices of franchisees may lead to treating the franchisor as a joint employer of the franchisees' employees. Additionally, some courts held in 2015 that restrictive covenants in a franchise agreement could be enforced by the franchisor against both the franchisees and persons who benefit from but are not signatories to the franchise agreement. Some franchisors have sued to enforce covenants in contracts with franchisees. An Ohio federal judge in 2015 ordered an ex-franchisee that had signed a confidentiality agreement to return to the franchisor

its operations manual, brochures, contracts, correspondence, client files, computer database, and other records relating to the franchise agreement. *H.H. Franchising Sys., Inc. v. Aronson*, No. 12-cv-708 (Jan. 28, 2015). Additionally, a Wisconsin judge held that an individual who was not a signatory to a franchise agreement that included a confidentiality clause, but who had benefitted from the franchise, was prohibited from using the franchisor's trade secrets. *Everett v. Paul Davis Restoration, Inc.*, No. 10-C-634 (E.D. Wis., Apr. 20, 2015). We expect to see more litigation involving franchisees and related parties in 2016.

7) Courts struggle with issues relating to the adequacy of consideration for restrictive covenants. The controversial *Fifield* decision by the Illinois Appellate Court several years ago continued to make waves in 2015. The court in *Fifield* held that a restrictive covenant executed by an at-will employee is unenforceable, for lack of adequate consideration, unless the employment relationship lasts at least two years beyond the date of execution. *Fifield v. Premier Dealer Service*, 993 N.E.2d 938 (Il. App (1st) 2013). The Illinois Supreme Court has not yet opined on that holding. This past year, several Chicago federal trial judges, adjudicating cases in which they decided it was necessary to predict whether the Illinois Supreme Court would agree with *Fifield*, reached opposing conclusions. Moreover, in *McInnis v. OAG Motorcycle Ventures, Inc.*, 35 N.E.3d 1076 (Il. App. (1st) 2015), a panel of the Illinois Appellate Court split 2-1 on the question of whether *Fifield* should be followed.

Another wrinkle involving consideration arose in Pennsylvania, which adopted the so-called "Uniform Written Obligations Act" ("UWOA") (solely in force in Pennsylvania). Under the UWOA, if a written contract contains a commitment to which the parties "intend to be legally bound," then the parties may not question the adequacy of consideration for the agreement. On the other hand, the state has a long history of disfavoring restrictive covenants in employment agreements. This past year, the Pennsylvania Supreme Court ruled unenforceable for lack of consideration a covenant entered into after the commencement of employment, but for which no benefit or favorable change in employment status was given to the employee. *Socko v. Mid-Atlantic Systems of CPA, Inc.,* Case No. 3-40-2015 (Nov. 18, 2015). This ruling came down notwithstanding the UWOA, even though the agreement expressly quoted the "legally bound" language of that law. *See id.* This decision does not alter the doctrine that covenants signed by employees upon hire are supported by adequate consideration. We expect to see more challenges to the adequacy of consideration by employees in 2016.

8) New state legislation concerning restrictive covenants. State legislatures have enacted, and probably will continue to enact, new laws bearing on restrictive covenants.

1. New Hawaii statute. Passed in 2015, it provides that a non-compete or non-solicit clause in an employment contract for an employee of a technology business is void.

2. New Connecticut, Montana, and Virginia statutes. In 2015, these three states joined more than a dozen others by enacting laws that restrict employer access to personal social media accounts of employees and job applicants. We predict that these laws will adversely impact employers' efforts to uncover trade secret theft.

3. New Mexico health care practitioner statute. A law passed in 2015 provides that an employer of a health care practitioner may not enforce a non-compete covenant restricting the practitioner from providing post-termination clinical health care services.

4. Alabama and Oregon statutes. Alabama revised its non-compete statute (effective January 1, 2016). The revised statute will make it easier for employers to enforce non-competes against Alabama employees. Additionally, Oregon limited the duration of non-competes with employees to 18 months. The new law is also effective January 1, 2016.

9) Rulings regarding validity of forum selection provisions in restrictive covenant agreements. Some multi-state employers use one-size-fits-all covenants, and that practice—coupled with a litigant's forum shopping—sometimes leads to unexpected inconsistencies. California's policy, articulated in Business and Professions Code Section 16600 (which provides that employee non-compete clauses are typically void), has figured in a number of these cases and likely will continue to do so. California courts continue to dismiss or transfer such cases to other states in accordance with contracting parties' forum choice notwithstanding employees' arguments that the forum state might enforce covenants which seemingly are void in California. We did see some reluctance by courts in Delaware and New York to impose broad restrictive covenants on employees in 2015, particularly where the designated choice of law may unfairly impact the employee.

10) Proposed EU Directive to protect trade secrets makes progress; vote nears on U.S. involvement in Trans Pacific Partnership. The European Union and other foreign countries have varying rules with regard to the protection of trade secrets. In some instances, there are no rules regarding trade secret protection or the laws are not enforced. A U.S. company doing business abroad may encounter a wide variety of practices applicable to trade secrets. There has been an effort to harmonize trade secrets law abroad to provide minimum standards as exemplified by the EU Directive.

As we reported, the proposed EU Directive crossed yet one more procedural hurdle with a provisional agreement on the Directive reached by the European Council (represented by the Luxembourg presidency) and representatives of the European Parliament. Now that the provisional agreement has been reached, the Parliament and Council will conduct a legal-linguistic review of the text. Once that process has been completed, the proposed Directive will then be submitted to the full Parliament for approval. Currently, the Parliament is expected to vote on the Directive around March 2016, but the precise date for a first reading has yet to be determined.

Additionally, as we reported, a proposed trade agreement, the Trans Pacific Partnership, was reached in October 2015 among a dozen Pacific Rim countries and the U.S. While the implementing legislation still needs to be passed by the signatory countries, the agreement will require signatory nations, such as Australia, Canada, Singapore, and Malaysia, to implement criminal procedures and penalties for the unauthorized misappropriation of trade secrets. The agreement signifies the Obama Administration's continued effort to enhance trade secret protections at home and abroad for the benefit of U.S. companies.

Trading Secrets

Best Practices Shared in Seyfarth Shaw's 2015 Trade Secrets Webinar Series Year in Review

By Robert B. Milligan (December 16, 2015)

Throughout 2015, Seyfarth Shaw'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 nine webinars:

1. 2014 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law
2. Protecting Confidential Information and Client Relationships in the Financial Services Industry
3. International Trade Secrets and Non-Compete Law Update
4. Employee Social Networking: Protecting Your Trade Secrets in Social Media
5. How and Why California is Different When It Comes to Trade Secrets and Non-Competes
6. State Specific Non-Compete Oddities Employers Should Be Aware Of
7. So You Want An Injunction in A Non-Compete or Trade Secret Case?
8. Social Media Privacy Legislation Update
9. Enforcing Non-Compete Provisions in Franchise Agreements

As a conclusion to this well-received 2015 webinar series, we compiled a list of key takeaway points for each program, which are listed below. For those clients who missed any of the programs in this year's series, the webinars are available on CD upon request, or you may click on the title below each webinar for the online recording. We are pleased to announce that Seyfarth will continue its trade secrets webinar programming in 2016, and we will release the 2016 trade secrets webinar series topics in the coming weeks.

2014 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete and Computer Fraud Law

The first webinar of the year, led by Michael Wexler, Robert Milligan and Daniel Hart, 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, and provided predictions for what to watch for in 2015.

- As demonstrated by high-profile hacking attacks and criminal prosecutions for trade secrets theft, companies' trade secrets are at greater risk today than ever before. To mitigate the risk of trade secrets theft, companies should review their security procedures, policies on IT

resources and email usage, and employee exit interview/termination processes to ensure that the company's assets are adequately protected.

- Use of social media continues to generate disputes. As more and more states adopt social media privacy laws, companies increasingly seek to assert an ownership interest in work-related social media accounts. Additionally, as the NLRB cracks down on social media policies that prohibited employees from engaging in protected activities, employers should periodically review their policies regarding use of social media in the workplace.

- Courts and regulatory agencies continue to scrutinize non-competes and other restrictive covenants. In light of these 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. To learn more, please see our 50 State Non-Compete and Trade Secrets Desktop Reference.

Protecting Confidential Information and Client Relationships in the Financial Services Industry

The second installment, led by Scott Humphrey and James Yu, 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 company's restrictive covenants and the steps your company has taken to ensure that its confidential information remains confidential will allow your company to successfully and swiftly evaluate its 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.

International Trade Secret and Non-Compete Law Update

In the third installment, attorneys Wan Li, Ming Henderson 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 and China as compared to the United States. This webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these countries to ensure protection of their trade secrets and confidential information, including the effective use of non-compete and non-disclosure agreements.

Trading Secrets

International…Local Law Compliance is Key

- One size does not fit all! Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. However, there are some common requirements and issues regarding enforceability based on the region (e.g., in Europe; see below). Bearing in mind non-compete covenants across the world 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.

- The general approach to restrictive covenants in Europe is that the restrictions should not go further than is reasonably necessary to protect the employer's legitimate business interests. This restrictive approach is a continuing trend across Europe. For example, there is a recent prohibition in the Netherlands on non-compete clauses in fixed-term contracts unless justified by the special interests of the company. In practice, this means that employers should particularly focus on the duration and scope (in terms of geographical coverage and the employee's own personal activities) of the restrictions and be mindful of any local payment obligations when preparing restrictive covenants (e.g., in France and in Germany). Europe is also making an attempt to remedy the uneven levels of protection and remedies in relation to trade secrets. The draft EU Directive for trade secret protection is currently making its way through the legislative process with no firm timeline for adoption.

- In addition to local or regional nuances, employers should take advantage of other contractual and/or tactical mechanisms as a "belt-and braces" approach, such as claw-backs and forfeiture of deferred compensation (where permitted), use of garden leave provisions, and strategic use of forum selection and choice-of-law provisions. Employers operating in the U.S. should also consider strategic use of mandatory forum selection and choice-of-law provisions in restrictive covenant agreements with U.S.-based employees.

- Practical measures should also be taken to protect 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…Do Not Miss the Deadline

- 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.

- Recent case law shows that French courts are strict when it comes to the interpretation of the non-compete clauses and the possibility to waive the non-compete clause. If an employer misses the relevant contractual deadline to release an employee from her/his non-compete, the financial compensation will be due for the entire period. Similarly, if the employer waives the non-compete prematurely, the courts will consider the waiver as invalid.

- 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

automatically include a confidentiality clause in employment agreements to strengthen the protection of the company's data post-termination. Good news for employers: the French High Court recently confirmed that, unlike non-compete covenants, a confidentiality clause does not require any financial compensation.

United Kingdom…Less is NOT More

- Restrictive covenants are potentially void as an unlawful restraint of trade. 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., by geographical scope), and is specific to the commercial environment. Unlike in some European jurisdictions, payment will not "rescue" an unenforceable restriction. In addition, the English courts tend to have an unforgiving nature when it comes to poor drafting even if the intention of the parties is obvious. Employers should therefore 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," which are narrowly defined, 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. Often the physical protection of confidential information is underestimated (e.g., encrypting data, installing passwords, secure storage, etc.), which can be a more effective and less costly approach for employers in the long-term. Employers should therefore also seek to retain physical control of such information in order to reduce and limit unwanted disclosure and misuse.

China….Stay ON TOP of An Evolving Regulatory System

- In China, employers should ensure that they have a non-compete agreement with the employee at the time of employment, so that the employer can decide whether to enforce or not to enforce the non-compete agreement for a period of post-employment.

- In addition, employers should ensure that documents are marked with "confidential," or that other measures are taken to protect confidential information. Otherwise, remedies may not be available under the Chinese law for breach of confidential obligations. Employers should also review and update rules and policies regarding confidentiality and security arrangements. Pre-employment vetting of R&D staff is also essential to prevent unexpected breach or non-compliance with trade secret and intellectual property rights.

- As a notable (and relatively recent) development, injunctive relief for trade secret misappropriation is available in Shanghai and Anhui.

Employee Social Networking: Protecting Your Trade Secrets in Social Media

The fourth installment, presented by John Tomaszewski, Eric Barton and Joshua Salinas, addressed the relationship between trade secrets, social media, and privacy.

Trading Secrets

Social Media Privacy Laws are on the Rise

- At least 20 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 "nonpersonal" accounts and on suspected data theft or workplace misconduct. To learn more, please see our Social Media Privacy Legislation Desktop Reference.

Safeguard Your Trade Secrets

- Protecting your company's valuable confidential information and trade secrets from disloyal employees is a very different exercise than keeping strangers and competitors locked-out. This exercise is further complicated by inconsistent privacy legislation, which can vary wildly from state to state. 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?

Social Media and Bring Your Own Device (BYOD)

- Social media is an extension of the trend to combine work, and non-work related activities within the same platform. Just like smartphones allow you to engage in both work and non-work related emailing, the social media platforms continue to drive the conflation of personal and employee activity. As a result, a holistic approach needs to be taken in managing the employee. Otherwise, what was once considered a reasonable policy at work may get applied to private or protected activity and thereby become at a minimum, unreasonable; and in some cases, illegal.

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

The fifth installment, directed 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, including: a discussion of the California Uniform Trade Secrets Act; the interplay between trade secret law and Business and Professions Code Section 16600 (which codifies California's general prohibition of employee non-compete agreements), and recent case developments regarding non-compete agreements and trade secret investigations. The panel discussed how these latest developments impact counseling, litigation and deals involving California companies.

- Broad "no re-hire" provisions in settlement agreements may, under certain circumstances, constitute unlawful restraints of trade under California law, as reflected in *Golden v. California Emergency Physicians Medical Group* (9th Cir. Apr. 8, 2015).

- Alone, voluntary dismissal of a trade secret claim is not a safe harbor to liability for attorneys' fees if the claim otherwise meets the criteria for having been brought or maintained in bad faith.

- The preemptive scope of California's Uniform Trade Secrets Act is very broad. As a result, tort or conversion claims that might be viable in other states may be preempted when pleaded in California with a trade secret claim, provided independent unlawful acts are not alleged.

State Specific Non-Compete Oddities Employers Should Be Aware Of

In Seyfarth's sixth installment, attorneys Michael Baniak and Paul Freehling 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. As trade secrets and non-compete laws continue to evolve from state to state in piecemeal fashion, companies should continually revisit their trade secrets and non-compete strategies in light of the evolving legal landscape and legislative trends.

- Enforceability of non-compete, non-solicit, and confidentiality covenants in employment agreements depends primarily on the applicable statutes, and pertinent judicial decisions and conflict of laws principles, regarding (a) the acceptable breadth of such covenants, and (b) appropriate balancing of the legitimate business interests of employers, employees, and the public. Enforceability requires constant vigilance in updating the covenants because the law, business, and employment evolves often very rapidly.

- Because each jurisdiction's version of the Uniform Trade Secrets Act as enacted (it has been adopted in one form or another in the District of Columbia and each of the 50 states except New York and Massachusetts) is unique, all relevant jurisdictions' versions must be analyzed.

- Oddities in the law of restrictive covenants include: (a) hostility in a few states to non-competes and/or non-solicit covenants in general; (b) in some states (whether by statutory provision or judicial fiat); certain employees are exempt from such covenants; (c) there are disparities in various courts' willingness to "blue pencil," reform, or invalidate covenants deemed overbroad as written; and (d) there are variations in different courts' views as to whether only actual disclosure, or also threatened or inevitable disclosure, of trade secret or confidential information will be enjoined.

So You Want An Injunction in A Non-Compete or Trade Secret Case?

In Seyfarth's seventh installment, attorneys Justin Beyer, Eric Barton and Bob Stevens focused on the issues confronting plaintiffs in preparing for and prosecuting trade secret cases and the various ins and outs of seeking both temporary restraining orders and preliminary injunctions.

- 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.

Social Media Privacy Legislation Update

In Seyfarth's eighth installment, Seyfarth attorneys Robert Milligan, Daniel Hart and Joshua Salinas discussed their recently released Social Media Privacy Legislation Desktop Reference and addressed the relationship between trade secrets, social media, and privacy legislation. We compiled a list of brief summaries of the more significant cases that were discussed during the webinar:

- In *KNF&T Staffing Inc. v. Muller*, No. 13-3676 (Mass. Super. Oct. 24, 2013), a Massachusetts court held that updating a LinkedIn account to identify one's new employer and listing generic skills does not constitute solicitation. The court did not address whether a LinkedIn post could ever violate a restrictive covenant.

- Outside of the employment context, the Indiana Court of Appeals in *Enhanced Network Solutions Group Inc. v. Hypersonic Technologies Corp.*, No. 951 N.E.2d 265 (Ind. Ct. App. 2011) held that a non-solicitation agreement between a company and its vendor was not violated when the vendor posted a job on LinkedIn and an employee of the company applied and was hired for the position, because the employee initiated all major steps that led to the employment.

- In the context of Facebook, a Massachusetts court ruled in *Invidia LLC v. DiFonzo*, No. 2012 WL 5576406 (Mass. Super. Oct. 22, 2012) that a hairstylist did not violate her non-solicitation 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."

- Similarly, in *Pre-Paid Legal Services, Inc. v. Cahill,* No. CIV-12-346-JHP, 2013 U.S. Dist. LEXIS 19323 (E.D. Okla., Jan. 22, 2013), 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

- The Virginia Supreme Court in *Allied Concrete Co. v. Lester*, 285 Va. 295 (2013) upheld a decision sanctioning a plaintiff and his attorney a combined $722,000 for deleting a Facebook account and associated photographs that undermined the plaintiff's claim for damages stemming from the wrongful death of his wife in a car accident. The deleted photographs showed plaintiff holding a beer while wearing a T-shirt with the message "I Love Hot Moms." Subsequent testimony revealed that the plaintiff's attorney had instructed his paralegal to tell the plaintiff to "clean up" his Facebook entries because "[they did] not want blowups of [that] stuff at trial."

- *PhoneDog v. Noah Kravitz*, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. 2012) involved a dispute over whether a Twitter account's followers constitute trade secrets even when they are publically visible. The court denied the defendant's motion to dismiss and ruled that PhoneDog, an interactive mobile news and reviews web resource, could proceed with its lawsuit against Noah Kravitz, a former employee, who PhoneDog claimed unlawfully continued using the company's Twitter account after he quit. The court held that PhoneDog had described the subject matter of the trade secret with "sufficient particularity" and satisfied its pleading burden as to Kravitz's alleged misappropriation by alleging that it had demanded that Kravitz relinquish use of the password and Twitter account, but that he refused to do so. With respect to Kravitz's challenge to PhoneDog's assertion that the password and the Account followers do, in fact, constitute trade secrets—and whether Kravitz's conduct constitutes misappropriation, the court ruled that such determinations require the consideration of evidence outside the scope of the pleading and should, therefore, be raised at summary judgment, rather than on a motion to dismiss. The parties ultimately resolved the dispute.

- The Second Circuit Court of Appeals in *Triple Play v. National Labor Relations Board*, No. 14-3284 (2d. Cir. Oct. 21, 2015) affirmed an NLRB decision 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. The Facebook activity at issue involved a former employee posting to Facebook, "[m]aybe 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!!!!" A current employee "Liked" the post and another current employee posted, "I owe too. Such an asshole." The employer terminated the two employees for their Facebook activity. The Second Circuit affirmed the NLRB's decision that the employer's termination of the two employees mentioned Facebook activity was unlawful.

Enforcing Non-Compete Provisions in Franchise Agreements

In Seyfarth's ninth and final installment, attorneys John Skelton, Erik Weibust and Anne Dunne focused on how to implement and enforce covenants against competition in the franchise context. A franchisor's trade secrets, confidential information, and goodwill are often among its core assets, and implementing

and enforcing covenants against competition are a common, and effective, means of protecting such business interests.

- For franchisors, non-compete provisions, especially post-termination restrictive covenants, are an important part of the franchise relationship because franchisees are given access to a franchisor's confidential information and trade secrets. Upon the termination, expiration or non-renewal of the franchise agreements, franchisors have a vested interest in preventing the use of such information in a competitive business and in protecting the integrity of the franchise network and their goodwill.

- The enforceability of non-compete provisions is most often litigated in the context of a request for a preliminary injunction, and thus franchisors need to be able present evidence to establish: (1) all of the necessary elements, especially that the franchisor will suffer irreparable harm to its legitimate business interests and goodwill if the franchisee violates the terms of the agreed upon non-compete; and (2) that the restrictions are reasonable in time and scope.

- The enforceability of non-compete provisions varies significantly by state, so national franchisors must ensure that restrictive covenants are drafted to comply with the various definitions of legitimate business interests and protected goodwill, and the different blue pencil, red pencil and reformation rules.

2016 Trade Secret Webinar Series

Beginning in January 2016, we will begin another series of trade secret webinars. The first webinar of 2016 will be "2015 National Year in Review: What You Need to Know About the Recent Cases/Developments in Trade Secrets, Non-Compete, and Computer Fraud Law" on January 29. 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. We are also tracking the latest on the movement to federalize trade secrets law. Please visit our dedicated page on the blog.

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

Trade Secrets Legislation

Trading Secrets

Latest Updates on Federal Trade Secrets Legislation

By Robert Milligan and Joshua Salinas

With increased activity regarding proposed federal trade secrets legislation expected next 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 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 federal legislation, the arguments on both sides of the debate, and our most current resource links.

How Are Trade Secrets Currently Protected?

Trade secrets are legally protectable information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, a trade secret has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being generally known. Examples of trade secrets include, plans, designs, negative information, computer software, customer lists, non-public financial information, cost and pricing information, manufacturing information, confidential information about business opportunities, and certain personnel information.

Trade secrets are generally protected by state law under a particular state's adoption of 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 and social media 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?

On July 29, 2015, with bipartisan support, Congressional leaders in both the House and Senate, including Senators Orrin Hatch (R-UT), Christopher Coons (D-DE) and Representative Doug Collins (R-GA), introduced bills to create a federal private right of action for the misappropriation of trade secrets. The identical bills are HR 3326 and S. 1890 and they were referred to their respective judiciary committee. The proposed legislation, titled the "Defend Trade Secrets Act of 2015" ("DTSA"), follows an unsuccessful attempt just last year to pass the "Defend Trade Secrets Act of 2014."

The proposed legislation would authorize a private civil action in federal court for the 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 proposed legislation features amendments from the 2014 bill and seeks to do the following: 1) create a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act; 2) provide parties pathways to injunctive relief and monetary damages to preserve evidence, prevent disclosure, and account for economic harm to companies; and 3) create remedies for trade secret misappropriation similar to those in place for other forms of intellectual property.

The DTSA has some similarities with the Uniform Trade Secrets Act. The DTSA defines "misappropriation" consistently with the DTSA, and provides for similar remedies, including injunctive relief, compensatory damages, and exemplary damages and the recovery of attorneys' fees in the event of willful or malicious misappropriation.

The DTSA, however, differs from the UTSA in several important aspects. Most notably, it opens the federal courts to plaintiffs for trade secrets cases. The DTSA also allows for an ex parte seizure order. A plaintiff fearful of the propagation or dissemination of its trade secrets would be able to take proactive steps to have the government seize its trade secrets prior to giving any notice of the lawsuit to the defendant. The proposed seizure protection goes well beyond what a court is typically willing to order under existing state law. Next, the DTSA's statute of limitations period is five years compared to just three under the UTSA. Additionally, the DTSA allows for the recovery of treble exemplary damages versus double under the UTSA. Finally, the DTSA contains no language preempting other causes of action that arise under the same common nucleus of facts, unlike the UTSA.

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. Legislation to create a civil cause of action for trade secret misappropriation in federal court has failed in at least three previous attempts.

Recent scholarly articles in the Gonzaga Law Review and Fordham Law Review have suggested 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, nation states, 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 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.

Another case involved the sentencing of a former DuPont employee who allegedly conspired with a South Korean company, Kolon Industries, to misappropriate trade secrets involving Kevlar, a well-known synthetic fiber product produced and sold by DuPont. Kolon Industries allegedly put a plan in place to recruit former DuPont employees so Kolon could create a product to compete with Kevlar without putting the time, effort, and expenditures into developing its own product. The former employee, even though he signed a non-disclosure agreement while at DuPont, allegedly retained DuPont documents upon his departure and turned them over to Kolon when they recruited him. Upon finding out about this scheme, the FBI investigated Kolon, and five of its executives were indicted for committing trade secret theft. Kolon plead guilty and was sentenced to pay $85 million in penalties and $275 million in restitution.

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 FBI has recently launched a nationwide awareness campaign and released a short film based upon an actual case, The Company Man: Protecting America's Secrets, aimed at educating anyone with a trade secret about the threat and how they can help mitigate it. The film illustrates how one U.S. company was targeted by foreign actors and how that company worked with the FBI to address the problem.

From the perspective of those in favor the legislation, 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, including what are reasonable secrecy measures 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. Obtaining necessary service of process and discovery can be extremely difficult or impossible under the current system.

Proponents and Sponsors of the Bills

Announcement of the proposed legislation on July 29, 2015 was joined by a letter of support on behalf of the Association of Global Automakers, Inc., Biotechnology Industry Organization (BIO), The Boeing Company, Boston Scientific, BSA | The Software Alliance (BSA), Caterpillar Inc., Corning Incorporated, Eli Lilly and Company, General Electric, Honda, IBM, Illinois Tool Works Inc., Intel, International Fragrance Association, North America, Johnson & Johnson, Medtronic, Micron, National Alliance for Jobs and Innovation (NAJI), National Association of Manufacturers (NAM), NIKE, The Procter & Gamble Company, Siemens Corporation, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, United Technologies Corporation and 3M. The joint letter expressed the need for a private right of action to supplement the existing Economic Espionage Act of 1996 ("EEA"), which only provides for criminal sanctions in the event of trade secret misappropriation.

In 2014, two similar trade secret bills were introduced and received support from various constituents.

The Heritage Foundation 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 with the PRATSA bill. Also, a diverse set of companies and organizations have previously came 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, National Association of Manufacturers, and the National Chamber of Commerce.

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 came out in favor of the 2014 house 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

Last August, 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 submitted an Opposition Letter to the 2014 bills. The professors cited 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. Following the letter, an Washington and Lee University School of Law professor Christopher Seaman critiqued the federalization of trade secrets law.

Shortly after the introduction of the bills in July 2015, law professors, David Levine and Sharon Sandeen, wrote a new letter to Congress setting forth seven differences between the 2014 bills and the 2015 bill while still contesting the arguments of the bill's supporters. The seven differences include: 1) the wrong is defined differently; 2) the *ex parte*civil seizure still remains but with apparently more stringent standards; 3) new encryption language has been added; 4) new concerns about employee mobility; 5) trade secrets are described as not intellectual property; 6) reporting of trade secret theft abroad is unclear as to whether it means "theft" or "misappropriation;" and 7) "Sense of Congress" provision, which presumes trade secret theft is always "harmful." They believe that the recently introduced legislation does not ameliorate the problems it seeks to fix.

Current Status Of Proposed Legislation

HR 3326 and S. 1890 were introduced into committee on July 29, 2015. The Senate Judiciary Committee held a hearing on the Senate bill on December 2, 2015. Senate Judiciary Committee leaders are reported to be in the process of marking up the bill. As of January 27, 2016, HR 3326 has 107 sponsors and S.1890 has 26 sponsors. We expect Congress to vote on the bills this year.

Additional News and Resources

Our Recent Blog Articles:

Update on the Senate Judiciary Committee's Hearing on the Protection of Trade Secrets - Dec. 2, 2015

U.S. Senate To Hold Hearing On Impact of Trade Secret Theft - Dec. 1, 2015

Proposed US and EU Trade Secrets Laws Progress but Unlikely to be Enacted This Year - Oct. 30, 2015

Trading Secrets

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:

The Anti-Cyberespionage Bill That Isn't, Or Never Was? – The Center for Internet and Society, Jan. 23, 2016

Updating the Defend Trade Secrets Act? – Freedom to Tinker, Jan. 23, 2016

Protecting Our Trade Secrets is Vital to Economic Growth – The Hill, Jan. 21, 2016

Why we Need a Seizure Remedy in the Defend Trade Secrets Act – Patentlyo.com, Jan. 18, 2016

US Senate Vote Awaited for Trade Secrets Seizure Legislation as Experts Chine In (again) – The IPKate, Jan. 17, 2016

Why I Support the Defend Trade Secrets Act – Legal Developments in Non-Competition Agreements Blog, Dec. 29, 2015

Potential Legal Implications of the Defend Trade Secrets Act – *Law.com* (subscription), Dec. 8, 2015

A Misguided Attempt to "Defend Trade Secrets" – *The Washington Post*, Dec. 2, 2015

IPO Sends Letter to Senate Leaders in Support of Defend Trade Secrets Act – *JD Supra*, Dec. 2, 2015

Do We Need a New Judicial Fast Lane to Combat Trade Secret Theft? – *Forbes*, Dec. 1, 2015

Time to Modernize and Strengthen Trade Secret Law – *Corporate Counsel*, Dec. 1, 2015

Senate Judiciary Panel to Probe Trade Secret Theft – *The Hill*, Nov. 24, 2015

New Professors' Letter Opposing The Defend Trade Secrets Act of 2015 – *WordPress*, Nov. 17, 2015

Lawmakers push to protect trade secrets from Chinese Hackers – *The Hill*, Oct. 9, 2015

Defend Trade Secrets Act of 2015 May Open Door To Employers Wishing To Pursue Trade Secret Claims In Federal Court – *Above the Law*, Aug. 13, 2015

Trading Secrets

The Defend Trade Secrets Act Has Returned – *Freedom to Tinker*, Aug. 3, 2015

Lawmakers Take Another Stab At Federal Trade Secrets Law – *Law360*, July 30, 2015

Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets – U.S. Senator Orrin Hatch, Press Releases, July 29, 2015

A Bibliography About Federal Trade Secret Law Reform (Guest Blog Post) – *Technology & Marketing Law Blog*, Apr. 2, 2015

Many Hope Trade Secrets Legislation Moves in Lame-Duck Session; Critics, Skeptical of Bills' Effectiveness, Ask: "Why Here, Why Now?" – Reproduced with permission from BNA's *Patent, Trademark & Copyright Journal*, 89 PTCJ 115 (Nov. 14, 2014). Copyright 2014 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

IP Bills Have Momentum in New Congress – *Law360*, Nov. 5, 2014

Hatch, Coons Applaud House Judiciary Committee Passage of Trade Secrets Legislation – Press Release, Sept. 17, 2014

Judiciary Committee Approves Trade Secrets Legislation – Press Release, Sept. 17, 2014

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

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

Trading Secrets

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

Federal Circuit Reverses Lower Court's Ruling That Plaintiff's Trade Secret Misappropriation And Conspiracy Claims Were Untimely And Unprovable

By Paul E. Freehling (January 12, 2015)

The Federal Circuit recently held that the dismissal of a trade secrets complaint for failure to state a justiciable claim was not warranted merely because the misconduct allegedly involved a number of wrongdoers and began many years before the complaint was filed.

Overview of the case

ABB alleged that, during a several decade period, some of its former employees engaged in a conspiracy to misappropriate — and to pass to alleged co-conspirator competitors — confidential information relating to its products. The district court dismissed on the grounds that the relevant statute of limitations had expired and that ABB had not been reasonably diligent in protecting its trade secrets. On appeal, the judgment was reversed. ABB's allegations of wrongdoing were deemed sufficient to withstand a motion to dismiss. The case was remanded for further proceedings. ABB Turbo Systems, AG v. TurboUSA, Inc., Case No. 2014-1356 (Fed. Cir., Dec. 17, 2014).

The alleged conspiracy and resulting lawsuit

In 1986, Hans Franken left the employ of ABB, a designer and manufacturer of turbochargers and turbocharger parts, and founded a competitor. Over the course of more than 20 years, employees of ABB allegedly transferred to Hans's company confidential information relating to parts embodying ABB's patented inventions.

In 2009, Hans sold his company to TurboUSA, a corporation managed by Hans's son Willem and partly owned by Hans. In connection with the sale, ABB's documents in Hans's company's files supposedly were altered to disguise their source. TurboUSA allegedly continues to use ABB's secrets, enriching Hans and Willem.

In 2012, ABB sued Hans, Willem, and TurboUSA for patent infringement, trade secret misappropriation, and conspiracy. The patent infringement claims were settled, Hans was dismissed as a defendant, and the trade secret and conspiracy case against TurboUSA and Willem continued until it was dismissed by the district court. ABB appealed.

The Federal Circuit's decision

a. Statute of limitations. According to the appellate tribunal, the district court erred when it dismissed the complaint based on the statute of limitations. That is an affirmative defense which ordinarily may not be used as a basis for dismissal on the pleadings unless the time-bar is evident on the face of the complaint (not so here). The trial court surmised that ABB "should have had at least an inkling that something was amiss." The complaint, however, alleges concealment efforts made by the defendants,

is silent with respect to when or how ABB discovered the misappropriation, and does not state facts demonstrating that ABB actually or constructively discovered the misconduct more than three years before the litigation was initiated.

b. Protection of confidentiality. ABB's pleading alleged various actions the company took to protect its trade secrets. The trial court surmised that ABB's efforts to protect secrecy probably would be deemed insufficient. The federal circuit held that only "reasonable" care is required, and "the complaint stage is not well-suited to determining what precautions are reasonable in a given context."

Takeaways

This case teaches that a complaint which alleges the relevant facts as the pleader understands them, and which aligns those factual allegations with the operative legal principles as ABB seemingly did here, has the best chance for surviving a Rule 12(b)(6) motion. On appeal, ABB's pleading was found to satisfy those minimum standards. So, the parties will have an opportunity to take some discovery before the trial court decides whether further litigation would be futile.

Employer Can Be Found Liable For Misappropriating An Employee's Trade Secrets

By Paul E. Freehling (March 10, 2015)

A Chicago federal judge denied summary judgment to an employer alleged to have misappropriated and converted a subordinate's trade secrets. *Stevens v. Interactive Financial Advisors, Inc.*, Case No. 11 C 2223 (N.D. Ill., Feb. 24, 2015) (Kennelly, J.).

Summary of the case

After 20 years as a licensed insurance broker, Stevens wanted to provide investment advisory services as well. However, he was not a registered investment advisor, and so he affiliated with Interactive which was registered. Stevens uploaded his insurance client and investment customer information — which he considered to be his trade secrets — to the electronic database of Redtail, a technology company also used by Interactive. When Interactive subsequently terminated Stevens' affiliation, it reassigned his customers to two other Interactive advisors and directed Redtail to block his access to his client and customer information. Stevens sued, charging Interactive and Redtail with trade secret misappropriation and conversion. The court granted the defendants' summary judgment motion as to Stevens' investment customers but denied it with regard to his insurance clients.

Stevens' relationship with Redtail

Although Stevens apparently had no written agreement with Redtail, he considered their relationship to be contractual. He paid Redtail for its services relating to his client and customer information.

Termination of Stevens

In year six of Stevens' association with Interactive, the firm accused him of involvement in a Ponzi scheme and terminated his affiliation. After he was terminated, he still could provide services to his insurance clients but not to his reassigned investment customers.

The litigation

Stevens' federal court complaint was based on diversity jurisdiction. He alleged that both by blocking access to his data base and by granting such access to other advisors, Interactive and Redtail misappropriated his trade secrets in violation of the Illinois Trade Secrets Act, converted his property, and committed other torts.

The court's decision on the defendants' motions for summary judgment.

1. *Investment customers.* Judge Kennelly observed that, as a result of the termination, Stevens no longer was affiliated with a registered securities advisor and, thus, could not legally service his investment customers. Interactive had to reassign them. Moreover, federal regulations and

Interactive's own policies provided that a terminated representative ceased to have a right of access to his investment customers' non-public personal information. The defendants were entitled to summary judgment, the judge concluded, with regard to Stevens' claims of misappropriation and conversion of his investment customers' information because no material issues were in dispute.

2. *Insurance clients.* Material facts were in dispute, according to Judge Kennelly, concerning Stevens' allegations of misappropriation and conversion of information relating to his insurance clients, and a reasonable jury could agree with Stevens that he owned that information, that it constituted a trade secret, and that Interactive misappropriated and converted it.

Further, the court ruled that a reasonable jury could find that Redtail acted as Interactive's agent by blocking Stevens' access to the data base and granting access to others designated by Interactive. According to the judge, if Redtail assisted Interactive in committing torts, Redtail could be held jointly and severally liable with Interactive. In addition, there was a genuine dispute relating to the existence and terms of a contractual relationship Stevens contended that he had with Redtail, and as to the duties Redtail owed to him. For these reasons, Redtail's motion for summary judgment as to Stevens' claims of misappropriation and conversion of his insurance clients' information was denied.

Takeaways

Several judicial opinions state in dicta that employers rarely are sued for conversion and trade secret misappropriation. The case of *Stevens v. Interactive* is one of those rare lawsuits. Judge Kennelly's decision illustrates that — like anyone else — an employer who takes and uses someone else's property without permission risks being sued for conversion. Further, if that property constitutes a trade secret, the employer also may be accused of misappropriation. To be sure, Stevens was an independent contractor, not an Interactive employee, but nothing in the court's opinion suggests that the ruling turned on that distinction.

Many Courts Are Reluctant To Permit Parties To Redact Filed Documents, Or To File Them Under Seal, Even When They Contain Trade Secrets

By Paul E. Freehling (March 25, 2015)

In a patent infringement case pending in a California federal court, the defendant moved for summary judgment. The parties jointly requested leave to submit to the court under seal, or with redactions, documents containing trade secrets and other confidential information. The court granted the request only in part. *Icon-IP Pty Ltd. v. Specialized Bicycle Components, Inc.*, Case No. 12-cv-03844 (N.D. Cal., Mar. 3, 2015) (Tigar, J.).

Status of the case

This hotly contested patent infringement lawsuit concerned bicycle seats. The defendant moved for summary judgment. By agreement of the parties, the defendant sought to support the motion with certain exhibits filed under seal, or redacted, and the plaintiff did likewise in opposition to the summary judgment motion. Sealing or redacting would have the effect of denying to the public access to all or parts of those documents. Judge Tigar granted leave to seal or redact some of the relevant documents, denied leave as to some, and as to the remainder he directed the parties to tailor more narrowly their sealing or redacting request.

Legal standards applicable to requests to seal or redact

Judge Tigar indicated that there are guiding principles which relate to all such requests in civil cases and additional rules that vary depending on whether the court is considering a non-dispositive or a dispositive motion.

1. *General principles*. The starting point, according to the court, is Fed.R.Civ.P. 26(c)(1)(G). In relevant part, it states that "The court may, for good cause, issue" a protective order "requiring that a trade secret or other confidential . . . commercial information not be revealed, or be revealed only in a specified way." Next, Judge Tigar pointed to Northern District of California local rule 79-5 which provides that a party seeking to seal or redact must establish that the document contains matter protectable by law and that the request is "narrowly tailored." An uncontested protective order (or stipulation) regarding confidentiality will not suffice, he said, because of the "strong presumption in favor of [public] access" to court documents. Other courts considering similar motions also have mentioned the burden that sealing and redacting places on judges and other court personnel as another relevant factor.

2. *Non-dispositive motions*. According to Ninth Circuit case law cited by the judge, if the motion to which the request to seal or redact relates is not for summary judgment (or if the motion is for summary judgment but the documents in question "would not be effectively dispositive of" any issues raised in the motion), the party requesting a stay or redaction need make only "a particularized showing under the good cause standard" of Rule 26(c)(1)(G). The *Icon-IP* case concerned a dispositive motion, and so the court had no occasion to define the phrase

"particularized showing." Other judges have written that the it means proof of specific prejudice or harm that will result if the information is disclosed.

3. *Dispositive motions.* Citing Ninth Circuit and California district court opinions, Judge Tigar stated that a party seeking to seal or redact a document submitted with respect to a dispositive summary judgment motion must overcome a "presumption of public access." This means articulation of "compelling reasons, supported by specific factual findings that outweigh the general history of access and the public policies favoring disclosure, such as the public interest in understanding the judicial process." In other words, courts should operate in the open and not behind a shroud of secrecy.

The court's rulings

1. Judge Tigar permitted redacting a portion of the deposition of a non-party who had been questioned about "highly sensitive business information regarding" his own company. Sealing the entirety of certain of the non-party's documents was denied, however, even though they contained confidential information which could be damaging to the non-party's business interests if it became public. Referring to Local Rule 79-5(b), the judge said that redaction might be permitted if a request was "narrowly tailored to seek sealing of only sealable material."

2. The court denied, for failure to present compelling reasons, the request to seal all or portions of deposition transcripts containing confidential information concerning the defendant's own research and development, budgets, marketing, sales, revenue, and consulting and licensing agreements. This denial may be without prejudice to a renewed request with more detail regarding the reasons for submitting it.

3. Judge Tigar held that compelling reasons were provided for sealing documents where he was satisfied that public access "would result in an invasion of [a] third party's privacy" and "would put Specialized at a disadvantage in future" licensing negotiations.

4. The judge observed that the "compelling reasons" and "good cause" tests also apply to an uncontested request to seal or redact exhibits or deposition transcripts bearing on a *Daubert* motion to exclude certain expert testimony. If the testimony is "aimed squarely at" a party's damages methodology, and exclusion "could cause a crippling blow to the sponsoring party's ability" to support its position with regard to summary judgment, the "compelling reasons" standard should be used. He added that if the testimony would not be dispositive with respect to any "central" issue, "good cause" is the applicable principle.

Takeaways

At one time, courts entered a sealing or redacting order based solely on the parties' stipulation, but no more. Today, in most courts, even an uncontested request to seal or redact confidential documents to be filed in connection with a non-dispositive pretrial motion requires a particularized showing of specific prejudice or harm. Such a request relating to a dispositive motion requires "compelling reasons" for overriding the public interest in the openness and transparency of court proceedings. Presumably, the "compelling reasons" test also is applicable even to uncontested requests to seal or redact exhibits (a) offered into evidence in a bench trial, or (b) to be submitted in a record on appeal. Contact your Seyfarth Shaw trade secrets attorney for advice regarding the complex rules relating to sealing or redacting confidential information in documents to be filed in court.

Trading Secrets

Webinar Recap! Protecting Confidential Information and Client Relationships in the Financial Services Industry

By J. Scott Humphrey and James Yu (March 30, 2015)

We are pleased to announce the webinar "Protecting Confidential Information and Client Relationships in the Financial Services Industry" is now available as a podcast and webinar recording.

In Seyfarth's second installment of its 2015 Trade Secrets Webinar series, Seyfarth attorneys will focus 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.

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

- 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.

Trading Secrets

SEC Cracks Down On Confidentiality Agreements Chilling Employees' Rights to Report Potential Securities Law Violations

By Ada Dolph, Christopher Robertson, and Robert Milligan (April 1, 2015)

The Securities and Exchange Commission (SEC)announced today that it had made good on its prior promises to take a hard look at employment agreements and policies that could be viewed as attempting to keep securities fraud complaints in-house. In *KBR, Inc.*, Exchange Act Release No. 74619 (April 1, 2015), the agency announced an enforcement action and settlement with KBR in which KBR agreed to amend its Confidentiality Statement to provide further disclosures to employees regarding their right to communicate directly with government agencies, notify KBR employees who had signed the Statement in the past, and pay a $130,000 civil penalty.

The SEC concluded that KBR's Confidentiality Statement violated SEC Rule 21F-17, adopted by the SEC after the Dodd-Frank Wall Street Reform and Consumer Protection Act was enacted in 2010. SEC Rule 21F-17 provides that "[n]o person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications."

According to the SEC Order, under its compliance program, KBR required that employees who were interviewed as part of the company's internal investigations into internal reports of potential illegal or unethical conduct, including potential securities violations, sign a Confidentiality Statement at the start of any company interview. The KBR Confidentiality Statement provided in part:

I understand that in order to protect the integrity of this review, I am prohibited from discussing any particulars regarding this interview and the subject matter discussed during the interview, without the prior authorization of the Law Department. I understand that the unauthorized disclosure of information may be grounds for disciplinary action up to and including termination of employment.

The SEC found that although it was not aware of any instance in which a KBR employee was actually prevented from communicating directly with the SEC, the Confidentiality Statement "impedes such communications by prohibiting employees from discussing the substance of their interview without clearance from KBR's law department under penalty of disciplinary action including termination of employment," thereby undermining the purpose of Rule 21F to "encourage[] individuals to report to the Commission."

As part of the enforcement action, KBR agreed to amend its Confidentiality Statement to include this provision:

Nothing in this Confidentiality Statement prohibits me from reporting possible violations of federal law or regulation to any governmental agency or entity including but not limited to the Department of Justice, the Securities and Exchange Commission, the Congress, and any Inspector General, or making other disclosures that are protected under the whistleblower provisions of federal law or regulation. I do not need the prior authorization of the Law Department to make any such reports or disclosures and I am not required to notify the company that I have made such reports or disclosures.

Additionally, KBR agreed to contact KBR employees who signed the Confidentiality Statement from August 21, 2011 to the present informing them of the SEC Order and including a statement that they need not seek permission from KBR's General Counsel before communicating with any governmental agency. The SEC also assessed a civil penalty of $130,000.

In a press release announcing the decision, Sean McKessy, Chief of the SEC's Office of the Whistleblower, is quoted as saying: "KBR changed its agreements to make clear that its current and former employees will not have to fear termination or retribution or seek approval from company lawyers before contacting us. . . . Other employers should similarly review and amend existing and historical agreements that in word or effect stop their employees from reporting potential violations to the SEC."

This appears to be the next step in the SEC Whistleblower Division's initiative to crack down on agreements that it views as violating SEC Rule 21F-17. In widely reported remarks before the Georgetown University Law Center Corporate Counsel Institute last spring, McKessy indicated that the agency was "actively looking for examples of confidentiality agreements, separation agreements, employee agreements that . . . in substance say 'as a prerequisite to get this benefit you agree you're not going to come to the commission or you're not going to report anything to a regulator.'" And just this past February, it was reported that the SEC had delivered official letters to several companies seeking several years' worth of their employee agreements, including nondisclosure and separation agreements.

In recent months, we have seen similar actions regarding agreements or policies by the Equal Employment Opportunity Commission (EEOC) and the National Labor Relations Board. Employers should review their existing employment policies and employment agreements, including confidentiality, non-disclosure and separation agreements, for any provisions that might go astray of these agency enforcement initiatives. As part of this enforcement action, the SEC found that the amended language cited above was acceptable in the employer's Confidentiality Statement. Employers should consider including this language or similar language in their agreements and policies specifying that the reporting of potential violations law or regulations to government agencies is not prohibited, and indicating that no prior employer approval is required.

Given this enforcement action by the SEC, it may be just a matter of time before the SEC also weighs in on whether employers can prohibit employees from taking and disclosing company documents in connection with their alleged whistleblowing activities. See our prior blogs on this issue here and here, and one of the more recent controversial administrative decisions addressing this issue here.

Ada W. Dolph and Christopher F. Robertson are Team Co-Leads of the National Whistleblower Team. Robert B. Milligan is Co-Chair of the National Trade Secrets, Computer Fraud & Non-Competes practice group. If you would like further information on this topic, please contact a member of the Whistleblower Team, your Seyfarth attorney, Ada W. Dolph at adolph@seyfarth.com, Christopher F. Robertson at crobertson@seyfarth.com or Robert B. Milligan atrmilligan@seyfarth.com.

Unsecured Networks More Susceptible to Data Theft

By Richard Lutkus and Matthew Christoff (June 19, 2015)

Over the past few years, users have become increasingly aware of the inherent dangers of connecting to unsecured Wi-Fi networks. Unfortunately, existing security vulnerabilities in the underlying network hardware may still open a user's computer to security issues.

Recently, Wired reported that security firm Cylance discovered a vulnerability in a specific brand of network routers deployed throughout many hotel chains throughout the world that could allow someone to install malware on guest' computers, analyze and record data transferred over the network, and possibly access the hotel's reservation and keycard systems.[1] Researchers were able to locate 277 vulnerable routers in 29 different countries across and over 100 of them were located within the United States.

This vulnerability was not exclusively limited to hotel chains, but also was discovered at conference centers and other facilities. It is critical that users continue to question and consider how they are connecting to the internet, especially when they are doing so on public networks or in public places, such as at coffee shops, restaurants, libraries, or even on airplanes. Any unknown access point could potentially allow an attacker to analyze and obtain sensitive information, including personal, banking, or health data. Further, additional software may be used to impersonate another person through intercepting and hijacking those transmissions. For example, an extension for the Firefox browser named Firesheep can allow an attacker to view unencrypted information from certain social media websites sent over their local network and can even allow the attacker to easily impersonate their victim on those websites. Even when information providers fix security holes that would allow Firesheep-type software to operate, hackers are quickly on their tail, attempting to exploit other weaknesses.

There are a number of effective method of protecting yourself while using public or unencrypted networks. The first is to use a Virtual Private Network, or VPN, which creates a secure connection between a user's computer and a private network in order to ensure that their communications are protected from other users on the public network. Many companies employ VPNs in order to protect their employees' connections while they are abroad, but there are many VPN providers that provide this service for a small fee. Alternatively, the prevalence of aircards and mobile hotspots through cellular phones can allow users to bypass public Wi-Fi networks entirely through the use of their own cellular networks.

The inherent risks when using unsecured networks is not limited to the theft of personal information, but can extend to the theft of corporate and proprietary data that can subject an employee or company to substantial legal risks or liability through the theft of trade secrets. However, one of the key factors that must be shown in order to recover under trade secret law is that reasonable precautions were taken to prevent disclosure or release of the allegedly secret information. With widespread instances of data breaches and theft, as well as the increasing availability of VPN networks and other security measures that can be employed to protect against those threats, taking no protection steps may not rise to the level of "reasonable precautions" that are necessary.

Finally, even though the most common threats can occur while a public network is being used, that may only be the first step in an attacker's plan. If an attacker compromises the security of a user's workstation, they may wait until it connected to a corporate network before deploying any malicious software or extracting sensitive data. Although corporate security measures may be able to identify and neutralize any such threat, the potential for damage once connected to a corporate network is substantially greater.

In some instances, the use of public networks is inevitable, but users should all be aware of the communications and associated information that are being transferred while connected to such a network. The possibility of legal risk increases dramatically when standard security measures are not followed. Seyfarth Shaw can advise you how to develop a proactive plan to mitigate risks to your employees, yourselves, and your business associates and customers.

[1] Big Vulnerability in Hotel Wi-Fi Router Puts Guests at Risk, *available at* http://www.wired.com/2015/03/big-vulnerability-hotel-wi-fi-router-puts-guests-risk.

New Jersey Supreme Court Confirms Aspiring Whistleblowers Can't Help Themselves to Confidential Documents

By Robert T. Szyba and Jade Wallace (June 24, 2015)

In a pivotal decision with broad implications for aspiring New Jersey whistleblowers, yesterday the New Jersey Supreme Court affirmed the Appellate Division's finding that no qualified privilege exists to protect an employee from criminal prosecution for taking confidential documents from her employer under the guise of gathering evidence for an employment lawsuit.

In *State v. Saavedra*, A-68-13 (June 23, 2015), a former public employee, Ivonne Saavedra, was criminally indicted on charges of second-degree official misconduct and third-degree theft of public documents after taking hundreds of highly confidential original and photocopied documents from her former employer, the North Bergen Board of Education. These documents, which contained sensitive personal information, such as individual financial and medical information regarding individual minor students, were taken by Saavedra in support of her whistleblower retaliation and discrimination claims against the Board. Saavedra alleged that she was a victim of gender, ethnic, and sex discrimination, as well as hostile work environment and retaliatory discharge.

Saavedra moved to dismiss the indictment, arguing that, in *Quinlan v. Curtis-Wright Corp.*, 204 N.J. 239 (2010), the New Jersey Supreme Court "establishe[d] an absolute right for employees with employment discrimination lawsuits to take potentially incriminating documents from their employers." In *Quinlan*, the plaintiff's employment was terminated after her employer discovered that the plaintiff copied about 1,800 pages of confidential information without authorization, and gave them to her attorney to use in the lawsuit. The plaintiff added a claim of retaliation to her lawsuit and was awarded a multimillion dollar verdict. The New Jersey Supreme Court upheld the jury verdict, finding that the plaintiff had engaged in protected activity that could not lawfully serve as a grounds for termination.

Analyzing Saavedra's argument, the Appellate Division found that *Quinlan* did not apply in criminal cases, and instead of a bright-line prohibition against taking company documents, established a totality-of-the-circumstances test for use in civil litigation.

The New Jersey Supreme Court agreed. It confirmed that the "decision in *Quinlan* did not endorse self-help as an alternative to the legal process in employment discrimination litigation. Nor did *Quinlan* bar prosecutions arising from an employee's removal of documents from an employer's files for use in a discrimination case, or otherwise address any issue of criminal law." On the contrary, the Court explained that the *Quinlan* decision stands for the proposition that an employer's interest must be balanced against an employee's right to be free from unlawful discrimination when assessing whether an employee's conduct in taking documents from his or her employer constitutes a protected activity. The Court pointed to the discovery procedures available to litigants that would have provided Saavedra access the same documents that she took, but would have allowed the trial court the opportunity to

balance her interests with the Board's interests, including any concerns about the privacy of minor students and their parents.

Despite the fact that the Court declined to provide an automatic shield from prosecution under *Quinlan*, the Court pointed out that in such circumstances, the employee will nevertheless be able to assert a claim of right defense or a justification. Thus, the employee will still be able to assert that his or her taking of the employer's documents was justified. And there, the Court suggested, *Quinlan*'s guidance may assist the trial court in analyzing the particular facts and circumstances to determine whether the employee can assert this defense.

The New Jersey Supreme Court has thus clarified that although self-help tactics may be justifiable in certain circumstances, *Quinlan* did not establish or endorse an unfettered right of employees to surreptitiously take documents from the workplace for their own use in litigation or otherwise. New Jersey employers, especially those who may be concerned with customer identity theft and data breaches, have won an important victory to assist in guarding against the unauthorized, and often covert, taking of confidential documents and information.

Robert T. Szyba and Jade Wallace are associates in the firm's New York office. If you would like further information, please contact a member of the Whistleblower Team, your Seyfarth Shaw LLP attorney, Robert T. Szyba atrszyba@seyfarth.com, or Jade Wallace at jwallace@seyfarth.com.

How a Trade Secret Could Have Saved a Running Royalty From a Nearly Invincible Law

By Michael Baniak (June 25, 2015)

In *Kimble v. Marvel Entertainment, LLC*, just handed down June 22, 2015, the Supreme Court reaffirmed the 50 year old holding of *Brulotte v. Thys Co.*, 379 U. S. 29 (1964), that patent royalties cannot extend beyond the expiration of the patent. So why is this case being discussed in a blog directed to trade secrets? Because the Court also reiterated that post-expiration royalties are allowable so long as they are tied to a non-patent right; and typically one of the most readily available such rights are trade secrets that almost invariably reside with the technology being licensed (or sold for that matter).

But first, back to the *Kimble* story, just for fun (and the Supreme Court did have some fun with this story).

Kimble developed a toy that would shoot "webs" (actually pressurized foam string from the palm of the hand). Naturally, he goes to Marvel Entertainment, home to Spider-Man. Marvel then comes out with its "Web Blaster," for "web-slinging fun"; but without paying Kimble. Kimble puts a spider-bite on Marvel and the resulting lawsuit produces a settlement under which Marvel bought the patent, paying a lump sum and a 3% royalty going forward–except the royalty provision has no expiration date.

Amazingly, both parties later professed that they knew not of the seminal *Brulotte* case when they entered into the agreement. But Marvel ultimately "stumbled across" it, and thus ensued a DJ action that Marvel could cease paying upon conclusion of the patent's story-arc. The case found its way to the Ninth Circuit, which while acknowledging extensive criticism of *Brulotte* over the years, concluded that its holding must reluctantly be followed. The Supreme Court then webbed-up the case on *certiorari*, to decide whether *Brulotte* should now be overruled.

Writing for the majority, Justice Kagan said *stare decisis* had to prevail, notwithstanding that the Court may now believe that the prior decision was incorrect: "we require as well what we have termed a 'special justification–over and above the belief 'that the precedent was wrongly decided.'" And since this case lies at the intersection of patent and contract, overturning *Brulotte* could "upset expectations" of agreements entered into. "As against this superpowered form of *stare decisis,* we would need a superspecial justification to warrant reversing *Brulotte*." (The dissent noted that no such "super-duper protection" for that decision existed). Good alone would not trump evil in this situation. "*Stare decisis* means sticking to some wrong decisions."

All said and done, the Supreme Court concluded that plainly Congress wasn't stirred to change the law over the last five decades. Justice Kagan stated the law "is simplicity itself to apply. A court need only ask whether a licensing agreement provides royalties for post-expiration use of a patent. If not, no problem; if so, no dice." No dice, because the patent monopoly would thereby extend beyond the life of the patent, violating an essence of the patent grant, which places the invention in the public domain

upon expiration, regardless of who you are (even a licensee). “Patents endow the holder with certain super powers, but only for a limited time.” Thus, it was up to Congress to do something, not the Supreme Court. “What we can decide, we can undecide. But *stare decisis* teaches that we should exercise that authority sparingly. Cf. S. Lee and S. Ditko, Amazing Fantasy No. 15: “Spider-Man,” p. 13 (1962) ([I]n this world, with great power there must also come—great responsibility)”. Therefore unlike Spider-Man, this Justice league would not be coming to the rescue.

So back to trade secrets. There are ways around *Brulotte*. One is that a licensee and licensor could agree to defer payments for pre-expiration use to a post-expiration period; of course, that could still not be keyed to anything smacking of ongoing “royalties.” Easier is the situation where there are trade secrets involved in the transaction, and know-how, show-how and who-doesn’t-know-what-how is so very often part of the deal. The so-called hybrid license. As Justice Kagan put it, “[t]hat means, for example, that a license involving both a patent and a trade secret can set a 5% royalty during the patent period (as compensation for the two combined) and a 4% royalty afterward (as payment for the trade secret alone).”

Frankly, that is a bit too much of a simplistic example, as the allocation between patent and trade secrets has implications, such as the impact on other just pure patent royalty deals to be had and valuation of the patent rights, just to name two. Further, savvy licensees are not likely to accept a deal that leaves the trade secret part of the arrangement running forever. But it can happen.

The point remains, however, that once you can toss something more into the license or sale of the invention rights beyond the patent, like trade secret transfer, then you can “do whatever a spider can” with royalty expiry.

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

By Robert B. Milligan, James D. McNairy, and Daniel Joshua Salinas (June 29, 2015)

We are pleased to announce the webinar "How and Why California is Different When it Comes to Trade Secrets and Non-Competes " is now available as a podcast and webinar recording.

In Seyfarth's fifth installment of its 2015 Trade Secrets Webinar series, Seyfarth attorneys focused on recent legal developments in California trade secret and non-compete law and how it is similar to and diverse from other jurisdictions, including: a discussion of the California Uniform Trade Secrets Act, the interplay between trade secret law and Business and Professions Code Section 16600, which codifies California's general prohibition of employee non-compete agreements, and recent case developments regarding non-compete agreements and trade secret investigations. The panel discussed how these latest developments impact counseling, litigation and deals involving California companies.

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

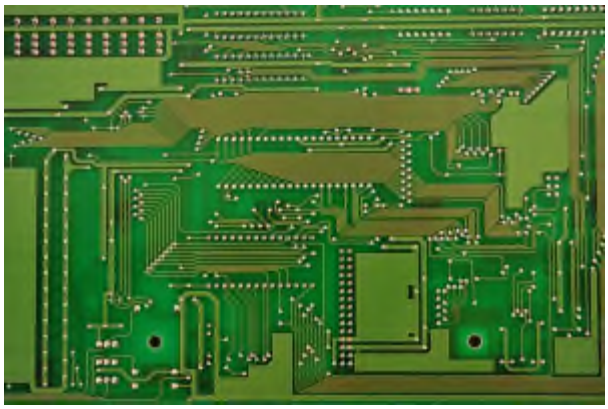
- Broad "no re-hire" provisions in settlement agreements may, under certain circumstances, constitute unlawful restraints of trade under California law, as reflected in *Golden v. California Emergency Physicians Medical Group*(9th Cir. April 8, 2015).

- Alone, voluntary dismissal of a trade secret claim is not a safe harbor to liability for attorneys' fees if the claim otherwise meets the criteria for having been brought or maintained in bad faith.

- The preemptive scope of California's Uniform Trade Secrets Act is very broad. As a result, tort or conversion claims that might be viable in other states may be preempted when pleaded in California with a trade secret claim, provided independent unlawful acts are not alleged.

Sales Of $8,000 Stemming From Trade Secret Misappropriation Results In Liability For $1.3 Million

By Paul E. Freehling (July 23, 2015)



At a time when an ex-employee's newly created company was subject to an injunction prohibiting misappropriation of his former employer's supposed trade secret, the new company allegedly used that confidential information on a few occasions in the course of providing services. The former employer sued. Although the trial court found no violation of the injunction, that ruling was reversed on appeal, and the new company was ordered to pay $1.9 million to the former employer. *Analog Technologies Corp. v. Knutson*, Case No. A14-1721 (Minn. App., July 13, 2015) (not for publication).

Summary of the case

Shortly after leaving the employ of Analog, an electrical engineering company, Knutson formed Dimation, a competitor company. Dimation allegedly used a trade secret process belonging to Analog for installing and repairing printed circuit boards. Analog sued for misappropriation and initially was awarded $1.9 million. The court also enjoined Dimation from using that process for three years. After filing for bankruptcy, Dimation executed a confession of judgment. The confession document contained an Early Payment Option (EPO). Pursuant to the EPO, the judgment would be satisfied if $600,000 was remitted by a specified date, but the EPO would expire if (a) there was a default in payment, or (b) the injunction was violated. Dimation paid as promised, but Analog rejected the final payment. It sued Dimation, claiming the EPO was void because the injunction had been violated. The trial court found no violation. A few days ago, the Minnesota Court of Appeals reversed and awarded Analog the full $1.9 million judgment less the $600,000 already paid.

The parties' litigation

Analog I. Analog's first trade secret misappropriation lawsuit resulted in a 2009 judgment against Dimation for $1.6 million and attorneys' fees. In addition, that company was enjoined from further misappropriation for three years. It filed for bankruptcy and then executed the confession described above. Dimation also challenged the injunction in the Minnesota appellate court. In 2011, that court substantially affirmed but remanded with instructions to clarify the injunction order.

Analog II. On remand, the parties agreed to certain modifications of the injunction, but Dimation proposed still more. In 2013, the trial court entered a new injunction in the form requested by Analog. Dimation appealed on the grounds that Analog had no protectable trade secret and that the trial court had not complied in full with the appellate court's remand instructions. Late in the year, the 2013 trial court order was affirmed.

Analog III. While *Analog II* was pending, Analog asked the lower court to find Dimation in contempt for violating the earlier injunction. Dimation responded by requesting entry of an order to the effect that the EPO terms had been satisfied. During an evidentiary hearing, Knutson testified that from April 2011 to

February 2012, Dimation had made "at the most" 10 infringing sales amounting to $8,000. The court held that Dimation did not violate the injunction and should not be held in contempt. Analog appealed. The Court of Appeals affirmed in part and reversed in part.

The ruling in *Analog III*

1. *Misappropriation.* The lower court was reversed. Dimation stressed that the lower court had found as a fact that Analog had failed to prove infringement of its supposed trade secret. The appellate tribunal held that the finding clearly was erroneous. Earlier decisions upheld the validity of Analog's trade secret. Knutson's own testimony established a violation of the 2009 injunction order, an order which *Analog I* did not vacate or reverse. Further, Dimation breached its contractual obligation (set forth in the confession of judgment) not to violate the injunction.

2. *Contempt*. The lower court was affirmed. Analog claimed that the lower court erred by refusing to find Dimation in contempt of the 2009 order. The appellate court found no abuse of discretion. It said that Dimation had been found to be in civil (not criminal) contempt, and that the purpose of civil contempt is remedial, not punitive. Since the court's decision in *Analog III* reinstated the original $1.9 million judgment, "finding Dimation in contempt would serve no further remedial purpose."

Takeaways

Dimation was held to have made the $8,000 in allegedly infringing sales during a period when it was prohibited by court order from making any. By also contracting not to make those sales, Dimation gave Analog a second string to its bow: breach of contract. Dimation seemingly speculated that (a) if it was sued for violating the injunction or breaching the contract, it could prove that Analog had no protectable trade secret, and (b) if that gambit failed, the miniscule amount of sales it had made would suffice to persuade a court not to find a violation that might result in a nearly $2 million judgment against Dimation.

The principal takeaway from the recent Minnesota Court of Appeals decision is that Dimation engaged in risky conduct. Judges rarely are sympathetic towards parties that violate court orders while simultaneously appealing the issue of whether the order is valid. Moreover, many court cases hold that violation of an injunction while it is in effect is inappropriate even if the injunction later is found to be unenforceable.

Trading Secrets

Trade Secret Protection: What are Reasonable Steps?

By Pamela Passman (July 31, 2015)

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)

Regional and national laws are increasingly focusing on the specific steps that companies should take to protect trade secrets. In the 1996 World Trade Organization (WTO) Trade-Related Aspects of Intellectual Property Rights (TRIPs) Agreement, and in many countries' laws, the definition of a trade secret includes the requirement that the owner or other controller undertake "reasonable steps" or "reasonable efforts" to protect the secrecy of its information. A "reasonable steps" requirement is also included in the draft EU Directive on the Protection of Undisclosed Know-How and Business Information (Trade Secrets) which, if adopted, would become part of the national legislation in all 28 EU member countries. New legislation proposed at the national level in the U.S. likewise has contained similar requirements.

In addition to implementing "reasonable steps" to prevent trade secret theft and misuse, taking such steps can also have crucial legal significance. Where the legal definition of trade secrets includes a "reasonable steps" or similar requirement, a court can find that a company's information is not in fact a trade secret at all if such steps are not taken. Failing to take adequate precautions to protect such information thus can preclude a company from getting any legal redress if the worst happens and an unauthorized disclosure or use of the information does take place. Case in point: the failure of the MBL (USA) Corporation to inform employees "what, if anything, [the company] considered confidential" was one of the key failures that led the court to dismiss MBL's case against its former employee.

What exactly are "reasonable efforts"? A new whitepaper by the Center for Responsible Enterprise And Trade (CREATe.org) offers insights into the evolving legal landscape, cases and recommendations for an effective trade secret protection plan. Here are some key takeaways:

- **Make sure agreements and policies are in place – and procedures as well.** Many companies rely on nondisclosure and other agreements with employees and third parties – and the courts have looked favorably on these as evidence of "reasonable steps." However, corporate policies – and equally important, procedures to ensure policies are being followed – are also critical. Companies that adopted procedures to implement key aspects of trade secret protection often prevail in lawsuits. These include procedures such as marking sensitive documents as confidential; segregating confidential information or processes into discrete parts so no single employee or vendor has full control; and conducting exit interviews that include the return of confidential information.

Trading Secrets

- **Identify, assess and manage risks.** To protect trade secrets, you first need to identify, classify and assess potential risks to confidential technical and business information. Courts have reviewed whether material is included in a trade secret registry and if reasonable efforts have been made to keep the information confidential.

- **Put an information protection team in place.** Trade secrets – which include information that ranges from customer lists and financial data to product prototypes, source code and unique know-how – often reside in many different parts of an organization. Putting together a cross-functional team headed by someone with overall control helps to ensure that adequate protections are in place throughout the organization, and provides the foundation for effective response in the event of trade secret misappropriation.

- **Extend physical and network security to address trade secret protection.** New government regulations are increasingly insisting upon robust security systems for protecting trade secrets. Courts look at such measures as well. In Japan, courts determining the adequacy of secrecy measures have insisted, among other actions, that a company must "implement physical and electronic access restrictions" in order to be protected by Japan's unfair competition rules protecting trade secrets.

It is important to note, however, that many IT and physical systems aren't designed with protection of trade secrets or other particular intellectual property in mind. Companies need to take steps to ensure that their valuable trade secrets are identified and that security systems are designed with a specific objective to make them secure – through access control, technical measures, physical restrictions, monitoring and other actions. For example when the U.S. government attempted to prosecute a former computer programmer who had worked on the investment bank Goldman Sachs's proprietary high-frequency trading platform, the trial court noted with approval the multiple electronic-security systems that Goldman had in place to protect such information. These included maintaining a firewall, monitoring employee use of internet sites, blocking access to certain websites, implementing pop-up banners that advised employees logging in to their computers of acceptable and prohibited uses, restricting access to firm computers, and restricting use of USB flash drives to only a few employees with administrative access.

- **Engage employees and third parties.** In addition to agreements, companies need to inform and educate staff and third parties such as suppliers and other business partners about what is considered confidential and their role in protecting trade secrets.

- **Monitor and take corrective actions.** Courts have looked favorably on companies that have approached trade secret protection in a systematic rather than an ad hoc fashion. Putting business processes in place and measuring and improving these over time offer companies a robust way to protect confidential information. In a case involving Aetna, the court looked favorably on the firm's practice of employees signing nondisclosure agreements annually rather than just when starting. It is a good example of building employee awareness and monitoring to ensure that agreements are in place.

Courts have also examined the corrective actions that companies have taken against breaches. For example, the Pre-Paid Legal Services company found that its practice of taking corrective actions against trade secret breaches – sending cease and desist letters and entering into agreed injunctions against former employees who had misappropriated trade secrets – was helpful in winning its case against former employees and contractors who had used the company's employee contact, performance and other confidential information to recruit other Pre-Paid staff.

Trading Secrets

Trade secrets are critical to virtually every modern company. To help mitigate the loss of proprietary and confidential information, and meet the “reasonable steps” requirement, it is vital for companies to put systems in place that embed trade secret protection in an ongoing and systematic way across an enterprise.

Pamela Passman is President and CEO of the Center for Responsible Enterprise and Trade (CREATe.org), a global nongovernmental organization helping companies prevent corruption and protect intellectual property. Prior to founding CREATe in October 2011, Passman was the Corporate Vice President and Deputy General Counsel, Global Corporate and Regulatory Affairs, Microsoft Corporation.

Recent Developments on Copyright Preemption of Trade Secret Claims in the Fifth Circuit

By Matthew Werber (August 5, 2015)

For the latest on the copyright preemption doctrine (codified at 17 U.S.C. § 301(a)) look no further than the Fifth Circuit, which, together with its district courts, issued a string of recent decisions regarding the preemption of trade secret claims involving software. Most recently, the Fifth Circuit found that preemption extends to all fixed original works of authorship, even those works incorporating ideas, systems and processes, among other types of noncopyrightable material as defined in § 102(b) of the Copyright Act. *Spear Mktg., Inc. v. BancorpSouth Bank*, Case No. 14-10753 (5th Cir. June 30, 2015).

Spear Mktg involved claims that the defendants violated the Texas Theft Liability Act ("TTLA") and several other Texas laws by allegedly stealing technical and business trade secrets incorporated in software products for the banking industry. The defendants removed the case to the N.D. Texas on preemption grounds because the plaintiff alleged they received the alleged trade secret information through screen prints and product demos — information and ideas fixed in a tangible medium as would be required in a copyright claim. The plaintiff petitioned for remand, which the district court denied.

On appeal, the Fifth Circuit focused on preemption of the TTLA claim, applying the well-established two-part test to determine whether a state law claim is preempted by the Copyright Act:

First, the claim is examined to determine whether it falls "within the subject matter of copyright" as defined by *17 U.S.C. § 102*. And second, "the cause of action is examined to determine if it protects rights that are 'equivalent' to any of the exclusive rights of a federal copyright, as provided in *17 U.S.C. § 106*.

For the first element, the court explained that it favored the defendants' reading of the preemption doctrine, finding that "state law claims based on ideas fixed in tangible media are preempted." In doing so, the Fifth Circuit sided with the Second, Fourth, Sixth and Seventh Circuits on this question, departing only from the Eleventh Circuit's reading. This was the Fifth Circuit's first time addressing this issue because, as the unanimous panel noted, its prior decisions generally focused on the second ("equivalency") element of the preemption test, which is typically more hotly litigated.

With regard to the second element, the court reasoned that the TTLA claim consisted of allegations of "copying, communicating, and transmitting," which the court found sufficiently equivalent to the exclusive rights protected by copyright law.

Trading Secrets

Another trade secret defendant may look to *Spear Mktg* for support in appealing a 15 million dollar judgment issued by the same Texas district Court. *GlobeRanger Corp. v. Software AG*, Case No. 15-10121 (5th Cir. 2015). *GlobeRanger*involves a Texas trade secret misappropriation claim, which the district court found was not preempted based on the presence of "extra" elements, such as improper use, not present in a copyright claim. *GlobeRanger Corp. v. Software AG,* 3:11-CV-0403-B (N.D. Tex June 11, 2015). These extra elements, according to the court, weigh against an equivalency finding.

Some commentators anticipate that *Software AG* will rely heavily on *Spear Mktg* in its appeal, but a closer look at the*Spear Mktg* opinion may give *Software AG* some pause. In particular, the *Spear Mktg* panel commented on*Globeranger* and an earlier appeal for that case, suggesting that Globeranger's trade secret misappropriation count differs from the TTLA count in *Spear Mktg*.:

GlobeRanger, our most recent foray into copyright preemption, appears to touch on the issue, but the claims in that case involved actual physical acts, not just software:

Software AG's opening brief in the *GlobeRanger* litigation is due later this month, and trade secret practitioners will be watching closely to determine if the Fifth Circuit choses to extend the preemption doctrine even further.

Employer's Action for Misappropriation of Trade Secrets Against Former In-House Counsel Who Engaged in Competitive Activities Not Subject to Anti-SLAPP Motion

By Enedina Cardenas (August 6, 2015)

There are indeed limits to the reach of the anti-SLAPP statute, particularly in the trade secret context. In *West Hills Research and Development, Inc. v. Terrence M. Wyles*, a California appellate court ruled that engaging in activity to set up a competing business is not protected activity under the anti-SLAPP statute.

Summary of the Case

West Hills, a medical products company, terminated Wyles, its in-house IP attorney, after discovering he was attempting to set up a competing business with trade secrets he allegedly acquired from West Hills. West Hills sued Wyles for misappropriation of trade secrets, intentional interference with economic advantage, negligent interference with economic advantage, computer fraud and abuse, conversion, breach of loyalty, breach of confidence, and unfair competition. West Hills alleged that Wyles had improperly taken documents containing trade secrets, and confidential and proprietary information.

Wyles denied accessing any trade secret information and claims he only took documents that were relevant to a derivative shareholder lawsuit that he contemplated bringing against the company.

The Anti-SLAPP Motion

Wyles moved to dismiss the complaint based on the Strategic Lawsuit against Public Participation (SLAPP) statute codified in California Code of Civil Procedure Section 425.16. The statute permits the court to strike a "cause of action against a person arising from any act of that person in furtherance of the person's right of petition or free speech." C.C.P. § 425.16(b)(1). The court focuses on the "principal thrust or gravamen" of the complaint.

Wyles' anti-SLAPP motion was premised on his claim that West Hill's officers embezzled money, engaged in tax fraud, and other financial malfeasance. Wyles argued that his conduct constituted pre-litigation communication and was therefore protected under Civil Code Section 47(b).

West Hills convinced the court that Wyles had in fact taken trade secrets belonging to West Hills, and that Wyles used that information to try to form a competing business. West Hills presented evidence that Wyles attempted to recruit West Hill's consultant to join the new company. Wyles told this consultant that his competing company would "take over" West Hills' business and patents. The consultant also saw agreements between Wyles' new company and West Hills' competitors.

West Hills also identified the following trade secret documents in Wyles' possession: a confidential business plan, privileged and confidential drafts of a patent application, a confidential technical product description, and confidential agreements with potential partners.

The trial court denied Wyles' motion, and Wyles appealed.

The Appeal

Applying de novo review, the California Court of Appeal, Second District, held that Wyles did not meet his burden of showing that West Hill's claims were actually based on his intention to file a derivative action. Instead, the gravamen of West Hill's complaint was Wyles' improper access and use of West Hill's trade secrets to form a competing venture.

The court focused its attention on the evidence submitted by the parties. Wyles did not deny taking trade secret information, rather he insisted that the documents supported his embezzlement claims against the company. The court found that these documents were not germane to the contemplated shareholder derivative lawsuit.

Competing Conduct Is Not Protected Activity

The court distinguished privileged pre-litigation *communications* from competitive *conduct*. The court also acknowledged that the anti-SLAPP statute recognized pre-litigation communications that are encompassed by the litigation privilege under Civil Code Section 47(b). However, the court rejected Wyles' argument that he had engaged in such protected activity. The court noted that the litigation privilege extended to communications, not conduct. Thus, the privilege applied to a statement Wyles made to a West Hill investor concerning the alleged financial malfeasance. But, the privilege did not apply to Wyles' *activities* in furtherance of establishing a competing business.

Takeaway

The anti-SLAPP statute was intended to protect the public's participation in government, in particular speech protected by the First Amendment. Indeed, courts generally give credence to anti-SLAPP motions where speech is involved. In the trade secret context, an anti-SLAPP motion can be successful when it involves purported defamatory speech or communication.

Therefore, a critical factor to fend off an anti-SLAPP motion appears to be defendant's competing activity or conduct, and not speech. West Hills alleged that Wyles engaged in competing activities. It supported those allegations with evidence which unequivocally demonstrated Wyles acted for his own financial gain, rather than communicating or making statements for purposes of bringing a shareholder derivative action.

A company wishing to protect its trade secrets should highlight conduct demonstrating the defendant's use of the trade secret. This, however, can present an obstacle for many plaintiffs at the onset of litigation. Since most anti-SLAPP motions are brought before discovery commences, a company may not always have sufficient evidence of competing conduct by the defendant.

Trading Secrets

Inevitable Disclosure Doctrine Held Inapplicable To Failed Business Transaction

By Paul E. Freehling (September 3, 2015)

An Illinois appellate court recently rejected applying the inevitable disclosure doctrine in a trade secret misappropriation spat arising out of a failed business transaction.

After first securing an executed confidentiality agreement, Destiny, the developer of a proprietary healthcare wellness program called "Vitality," shared details of it with Cigna, a healthcare insurer. The insurer decided instead to create a wellness product of its own called "Empower." Destiny sued Cigna for trade secret misappropriation and breach of contract, alleging circumstantial evidence and "inevitable disclosure." Cigna's summary judgment motion was granted, and the appeals court affirmed. *Destiny Health, Inc. v. Connecticut Gen. Life Ins. Co.*, No 1-14-2530 (Ill. App. Court, 1st Dist., Aug. 21, 2015).

Status of the case

Because of a possible interest in "Vitality," Cigna was considering entering into a joint venture or partnership with Destiny, or making an offer to acquire the company. Destiny obtained a signed non-disclosure agreement, prohibiting use or misappropriation of Destiny's confidential information, and then allowed Cigna to take a "deep dive" into data relating to "Vitality." The insurer ultimately decided that "Vitality" was too expensive and lacked flexibility. Thereafter, with the assistance of others, Cigna created and began using "Empower." Claiming that Cigna inevitably misappropriated Destiny's intellectual property and breached the confidentiality agreement, the developer sued the insurer but to no avail.

Background facts

"Vitality" was used to motivate employees to engage in specific healthy activities and to be rewarded for doing so. After deciding not to use "Vitality," Cigna designed and developed "Empower" with some assistance from a different vendor. Both "Vitality" and "Empower" incentivize healthy activities by providing rewards. "Vitality" does not permit employers to change the activities or the points to be awarded for each whereas employers using "Empower" can customize both the activities and the awards. Soon after "Empower" was launched, Destiny sued in the Circuit Court of Cook County. Following several years of discovery, Cigna moved for summary judgment.

Arguments for granting Cigna's motion

The insurer maintained that Destiny provided it with no trade secrets and that, in creating "Empower," it used nothing learned from the developer. Cigna also asserted that Destiny cannot prove damages.

Several Illinois court rulings recognize the "inevitable disclosure" doctrine. Cigna purported to distinguish those decisions on the grounds that they all came early in the litigation, in connection with motions to dismiss or for a preliminary injunction, and all involved employer-employee disputes. According to Cigna, since the instant lawsuit had passed those preliminary points and had reached the summary judgment stage, and because the case concerned a failed business transaction, the doctrine was inapplicable. Cigna cited *Omnitech Int'l v. Clorox Co.*, 11 F.3d 1316, 1325 (5th Cir. 1994), which held that, in a failed business transaction case, absent evidence of actual disclosure, an inference of misuse or misappropriation of trade secrets cannot be based on unsupported speculation. Cigna also referred the court to Connecticut and New York court decisions holding that the "inevitable disclosure" doctrine cannot be used to create a triable issue of fact in opposition to a summary judgment motion.

Arguments against granting summary judgment

Destiny admitted relying on circumstantial evidence but emphasized that it often is used to prove misappropriation. The developer stressed that the Cigna team members who had evaluated "Vitality" had no prior experience with incentive-points platforms, and yet they designed "Empower" quickly after concluding that evaluation. According to the developer, what the insurer learned from Destiny inevitably provided "a footprint for Cigna to work from in creating its own wellness" product. Destiny insisted that the insurer should have constructed a "firewall" or "white room" to insulate the "Vitality" evaluation team from participating in the creation of "Empower."

Further, Destiny contended that the question of whether the insurer inevitably used the developer's intellectual property involved disputed issues of material fact which precluded entry of summary judgment for Cigna. Destiny also argued that the same policy reasons underlying application of "inevitable disclosure" in a dispute between a former employer and its ex-employee apply when a business suitor is given access to confidential information and then uses it to create a competitive product.

The ruling

The Illinois Appellate Court affirmed judgment for Cigna:

"The fact that the information provided by Destiny might have made Cigna more informed in evaluating whether to partner with Destiny or another vendor in the development of an incentive-points program does not support an inference that Cigna misappropriated Destiny's trade secrets absent some showing that Cigna would not have been able to develop its incentive-points program without the use of Destiny's trade secrets."

Takeaways

As Cigna argued and both courts agreed, *Omnitech Int'l* is the leading decision regarding the inapplicability of the "inevitable disclosure" doctrine to a failed business transaction. The court there stated that a potential acquiring company must be free to examine the books of all potential targets and should not be presumed to have revealed confidences.

Unless precluded, a potential acquirer often uses the same team to evaluate all targets. A target concerned about an "inevitable disclosure" would be well advised to obtain an express commitment from the potential acquirer to create a "firewall." Without such a commitment, the target may be unable to win a failed business transaction lawsuit claiming misuse of proprietary data unless (a) the target can show instances of actual misappropriation of its confidential information, or (b) the target can demonstrate that the potential acquirer could not have succeeded in entering into competition with the target without using the target's secrets.

Trade Secrets or Patents – Why Software Presents No "One Size Fits All" Solution

By Patrick Muffo (September 14, 2015)

There are many ways to obtain intellectual property protection for software creations. Many keep the software code confidential and maintain the software as a trade secret. Others seek patent protection on the software, which discloses the higher-level concepts surrounding the software without explicitly publishing the source code. Recent changes in patent law have changed what types of software inventions are patentable and the requirements for obtaining such patents. However, the evolution of the law has been ongoing for quite some time.

The Supreme Court has struggled to define what types of software inventions are patentable in a string of cases over the past fifty years. The most recent case, *Alice Corp. Pty. Ltd. v. CLS Bank Intern.*, 134 S. Ct. 2347 (2014), held that an invention directed to an abstract idea is not patentable simply because it is implemented on a general purpose computer. In particular, *Alice* and its progeny held that a software invention is not patentable if it (1) recites an abstract idea; and (2) does so without claiming "something more" that transforms "the nature of the claim into a patent-eligible application." *Id*. at 2357.

The "abstract idea" prong has been confusing at best. *Alice* failed to define the test for determining what constitutes an abstract idea. *Id*. "[W]e need not labor to delimit the precise contours of the 'abstract ideas' category in this case." As a result, courts and patent practitioners have struggled with this lack of guidance from the Supreme Court, with one court even recognizing it "could never succeed in intelligibly" defining what constitutes an abstract idea, but that "I know it when I see it." *McRO Inc., v. Activision Pub., Inc.*, No. CV 14-336-GW, 2014 WL 4759953, at *5 (C.D.Cal. Sept. 22, 2014). The Patent Office itself declined to issue a bright line rule, instead opting to rely on examples provided by the courts. July 2015 Update to Interim Guidelines, p. 1 "Because the courts have declined to define abstract ideas, other than by example, the 2014 IEG instructs examiners to refer to the body of case law precedent in order to identify abstract ideas by way of comparison to concepts already found to be abstract." Nonetheless, many software inventions are not considered abstract ideas.

The "something more" prong has borne more fruit for software patents. For example, the Court of Appeals for the Federal Circuit declined to invalidate a patent for an invention that overcomes a problem in computer networks. *DDR Holdings v. Hotels.com*, No. 2013-1505 (Fed. Cir. December 5, 2014). The patents in *DDR Holdings* addressed a problem in e-commerce, that a third party merchant can "lure" away visitors of a host web page when a user clicks on the link of the third party merchant. The system of the *DDR Holdings* patents "generates and directs the visitor to a composite web page that displays product information from the third-party merchant, but retains the host website's 'look and feel.'" *Id*. at 3-4. While the majority opinion did not specify whether the invention was directed to an abstract idea, it held the invention was patent-eligible due to its function of improving computer technology. The software in*DDR Holdings* is but one example of a patent-eligible software invention.

Trading Secrets

Takeaway

There is no “one-size-fits-all” solution for protecting software. Trade secret protection can be inexpensive, but can become weak if the software is publicly disclosed or otherwise disseminated. Also, trade secret protection can be obtained in combination with patent protection, with the patent protecting the higher level concepts around the software and the trade secret protecting the source code or other details. In the end, it is best to determine the type of invention sought to be protected and the best form of intellectual property that fits the particular invention. The Seyfarth PTAB Blog discusses many of these trends at www.seyfarth.com/PTAB-blog.

This is a guest post from Patrick Muffo, a writer at the Seyfarth Patent Trial and Appeal Board blog (www.seyfarth.com/PTAB-blog). The Patent Trial and Appeal Board (PTAB) blog discusses recent decisions and trends of the PTAB and provides an overview of prevailing patent topics.

Trading Secrets

Frequently Asked Questions Regarding Trade Secret Disputes and Employment Risks Answered

By Robert B. Milligan and Michael Wexler (September 18, 2015)

In today's post, we have answered some of the most frequent and significant questions that we are asked about trade secret disputes and employment risks.

1. **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 organized 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 unionized 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.

2. **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 utilizing non-compete or non-disclosure 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 employees/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.

3. **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, pro-active 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 employees, including using or disclosing their former employers' trade secrets, and retaining any of their former employers' property. It's 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 analyze 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 email accounts can alert an employer to theft of information. More sophisticated methods such a 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.

4. **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 in 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 realizing 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 your company's review and access of such information does not violate applicable law.

5. **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 honor 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's important to preserve data, review emails, and talk to relevant witnesses to interpret the forensic data. A digital forensics examination often includes collecting and analyzing artifacts from the operating system, internet history, and unallocated space. Routine eDiscovery does not typically delve into questions about the source computer or storage device and ESI, although eDiscovery may uncover the need to ask questions related to internet history, webmail, cloud storage, mobile devices and phone back-ups, and removable devices.

6. **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 and/or Computer Fraud & Abuse Act claims as well as similar state criminal laws, but businesses need to be aware of two important points:

1) 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, and 2) 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 U.S. Senate and House are currently considering legislation on this issue.

7. **What kinds of challenges do US companies face in pursuing trade secrets and non-compete claims against foreign companies, particularly from China?**

Milligan: U.S. companies may face the challenge of not being able to enforce injunctive relief orders and judgments, as well as jurisdictional challenges posed by foreign companies. Additionally, in some cases, Chinese companies doing business in the U.S. have quite limited assets in the U.S. and individual defendants may be judgment proof. Even if a U.S. company obtains a favorable judgment from the U.S. court, the judgment may not be recognized or enforceable in China, and thus, the company may not obtain sufficient monetary or equitable remedy. Therefore, the U.S. company must carefully select its business partners and the jurisdiction in a confidentiality or non-compete agreement to attempt to enhance its ability to obtain an injunction and judgment. If forced to sue abroad, remember the court systems are different and there are different views on IP. Your company may not be able to get complete relief in a foreign jurisdiction. The EU Commission has proposed a directive to harmonize trade secrets law in Europe that may assist in this regard in the future if approved.

8. **What are some practical considerations for US companies or multinational companies doing business in Asia and Europe to protect their trade secrets and confidential information?**

Wexler: Know your business partners. Have them fully vetted so they don't steal your IP. Try to protect your supply side with appropriate agreements. You should also be careful about what you share with your business partners. If it is bet-the-company information, consider keeping that internal. In addition to getting employees and business partners to execute well-prepared agreements, training — both on-board and on-the-job — can be a powerful measure. Employers should make sure that access to trade secrets and confidential information is granted only to those with necessity to know and make sure your local workforce abroad is trained on company policies and signs appropriate agreements to protect IP. Realize that you are not in the U.S., and the legal systems and respect for IP may be different. For example, in China, different locales may have different views on trade secret protections and non-compete agreements. For instance, the statutory minimum non-compete compensation in Shenzhen is

higher than the one in Shanghai. U.S. companies or multinational companies doing business in China should be aware of such local variations and may need to take different measures in different places to ensure protection.

Milligan: Within a foreign forum the selection of the right venue, meaning a locale where the court is more willing to implement the rule of law is essential. In China, for example, the enforcement varies by locale. For instance, recent decisions indicate that Shanghai courts are more willing to give protection to the employer in trade secret and non-compete cases, including issuing injunctive relief. Try to use contractual choice of law, consent to jurisdiction, and forum clauses for the most favorable forum for you. Also consider international arbitration. Assess your security vulnerabilities, particularly in light of the foreign locale, and put in place appropriate safeguards. Carefully access your IT security in foreign countries and be alert for unauthorized monitoring and surveillance. Provide training to executives on traveling abroad and conducting business abroad to ensure that trade secrets are not carelessly compromised.

9. **In your experience, what should a company do if a trade secret dispute arises between it and a former employee?**

Milligan: If a company suspects that valuable information has been improperly taken or compromised, you need to first assess the potential competitive threat to the company. It's important to take fast, effective action and consider whether to pursue civil remedies or criminal intervention against the former employee. If litigation is anticipated with the departure of an employee, you should take precautionary steps immediately:

- Secure and establish a chain of custody for all items returned by the departing employee, including laptop computer, desktop computer, USB devices, tablets, and physical property.
- Secure and maintain a chain of custody of the employee's office and the items in that office until it is searched.
- Retain outside counsel to investigate the departure and have outside counsel secure the services of a digital forensic investigation firm with a good reputation.
- If the employee is computer savvy, do an immediate search of the internet for relevant materials posted to social media sites, including LinkedIn, Facebook, and Twitter.

Wexler: When our clients are faced with possible trade secret misappropriation by former employees, we immediately investigate and develop the facts through interviews, document review, and collaborate with a qualified digital forensic expert. Forensic investigation of computing devices to identify the possible theft of confidential information is a must. We assess the company's business objectives as well as the chance of success, and assuming that there is sufficient evidence to pursue, we demand compliance and appropriate remedies via cease and desist demands prior to the initiation of litigation. Should written requests for compliance not be successful, we seek injunctive relief and damages to protect company assets and further our client's objectives.

10. **In the battle against trade secret theft and related disputes, do companies place enough importance on the language and provisions contained in employment contracts? How**

can employment contracts be strengthened to either reduce trade secret theft or improve the company's chances of reaching a successful outcome in a trade secret dispute?

Wexler: In our experience, companies should place more importance on their agreements with employees, vendors, and business partners to protect trade secrets. Companies need to strengthen the language and provisions contained in such agreements, including clearer definitions of protectable trade secrets, return of company property provisions, appropriate restrictive covenants, and appropriate forum and choice of law provisions. Well-drafted agreements can reduce the risk of information being misappropriated. Such agreements should be updated annually, as needed, based on changes in the law, and companies should routinely audit their practices to make sure each employee has an appropriate agreement. Companies should also make it an agreed requirement for employees to sit for an exit interview and return any company confidential information stored on any personal devices. Finally, agreements should include an attorneys' fee provision for breach.

Milligan: Additionally, a thorough exit interview should be conducted at the time any employee separates, and as part of that exit interview process, each exiting employee should be given a written reminder of their ongoing trade secret, confidentiality and social networking obligations, and should be asked to sign the reminder acknowledging receipt and their agreement to comply with such obligations. The exit interview is also the time to get company property returned by the departing employee and make any arrangements for the return and remediation of company property on any personal devices.

Trading Secrets

When E-Filing Goes Wrong: How to Protect Your Trade Secrets in the Event of Inadvertent Online Disclosure

By Lauren M. Gregory (September 23, 2015)

It is frightening to think that valuable corporate trade secrets could be lost with the click of a mouse. But as electronic court filing becomes increasingly prevalent, the risk of inadvertent disclosure of sensitive information online—and the resulting loss of trade secret protection—is becoming more and more real.

A litigant in New York recently learned this lesson firsthand, narrowly escaping what could have been extremely harsh consequences from an accidental e-filing. In *HMS Holdings Corp. v. Arendt*, the Supreme Court of New York refused to create a per se rule that would unfairly punish Plaintiff HMS Holdings Corp. ("HMS") for its mistaken disclosure of more than 1,500 pages containing corporate trade secrets, but the court did leave room for serious consequences in future cases.

The *HMS* court has created a ten-factor test that could result in loss of trade secret status under some circumstances. However, careful study of these factors can help avoid—or at least mitigate—damage in the event a mistake is made.

HMS Holdings Corp. v. Arendt

HMS owns certain proprietary systems, methodologies, and technologies specific to a niche market: state Medicaid agencies who need assistance identifying and verifying alternative forms of healthcare coverage and funding from third-party payors. HMS carefully guards these systems, methodologies, and technologies as trade secrets. So when a group of employees left to go work for a rival and attempted to bring several of HMS's customers to the competing business, HMS sought preliminary injunctive relief against them.

But the trouble really began for HMS when it filed its motion papers in preparation for its injunction hearing. Although a stipulated protective order was in place that allowed the company to designate its supporting affidavit and annexed exhibits "Attorneys' Eyes Only," HMS inadvertently e-filed an unredacted affidavit with more than 1,500 pages attached that detailed the trade secrets at issue.

The company learned of this mistake in the worst way possible: defense counsel raised the issue during the injunction hearing, insisting that filing on the New York State Courts Electronic Filing ("NYSCEF") system rendered the information public and thus vitiated its trade secret status.

Indeed, the information had been available on the Internet via NYSCEF for almost a month between the filing and the hearing, when the court issued an immediate sealing order on consent. Luckily for HMS, the court rejected the defendants' argument, noting that although NYSCEF could be accessed

online, “it does not follow that the inadvertent e-filing of an unredacted document on NYSCEF necessarily constitutes a posting to the Internet that renders the information generally known.”

The Ten Factor Test

Ultimately, the *HMS* court was hesitant to adopt a “rigid and formulaic” rule regarding inadvertent e-filing, as there was no clear precedent governing the issue. Defendants cited cases that either did not involve e-filing or predated its widespread adoption, with the exception of a single opinion finding waiver of trade secret status after “multiple, unrectified publications in court records over a span of several years.” Furthermore, there were overarching public policy concerns to consider. According to the court, creating a per se rule in this context would “frustrate the Judiciary’s important objective of promoting a modern, technologically advanced court system.”

Therefore, the court analyzed the issue by adopting factors set forth in the Restatement of Torts to determine whether “the alleged trade secrets have become generally known or readily ascertainable through proper means.”

Specifically, the court started by considering six factors:

(1) the means by which access to the filing was available;

(2) the class of persons who have (or had) access to the information;

(3) how long the filing remained accessible;

(4) the extent to which the filing actually was viewed and/or downloaded;

(5) the extent to which the material was indexed and/or made searchable on the Internet; and

(6) whether the material remains cached or otherwise available on the Internet.

The court noted that in cases where the alleged trade secrets have, in fact, been accessed and downloaded by third parties, it is also proper to consider:

(7) the extent of any re-dissemination;

(8) the likelihood of any future re-dissemination;

(9) the extent to which recipients already knew the secrets; and

(10) the extent to which such recipients are obliged to maintain the secrecy of the information.

HMS’s Trade Secret Status Remains Intact…For Now…

Certain facts in the *HMS* case raised the court’s suspicion: two former HMS employees claimed they happened to independently download the affidavit and exhibits from NYSCEF on the very same day, “simply out of a desire to stay abreast of developments concerning HMS.” The court noted that these particular individuals were former vice presidents of HMS who had access to much of the same material during their employment and who are subject to both common law and contractual obligations preventing them from re-disseminating it. Under those circumstances, the court refused to punish HMS for the inadvertent e-filing, holding that the e-filing did not destroy trade secret status so as to deprive

HMS of a likelihood of success on the merits of its trade secret claim. However, the court promised to revisit trade secret status after discovery, when "the myriad of factors necessary to the determination of that issue can be applied to a fuller and firmer factual record."

Takeaways

The *HMS* court's analysis is helpful in formulating proper internal controls for e-filing procedure. Access to trade secret information should be limited to as few individuals as possible, but not so few that an organization cannot put checks in place to ensure that each electronic court filing is completed without release of sensitive information. Prompt review after each filing should ensure that, in the event a mistake has been made, the secret information can be removed as soon as possible, reducing the number of people who can access, view, and/or download the material.

The U.S. District Court for the Northern District of California offers guidelines on its website for ensuring prompt and effective removal of erroneous e-filings. The Court suggests taking the following steps upon discovery of an inadvertent filing containing confidential information:

(1) If your judge has a docket correction e-mail, send a message to that address immediately, including your case number, docket number, and a brief description of your problem. If possible, mark your message "urgent."

(2) If during business hours, call the court to request expedited handling.

(3) File a Motion to Remove Incorrectly Filed Document(s) as soon as possible. If your Motion is granted, the erroneously filed document(s) can be permanently removed from the court's online records system.

(4) E-file a corrected (*i.e.*, redacted) version of the document. Note: you can do this right away, without awaiting the outcome of steps 1 through 3 above.

Ideally, with these protocols in place, compromises to valuable trade secret information can be kept to a minimum in the future—at least when it comes to e-filing.

Financial Projections, Strategic Plans, And Customer Contract Proposals Can Be Trade Secrets

By Paul E. Freehling (September 28, 2015)

Two competitors who do research and analysis for advertisers and media companies, concerning how television viewing impacts consumer purchasing, have been in a legal battle over alleged trade secret misappropriation, patent infringement, and other causes of action. The dispute already has produced at least six district court opinions. Recently, in a 47-page non-precedential order issued by the Court of Appeals for the Federal Circuit, the district court's summary judgment order — reported at 984 F. Supp. 2d 205 (S.D.N.Y. 2013) (Scheidlin, J.) — was affirmed in part, reversed in part, vacated in part, and remanded. *TNS Media Research, LLC v. TiVo Research & Analytics, Inc.,* No. 2014-1668 (Fed. Cir., Sept. 16, 2015).

Status of the case

TNS Media Research (referred to by the courts as "Kantar") sued TiVo (referred to as "TRA"). Kantar sought a declaratory judgment that it did not infringe a particular TRA patent. TRA counterclaimed for infringement of that patent and two others, plus misappropriation of trade secrets, breach of contract, and breach of fiduciary duty. After extensive discovery, TRA moved for summary judgment. Judge Scheidlin granted the motion in substantial part. She (a) held that TRA did not infringe Kantar's patents, (b) dismissed TRA's misappropriation claim as a discovery sanction, (c) ruled that TRA's allegedly confidential information did not constitute trade secrets, (d) held that TRA submitted insufficient evidence to support a claim for damages, and (e) denied TRA's requests for injunctive relief relating to allegations of a breach of fiduciary duty and for a jury trial on compensatory damages. According to the appeals tribunal, many of these rulings were erroneous.

Background

Before they were competitors, Kantar was a substantial investor in TRA, a seemingly valuable corporation at the time. As a result of its investment, Kantar was given a seat on TRA's Board and considered merging with TRA. Kantar allegedly was given access to TRA's trade secrets both as a Board member and in the course of the companies' merger negotiations, ultimately abandoned. After Kantar purchased and began operating a competing analytics company, TRA's fortunes dwindled, and it was sold for a fraction of its former value. The purchaser continued to operate the acquired company under the TRA name.

The ruling below regarding TRA's trade secret claims

Absence of trade secrets. In its counterclaim, TRA alleged that Kantar misused TRA's confidential information. After originally asserting more than 20 categories of trade secrets, on the eve of summary

judgment briefing TRA reduced the number to five including characteristics of its products and its strategic plans.

Judge Scheidlin found that TRA had disclosed publicly most of the properties of its products. Further, she ruled that there was no evidence that Kantar's products used any of TRA's technical information. Regarding TRA's strategic plans, she concluded that these were merely goals which are not protectable trade secrets under New York law. Judge Scheidlin added that "TRA's trade secret claims had no colorable basis and were brought in bad faith." Thus, she granted summary judgment as to misappropriation. She did not consider whether TRA's customer contract terms, proposals and pricing were protectable.

Dismissal as a sanction. Kantar alleged that TRA had failed during discovery to identify trade secrets with sufficient specificity. The district court agreed. It held that dismissal of the misappropriation claims was warranted as a sanction because TRA's violation of Federal Civil Procedure Rule 26(e) (requiring timely supplementation or correction of disclosures and responses) was "manifestly prejudicial to [Kantar] and taxing on the Court."

Rulings on appeal by the Federal Circuit

Grant of summary judgment. TRA had a proprietary product called Media TRAnalytics. The company claimed that the product's speed, reliability, scalability and performance were trade secrets. The Federal Circuit concluded that the information concerning Media TRAnalytics that was publicly disclosed was merely an overview. In addition, the court held that the question of whether Kantar improperly used TRA's confidential product information to gain a competitive advantage requires a determination by a fact finder rather than a summary disposition. Further, proprietary financial projections and strategic plans may be protectable if "not publicly known, not readily identifiable, or otherwise complex."

In the Federal Circuit's view, customer contract terms, proposals and pricing can be trade secrets. The district court was held to have committed reversible error by granting summary judgment regarding misappropriation without considering whether TRA's customer information warranted protection. Similarly, "TRA presented sufficient evidence to create a colorable question about Kantar's intent to injure TRA," and so TRA was entitled to a trial on the subject of its entitlement to punitive damages.

Dismissal of trade secrets claims as a sanction. The Federal Circuit said that dismissal as punishment was not warranted here: "[T]here is no indication that TRA purposefully shirked its discovery obligations." Further, TRA was not given a warning, and the lower court's finding of prejudice to Kantar was unexplained. On remand, the district court was directed to consider a less harsh sanction.

Takeaways

The Federal Circuit's order teaches that proprietary financial projections, strategic plans, and customer contract terms, proposals and pricing, all may be trade secrets. Further, a mere overview, or only partial disclosure, of a product's confidential characteristics does not defeat trade secret protection for the undisclosed portion. In addition, whether a party's protected information was used by another to gain a competitive advantage is a question to be decided by the fact finder.

Getting Your Money Back: New Jersey Employers Can Disgorge A Disloyal Employee's Salary

By Christopher Lowe and Robert T. Szyba (October 1, 2015)

In a recent ruling, the New Jersey Supreme Court gave employers a great recourse for dealing with former employees who breach their duty of loyalty. In *Bruce Kaye v. Alan P. Rosefielde*, the Court allowed an employer to recover compensation paid to a disloyal, recently terminated, employee, even where the employer sustained no economic hardship from the employee's acts of disloyalty.

Background

In *Kaye*, the employee, an attorney, who was only licensed to practice in New York, was hired as Chief Operating Officer ("COO") and General Counsel for plaintiff's business selling and managing timeshares in Atlantic County, New Jersey. Interestingly, although the defendant's contract refers to his salary as a retainer for his services, and it appeared that both parties intended defendant to be an independent contractor, both parties agreed that defendant performed the services of an employee rather than an independent contractor.

While employed in the hybrid COO/General Counsel role — earning a salary of $500,000 per year — the Court found that the employee committed a number of "egregious" acts that ultimately resulted in the termination of his employment, including: (1) expensing a $4,000 personal trip to Las Vegas, the cost of which included a hotel suite with three "adult film stars"; (2) fraudulently applying for health insurance; (3) forging signatures on false quitclaim deeds of defaulting timeshare owners; (4) carved out a greater-than-agreed-upon personal interest in one of his employer's corporate entities; (5) creating an entity under his employer's name, without his employer's consent, taking a 20% interest in that entity for himself (the employee); and (6) making numerous sexual advances towards other employees. When the employer learned what was going on, he fired the employee and sued him for breach of fiduciary duty, fraud, legal malpractice, unlicensed practice of law, and breach of duty of loyalty.

The Trial and Appellate Courts

After a 26-day bench trial, the trial court found that the former employee breached his duty of loyalty to the employer, and committed legal malpractice and fraud. The employer was awarded $4,000 for the Las Vegas trip, over $800,000 in counsel fees and costs, and rescission of all of the employee's ill-gotten interests in the employer's other companies. But despite it being "difficult to imagine more egregious conduct by a corporate officer," the trial court declined to order equitable disgorgement for the former employee's compensation during the period of disloyalty. The trial court interpreted a prior Supreme Court decision, *Cameco, Inc. v. Gedicke*, as holding that "in order to compel disgorgement of a disloyal employee's compensation, a court must first find that 'the employee's breach proximately caused the requested damages.'" The Appellate Division agreed with the trial court on that point and affirmed that the employer could not disgorge the compensation paid to the disloyal former employee because it could prove no actual harm.

The New Jersey Supreme Court granted certification only to address the specific question of "whether a court may remedy disgorgement of a disloyal employee's salary to an employer that has sustained no economic damages."

The Court reversed the courts below, holding that disgorgement is an equitable remedy within the trial court's authority, including where a disloyal former employee's misconduct is not tied to an economic loss suffered by the employer on account of the employee's disloyalty. The Court directed lower courts to consider four factors to determine whether an employee breaches his/her duty of loyalty:

(1) the existence of contractual provisions relevant to the employee's actions;

(2) the employer's knowledge of, or agreement to, the employee's actions;

(3) the status of the employee and his/her relationship to the employer (for example, corporate officer or director versus production line worker); and

(4) the nature of the employee's conduct and its effect on the employer.

In effect, courts are directed to consider "the parties' expectations of the services that the employee will perform in return for his or her compensation, as well as the 'egregiousness' of the misconduct that leads to the claim."

The Court further clarified that once the employee is found to have breached the duty of loyalty, courts should decide whether disgorgement is a proper remedy by considering: "[t]he employee's degree of responsibility and level of compensation, the number of acts of disloyalty, the extent to which those acts placed the employer's business in jeopardy," "the degree of planning to undermine the employer that is undertaken by the employee," as well as "other factors" that may be relevant. And once disgorgement is found to be appropriate, the court suggested apportionment commensurate to misconduct at issue, as opposed to "wholesale disgorgement."

Outlook for Employers

New Jersey employers scored a significant win and a meaningful tool to deter and redress a breach of an employee's duty of loyalty. The *Kaye* Court addressed the circumstance of a disloyal employee who's employment was terminated, however the analysis is certainly instructive in addressing situations with current employees. The ability to recoup some or all of a disloyal employee's salary/compensation is certainly a powerful tool in the right circumstances, and certainly something to consider when faced with a breach of the duty of loyalty.

Trading Secrets

Webinar Recap! So You Want An Injunction in a Non-Compete or Trade Secret Case?

By Justin K. Beyer, Eric Barton, and Bob Stevens (October 2, 2015)

We are pleased to announce the webinar "So You Want An Injunction in a Non-Compete or Trade Secret Case? " is now available as a podcast and webinar recording.

In Seyfarth's seventh installment in its series of 2015 Trade Secret Webinars, attorneys Justin K. Beyer, Eric Barton and Robert C. Stevens focused on the issues confronting plaintiffs in preparing for and prosecuting trade secret cases and the various ins and outs of seeking both temporary restraining orders and preliminary injunctions.

- 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

Daily Trade Secret Theft for Daily Fantasy Sports?

By Marcus Mintz (October 7, 2015)

While season-long fantasy sports leagues have long been in existence, the emergence of daily fantasy sports ("DFS") has been relatively recent. DFS allows participants to enter daily contests for money where a salary cap is used to "draft" a team and compete against anywhere from one to hundreds of thousands of other participants. Points are allocated based on each player's respective performance (e.g., receiving yards, touchdowns, etc.) and winners receive cash payouts that can be in the millions.

If the ever-present commercials did not make you aware already, DFS is big business. Reports indicate that the industry collected approximately $2.6 billion in entry fees this year and may reach as much as $2 billion in revenues by 2020.

On October 5, 2015, the nascent industry was rocked when the New York Times reported that an employee of Draft Kings, the current market leader, used proprietary information regarding player usage in Draft Kings' contests to win $350,000 in a contest hosted by competitor Fan Duel. The industry, and Draft Kings in particular, have since come under a flood of criticism for a lack of internal controls and running a rigged game.

The information that was allegedly misused by the Draft Kings employee is player usage data — the percentages that particular players are "drafted" by contest participants. This information is neither public nor available by any lawful means until changes to a participant's line-up are "locked" and cannot be changed. By having this information prior to being "locked" in, a DFS participant would get an unfair advantage by being able to calculate a line-up around the players that are owned by existing participants and thus may have a statistically higher change of winning certain large-format contests where a unique line-up makes the chances of winning much greater.

Prior to the incident becoming public, no ban was in place prohibiting employees from playing on other sites; they were only prohibited from playing in contests hosted by their employers. The amount of money at stake, however, raises significant questions about how DFS trade secrets may be misappropriated and misused. Risks include not only employees misusing insider information regarding player usage to compete in competitor's games, but also leaks to an insider's friends and family or an employee unfairly competing through an account set-up under an alias.

This scandal evidences the need for public-facing companies in particular to make sure that adequate measures are taken to safe guard company trade secrets and confidential information. Draft Kings in particular has come under criticism for a lack of internal controls and safeguards to prevent the unauthorized access and use of its non-public information. If sufficient safe guards are put into place, the threat of a trade secret claim against an employee or other user of player usage data may be used as another tool to prevent unfair competition and a corresponding loss in public confidence. Trade secret protection, however, is only available to those who establish sufficient safe guards to keep the information confidential in the first place.

Trading Secrets

While industry leaders Draft Kings and Fan Duel announced the retention of a third-party auditor to investigate their internal controls, only time will tell if the industry can regain the trust lost by this week's news.

Dueling Dumpling Trade Secret Dispute Heads to District Court

By Dawn Mertineit (October 14, 2015)

For Dumpling Daughter and its newly opened rival Dumpling Girl, things are heating up in the kitchen *and* the courtroom, as reported by the Boston Globe, after the former filed a lawsuit in federal court in Boston asserting a host of claims against Dumpling Girl and its three owners, including misappropriation of trade secrets, unfair competition, trademark infringement, conversion, and unjust enrichment.

Dumpling Daughter claims that the individual defendants, two of whom are former Dumpling Daughter employees, opened a virtually identical restaurant using Dumpling Daughter's confidential and proprietary recipes, a nearly indistinguishable menu, and "ordering, check-out, food preparation, and food delivery operations" that are likewise identical to Dumpling Daughter's. The complaint alleges that Dumpling Girl's actions have already confused several Dumpling Daughter clients, who have asked the latter's owner if she is opening a new restaurant where Dumpling Girl is currently located (and in fact, the complaint attaches documentary evidence of such queries from customers).

The verified complaint also attaches the aforementioned menus which bear more than a mere resemblance — in fact, Dumpling Girl's menu is a near duplicate of Dumpling Daughter's menu. By way of example, the description for the restaurants' respective pork ramen dishes are nearly verbatim. Dumpling Daughter's description reads:

NOT the instant kind!!!!!!!! Classic pork broth, fresh ramen noodles, pork belly, soft egg, bamboo red pickled ginger, kombu seaweed, scallions.

In contrast, Dumpling Girl's pork ramen dish is described as follows:

NOT the instant kind!!!!!!!! Classic pork broth, fresh ramen noodles, pork belly, soft egg, bamboo red pickled ginger kombu seaweed, scallions.

The *only* changes in Dumpling Girl's description are one fewer exclamation point and a missing comma. Nearly every other menu item is similarly alike. With these striking similarities (which, when taken cumulatively, no reasonable person could claim are mere coincidences), it seems like Dumpling Girl will have an uphill battle proving to the that its restaurant is not merely a carbon copy of Dumpling Daughter. Further compounding Dumpling Girl's plight are alleged admissions by its employees that the purpose of the restaurant is to copy Dumpling Daughter's concept, and their alleged attempts to hire Dumpling Daughter's vendor to manufacture dumplings and buns using Dumpling Daughter's exact recipes.

Of course, to prevail on its misappropriation claim, Dumpling Daughter will have to prove to the court that its recipes are trade secrets; while we frequently see client lists and highly technical inventions as the alleged trade secrets in misappropriation cases, there's no reason why recipes can't be trade

secrets under the right circumstances. In fact, an oft-cited Massachusetts case, *Peggy Lawton Kitchens, Inc. v. Hogan*, 18 Mass. App. Ct. 937 (1984), held that a chocolate chip cookie recipe constituted a trade secret. Accordingly, Magistrate Judge Donald Cabell will likely consider the following six-factor test utilized by Massachusetts courts in determining whether Dumpling Daughter's recipes are trade secrets:

1. The extent to which the information is known outside of the business;
2. The extent to which the information is known by employees and others involved in the business;
3. The extent of Dumpling Daughter's measures to guard the information's secrecy;
4. The information's value to Dumpling Daughter and its competitors;
5. The amount of effort or money Dumpling Daughter spent to develop the information; and
6. The ease or difficulty for others to properly acquire or duplicate the information.

Given the complaint's many allegations regarding the secrecy with which Dumpling Daughter protected the restaurant's recipes and the time and expense its owner devoted to their development, the court very well may determine that the recipes are indeed trade secrets, assuming discovery supports these allegations.

Thus far, Dumpling Girl has not responded to the suit, and it remains to be seen whether it will get its just desserts. Stay tuned for the outcome of this delicious dispute.

Trading Secrets

Utah Supreme Court Lays Out Pro-Plaintiff Presumption of Harm Standard in Trade Secret Cases

By Robert B. Milligan and Amy Abeloff (October 14, 2015)

The Utah Supreme Court recently issued a significant decision laying out a presumption of harm evidentiary standard in trade secret cases, which will be very useful for plaintiffs seeking injunctive relief in cases involving trade secret and breach of non-disclosure claims. *InnoSys v. Mercer*, 2015 UT 80 (August 28, 2015).

The trade secret battle involved a defense industry-focused technology company, InnoSys, Inc., and its former engineer, Amanda Mercer.

InnoSys alleged that Mercer violated a non-disclosure agreement she signed at the time of hire, which memorialized her promise not to copy or transmit any company-protected information. InnoSys further alleged that Mercer engaged in misappropriation of trade secrets when she sent company information and a confidential company business plan to her personal email account and downloaded it onto a personal thumb drive and used the information in an administrative unemployment hearing following her dismissal from InnoSys.

In district court, Mercer prevailed on her motion for summary judgment based on the determination that InnoSys had not met its burden of showing that Mercer's acts amounted to actual, irreparable harm. As a result, InnoSys was slapped with sanctions under Federal Rule 11 and Mercer recovered her attorney's fees under Utah state law.

The Utah Supreme Court reversed the district court in a 3-2 decision, asserting that "Mercer's disclosures [of InnoSys' confidential information] at least arguably sustain[ed] a presumption of harm to InnoSys."

First, the Court reasoned that InnoSys "at least arguably" asserted a prima facie case of misappropriation of trade secrets under the Utah Uniform Trade Secret Act (UTSA). Under the UTSA, a prima facie case of misappropriation is established on the basis of two elements: 1) existence of a protectable trade secret by a plaintiff; and 2) demonstration of misappropriation by a defendant. Utah Code § 13-24-2. The Court found that the business plan and other confidential information indisputably were trade secrets because they derived independent economic value from not being generally known by others. In determining whether Mercer was entitled to judgment as a matter of law on this issue, the Court reasoned that InnoSys arguably made a prima facie showing of infringement under the UTSA and under its claim of breach of the non-disclosure agreement, which showing sustained a presumption of irreparable harm.

Second, the Court noted undisputed evidence of misappropriation on the summary judgment record, which included proof of unlawful disclosure and unlawful acquisition. Only a showing of one is necessary under the UTSA. *Id.* § 13-24-2(2)(a), (b). Mercer's transmission of company information from the company system to a personal email account and thumb drive coupled with her subsequent use of that information in an administrative proceeding "at least arguably amount[ed] to misappropriation"

under the UTSA, the Court concluded. Moreover, the UTSA provides no basis for a defense to the unauthorized disclosure of a trade secret, no matter the circumstances. Therefore, Mercer had no reasonable basis grounded in the UTSA to disclose company information in the way she did to the administrative body during her proceeding; such a lack of a defense further supported InnoSys' prima facie showing.

The Court reasoned that InnoSys was able to withstand Mercer's motion for summary judgment because its prima facie showing gave rise to a rebuttable presumption of irreparable harm, to which Mercer provided no rebuttal. The court further discussed the presumption of irreparable harm upon the showing of misappropriation, noting that trade secrets, as property rights, are protected by such a legal presumption. Any trespass on such a right is subject to injunctive relief to "vindicate that right and prevent future harm." The Court emphasized that such a presumption is "rarely questioned," and exists as strong precedent in trade secret law.

The Court later analyzed how Mercer failed to rebut the presumption of irreparable harm. The Court considered the possibility, given expert testimony supporting such a hypothesis, that Mercer kept other copies of the confidential information elsewhere, despite deleting some documents in the presence of her sister and attorney. If she did not harbor such information, injury to her upon the issuance of an injunction would harm her little; if she did harbor the information with the intention to further harm InnoSys, then the injunction would be priceless for InnoSys. In other words, issuing an injunction in favor of InnoSys at the very least would protect it from any fathomable future disclosure by Mercer, with little harm to her.

Even without the presumption, the Court stated that InnoSys provided actual evidence of threatened harm, which would allow its claim to survive summary judgment. This actual evidence included a showing of Mercer's use of a web-based personal email account to access InnoSys' trade secrets. Transmission of protected company information to an email server not bound to any confidentiality agreement nor capable of ever actually deleting a message, InnoSys argued, amounted to an ongoing threat of harmful disclosure. Further, the Court noted that Mercer could go and re-access her administrative hearing file, which contained the trade secret information at issue. Moreover, Mercer's recurring inconsistent statements made throughout the history of the case undermined her credibility and introduced a "core genuine issue as to her supposed intent to reform and never again harm InnoSys."

Regarding the breach of the non-disclosure agreement claim, the presumption of irreparable harm in and of itself, the Court noted, was enough to sustain InnoSys' prima facie case. The court reversed the summary judgment on the breach of fiduciary duty claim and attorney's fees as well for the reasons outlined above, and others. In sum, the Court held that because Mercer made no attempt to rebut the presumption of irreparable harm to InnoSys, the district court's grant of summary judgment, Rule 11 sanctions, and attorney's fees was improper.

The majority opinion, authored by Associate Chief Justice Lee ("ACJ Lee"), acknowledged the dissent's arguments several times throughout the opinion. Perhaps most interestingly, the dissent asserted that Mercer was entitled to summary judgment because InnoSys failed to show an actual threat of future harm by Mercer. ACJ Lee directly addressed this argument, noting that it fell short on two grounds: 1) the issue it raised was not preserved; and 2) Mercer's deletion of emails failed to rebut the presumption of irreparable harm. Regarding the former, ACJ Lee noted that Mercer's entire argument was that InnoSys never produced evidence of actual or threatened harm; meaning, InnoSys never showed the economic impact following Mercer's disclosures. Such failure to produce was not enough to affirm a summary judgment ruling, in the majority's opinion. As to the latter issue, the ACJ recalled that a defendant's claiming her voluntary compliance moots a case bears "a formidable burden of showing that it is absolutely clear the allegedly wrongful behavior could not be reasonably expected to occur."

The dissent argued that the fact that Mercer deleted all of the confidential information from her email was undisputed and that InnoSys failed to produce evidence that she would be a future threat of harm, but the majority disagreed because it assumed facts not made of record and gave the benefit of the doubt to the wrong party, the movant. The majority continued that Mercer failed to meet the aforementioned formidable burden because her acts of deletion could be construed as self-serving and not enough to defeat summary judgment.

Takeaways

This case provides a significant evidentiary tool to plaintiffs who have evidence of illicit data transfer despite claims by the defendant that the data has subsequently been deleted and/or that there has been no harm to the plaintiff. Additionally, the case underscores the importance for trade secret victims to conduct thorough computer forensic investigations to uncover evidence of data misuse to support their claims.

Poor Employer Onboarding and Departure Procedures Can Lead to Horrifying Results Including the Loss of Trade Secrets

By Robert B. Milligan and Daniel Joshua Salinas (October 30, 2015)

This upcoming Halloween reminds us that employers face their own terrors in trying to protect trade secrets and other valuable company information in the workplace, particularly if they have poor onboarding and departure protocols with their employees.

The following video illustrates some of the bad practices committed by both company personnel and employees that can "trick" companies into losing trade secrets or other confidential information or expose them to other liability.

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

Our recent Halloween-themed best practices presentation provides several "treats" for companies as it highlights some of the practical strategies to avoid the potential horrors illustrated in the video above. These best practices include:

- Creating a culture where employees understand confidentiality and what information the company considers confidential
- Making it clear to employees that they should not use or bring any former employer's confidential information

Trading Secrets

- Emphasizing the importance of the company's non-disclosure and trade secret protection agreements
- Considering the implementation of computer, network, and social media use and access agreements and policies
- Conducting exit interviews and ensuring all company property (both hard copy and electronic) is returned when employees depart
- Training modules with examples of "dos" and "don'ts"
- MARK THINGS CONFIDENTIAL!!!
- Provide access on need to know basis
- Make security protocol familiar and uniform

Have a safe and happy Halloween!

Protecting Intellectual Property Throughout Its Lifecycle

By Guest Author for TradeSecretsLaw.com (November 5, 2015)

As a special feature of our blog—special guest postings by experts, clients, and other professionals—please enjoy this blog entry from Stroz Friedberg, a global leader of cybersecurity, investigations and risk management. The firm recently launched Strategic Intellectual Property Protection Services (SIPPS), an offering Stroz Friedberg designed to help companies best handle intellectual property throughout its lifecycle.

Across industries ranging from pharma to entertainment to electronics, the success of an organization is often directly tied to its intellectual property. However, many companies don't effectively determine whether their products or internally developed solutions constitute protected intellectual property until there is a need for enforcement action.

It's better (and easier) for a company to identify its intellectual property and trade secrets at the outset than it is for a company to retrofit its intellectual property and trade secrets to a bad event. Waiting until intellectual property is misappropriated delays enforcement, and is generally less successful overall than defining intellectual property early on. After identification, it is also important for an organization continually to evaluate how it safeguards its intellectual property. If a company proactively identifies and protects its trade secrets, enforcement efforts, if necessary, will prove much easier—even more so when a detailed response plan is already in place.

Stroz Friedberg has been called upon to help clients at distinct points in the IP lifecycle, and helps its clients and counsel think strategically and mitigate risks such as insiders, hackers and even simple negligence. This posting is designed to give the reader a quick overview of Strategic Intellectual Property Protection Services—from identification, to prevention, to enforcement. SIPPS is a complete misappropriation readiness solution.

Identification

If you are a regular reader of this blog, you know that a company's intellectual property is vulnerable while it is still being developed: "The idea must be kept secret in order to enjoy the later protection," writes Bartosz Sujecki in a previous *Trading Secrets* post about proposed new trade secrets in Europe,http://www.tradesecretslaw.com/2014/12/articles/trade-secrets/new-rules-on-trade-secrets-in-the-eu-the-european-commission-proposal-on-the-protection-of-know-how-in-the-eu. The relatively unstructured way in which some ideas come to life does not obviate the need to take reasonable steps proactively to identify and protect trade secrets. See, e.g., http://www.tradesecretslaw.com/2015/07/articles/trade-secrets/trade-secret-protection-what-are-

reasonable-steps/. Without early and robust identification, trade secret enforcement down the road often proves far more difficult.

Understanding early on the way in which the law protects intellectual property is not always an easy task. The identification process should not be kept so secret that outside experts are not called in to help. Leveraging outside experts at the early stages—with the same physical and technical controls in place that safeguard early development intellectual property from insider and outsider threats alike—will best position the company to evaluate whether secrets should remain confidential, be prosecuted as patents, or otherwise be afforded special protection. Meanwhile, critical development employees are left to focus on the creative production and refinement of the intellectual property itself.

When an organization can identify its trade secrets early, the organization will be better prepared to safeguard those secrets. Such early identification of trade secrets helps ensure that the company is taking reasonable steps to protect its intellectual property, which in turn demonstrates the history of diligence necessary to successfully pursue legal remedies down the road.

Protection

After the arduous process an organization undergoes to define its intellectual property, it needs to apply the same diligence and focus to protecting it. Protecting intellectual property involves a combination of people, process, and technology. How is it segregated within the company's environment? Who has access to it? How are permissions and access controlled? What technologies exist within the environment to monitor unauthorized access? How well do the organization's existing policies and procedures protect it?

This may also be the ideal time for a security risk assessment to ensure that no physical or technical vulnerabilities exist at the end user or enterprise level that would make data exfiltration possible. No one wants to see a competing product come to market two weeks after theirs—but it does happen.

Enforcement

Having a well-developed enforcement plan of action around identified and protected intellectual property *before* a misappropriation event occurs makes all the difference in the world. Seeking inchoate relief to immediately block a perpetrator from misusing valuable intellectual property involves stringent timing and other requirements. Organizations that have invested time and energy in working with experts to tailor a readiness position are better equipped to meet those requirements—especially when necessary business stakeholders, outside counsel, forensic experts, and even source code specialists are lined up and at the ready to react, engage, and pursue relief.

Assistance with Trade Secret Strategy throughout the IP Lifecycle

Intellectual property is always vulnerable to some degree, but the more proactive a company is, the better it can harness the value of its assets. With a thorough understanding of your intellectual property—where it is located, how it is protected both legally and digitally, and how you will respond in the event of theft—you will be best positioned for whatever challenges come your way. Leverage outside expertise throughout the process, and use the same experts who are familiar with your intellectual property lifecycle to help enforce your rights.

As experts who have helped organizations deal with the aftermath of data breaches and computer crimes, we have witnessed firsthand how crucial it is to be prepared—but even in the aftermath of a breach or theft, we focus on more than just dealing with the aftermath, and work on developing new

solutions that could be used to help organizations in the future. For example, while helping a video game engine developer win a trade secret case (see:https://www.elys.com/case-studies/an-epic-battle-of-game-giants), we wrote proprietary software tools that could compare source code versions across repositories. We have developed a range of other preventative services, including Payment Card Industry assessment, data analytics and transaction monitoring, privacy audits, and incident response plans, to name a few. We know what makes a trade secret or other piece of intellectual property unique, and we can help you come up with a unique plan to protect it.

Trading Secrets

“Reasonable Suspicion” of Trade Secret Misappropriation Isn’t Always Enough

By Lauren M. Gregory (November 6, 2015)

Though an employer may be eager to bring a trade secret claim against former employees as soon as possible, filing suit before properly vetting the claim can lead to serious consequences: a malicious prosecution case against the lawyers who signed the pleadings.

A law firm is fighting such allegations in California after losing at bench trial on behalf of FLIR Systems, Inc. and Indigo Systems Corporation (collectively, “FLIR”), who brought suit against a group of former employees attempting to launch a competing business. Though the California Court of Appeal for the Second District affirmed a lower court’s ruling that the employee’s malicious prosecution suit could not proceed, *Parrish v. Latham & Watkins*, 238 Cal.App.4th 81 (2015), the California Supreme Court recently announced it will reconsider that decision.

The Underlying Dispute

FLIR developed and sold microbolometers, devices used to detect infrared radiation for infrared cameras, night vision, and thermal imaging. In 2004, while still working for FLIR, the group of employees presented FLIR with a business plan to outsource microbolometer manufacture. When the group left to form another business in 2006, FLIR believed their plan to launch a new business had to have incorporated intellectual property owned by FLIR.

The former employees had several meetings with FLIR to ensure the company that they had no intention of using its intellectual property. The business plan they were using had been created by one of the individuals prior to joining the company and involved licensing the necessary intellectual property from a third party.

FLIR was nonetheless convinced that the new business plan “necessarily presume[d]” use of its trade secrets and filed suit. In support of its position, FLIR presented two brief expert declarations stating that the experts were unaware of any third parties in the infrared market other than FLIR with the requisite intellectual property, and concluded that this meant FLIR’s ex-employees “could not pursue” their business plan without the use of FLIR’s trade secrets.

The trial court denied the employees’ motion for summary judgment, finding that although they “made a compelling argument” that they were entitled to summary judgment, the concepts involved in the litigation were “highly technical” and merited further review. However, the same judge who had denied summary judgment ruled in the employees’ favor after a bench trial, not only denying FLIR any relief but also finding that FLIR had brought and pursued the action in bad faith and should pay more than $1.6 million in attorney fees.

Trial Court Finds Bad Faith

The court pointed to the fact that California law does not recognize the "inevitable disclosure" theory, which permits a trade secret owner to prevent a former employee from working for a competitor despite the owner's failure to prove the employee has taken or threatens to use trade secrets, as long as it can be demonstrated that the employee's new job duties will inevitably cause the employee to rely upon knowledge of the former employer's trade secrets. While FLIR's former employees had raised a "reasonable suspicion that they might misuse [FLIR's] trade secrets," the court concluded that "reasonable suspicion" is not an adequate basis for relief under the Uniform Trade Secrets Act.

The court noted that its earlier denial of the employees' summary judgment motion did not preclude it from ruling that the action had been brought in bad faith, an issue that was not pertinent at that stage, as the court had not yet heard all the evidence or considered witness credibility. After the bench trial, it became clear to the court that FLIR had been "unwilling to take the risk that [the former employees] might be able successfully to complete without misuse of [FLIR's] trade secrets." The court made several findings consistent with objective and subjective bad faith, including that FLIR:

- "unreasonably discounted ways in which [the former employees] could have proceeded with their new company lawfully;"
- "downplayed" the former employees' plans to license technology from a third party and to make sales to that third party; and
- "failed to take reasonable measures to ally [its] fears by learning more about [the former employees'] plans."

In fact, three of FLIR's witnesses testified at trial that they did not know at the time the lawsuit was filed that the former employees planned to work with a third-party company, and that, "had they known such facts, their concerns regarding [the former employees] would have been allayed."

Malicious Prosecution Case Pending

The trial court's award was affirmed on appeal, and the employees brought an action against FLIR's law firm for malicious prosecution. They asserted that the firm pursued the action even though they knew the legal basis for their theory, inevitable disclosure, was discredited in California, and even though they knew that FLIR had an anti-competitive purpose in suing them.

The California Court of Appeal has held that the malicious prosecution claim is barred by the "interim adverse judgment rule," which holds that the denial of a dispositive motion on the merits in an underlying action precludes the maintenance of a subsequent malicious prosecution action. In other words, because the trial court had denied the former employees' motion for summary judgment before granting judgment in their favor, there was probable cause for the underlying trade secret suit, and thus no basis for malicious prosecution.

However, the California Supreme Court's decision to rehear the case means the firm is not yet off the hook. Hopefully, whatever the outcome, the Supreme Court's opinion will provide guidance for trade secret litigators trying to zealously advocate for their client without putting both the client and themselves at risk.

Perspectives From the Bench: A Recap of the AIPLA Trade Secret Law Summit's Judicial Panel

By Erik Weibust and Dawn Mertineit (November 13, 2015)

Several members of Seyfarth's Trade Secrets, Computer Fraud & Non-Competes Practice Group attended the AIPLA's annual Trade Secret Law Summit on November 12-13, 2015. Rick Lutkus spoke on a panel that was moderated by Erik Weibust entitled "The Ethics of Data Security and Trade Secret Protection for Lawyers," which we will post about separately.

Another session, entitled "Perspectives From The Bench: How State and Federal Judges View the Growth and Scope of Trade Secret and Restrictive Covenant Disputes," featured an impressive panel of the Honorable Mitchell H. Kaplan and the Honorable Janet L. Sanders, both of whom sit in the Business Litigation Session of the Suffolk Superior Court, and the Honorable F. Dennis Saylor, IV, a district court judge for the U.S. District Court for the District of Massachusetts. These judges provided some very valuable insights with respect to seeking injunctive relief in a trade secret and/or restrictive covenant case.

Here are some key takeaways from the panel:

- **Equitable factors matter.** All three judges agreed that notwithstanding the terms of an employment agreement, they are far more sympathetic to young or low-level employees who might be prevented from earning a living due to the enforcement of a non-compete agreement, as opposed to a CEO or other high level executive, particularly where he or she was paid a handsome severance package. Indeed, the panel agreed that the language of the agreement is "just the beginning" of the analysis, and that they will certainly consider other equitable factors such as this.

- **Ex parte motions are disfavored**. The panel consistently agreed that they only grant ex parte orders sparingly, and instead will typically issue a short order of notice to allow defendants some time to respond to plaintiffs' allegations. Judge Sanders further noted that she is typically not swayed by plaintiffs' counsel's outraged protestations that they have not had an opportunity to review defendant's opposition papers when the plaintiff has demanded an expedited hearing. In other words, the plaintiff made its bed and now has to sleep in it.

- **Forensic discovery should not be a battleground.** Judge Saylor noted that it is relatively easy for forensic experts to make mirror images of parties' electronic devices, and accordingly he is generally receptive to requests to conduct forensic discovery to determine whether and to what extent confidential information or trade secrets has been misappropriated and/or misused. He further noted that parties should not object to a neutral third party forensic expert, which should allay concerns that competitors will be rooting around in the company's "crown jewels." Finally, he warned that to the extent employees put company documents on personal devices, they cannot then complain about the prospect of a forensic expert accessing those personal devices .On this same topic, Judge Sanders explained that parties should do their

best to work cooperatively on forensic discovery, given that judges are frequently not as savvy regarding the technological details of forensic discovery. That said, she did suggest that the party seeking forensic discovery should not seek broad forensic searches on a competitor's entire network (which she deemed a "red flag" that the moving party is being unreasonable); instead, absent extreme circumstances, forensic discovery should be limited to the departing employees' relevant devices.

- **The parties' pre-litigation conduct matters.** Judge Kaplan explained that the parties' behavior leading up to litigation can be incredibly persuasive. Obviously, "bad actors" will suffer grave consequences, and conversely, an employee who takes steps to ensure that his or her departure goes smoothly with sensitive materials promptly returned to the employer will have a much easier time convincing the court that an injunction is unnecessary. Judge Sanders concurred, noting that she is more sympathetic to employees who are terminated without cause, although she admitted that her thinking may shift if the employer attempted to "do right" by the terminated employee by providing severance. Judge Saylor agreed that an employee who ignores inquiries by her former employer regarding whether she retained trade secrets will have a much more difficult time arguing to the court that she didn't know that she had done anything wrong. Judge Kaplan concurred, contrasting that scenario by noting that a party who responds to a cease and desist letter representing that it will abide by contractual, common law, or statutory obligations to the extent reasonable will go a long way in convincing the court that an injunction is unnecessary. Both Judge Saylor and Judge Kaplan agreed that while pre-litigation correspondence between the parties can at times be useful, angry emails between attorneys that are clearly written for purposes of motions for injunctive relief are rarely compelling to the court.

- **Make life easy for your judge.** In addition to cooperating with the opposing counsel on such matters as timing and scope of discovery, the panel stressed how useful it is for the parties (whether jointly or separately) to bring a reasonable, clear proposed order that the judge can simply sign, without significant (or any) edits. This is particularly useful in cases where the judge may not have the same depth of understanding as the parties on highly technical terms.

- **Be wary of over-redacting.** The panel discussed motions to impound or seal materials that parties deem confidential. The panel's consensus was that many litigants over-designate materials as confidential, and stressed that attorneys should discuss with clients how to limit redacted or sealed pleadings, notwithstanding that it is frequently a difficult conversation. The judges emphasized that litigation happens in the public forum, and parties should take pains to limit their redactions to what is truly necessary to protect confidential information and trade secrets.

- **Finally – Be reasonable!** While this should be obvious, it bears noting that *all* judges stressed the need to be reasonable in requests for injunctive relief (as well as in oppositions). Judge Saylor specifically noted that while judges oftentimes want to find a middle ground, judges tend to migrate towards the party that is being more reasonable. Pressing for the most draconian measures — or conversely, refusing to agree to "no-brainers" such as refraining from using obviously misappropriated information — is unreasonable and could backfire.

Of course, given the fact-intensive nature of non-compete and trade secret cases, and the broad latitude that judges are given to issue equitable relief, the facts of the case, the relief being requested, the economy, and even the proclivities of the judge can make or break a case. Nevertheless the advice above should be considered in each case.

Untrusted Advisor: How Your Law Firm May Fail to Protect Your Data

By Richard Lutkus (December 4, 2015)

In recent years, the prevalence of data and information security breaches at major corporations have become increasingly more commonplace. While general awareness may be increasing, many companies are still neglecting to address serious information security issues.

Breached data can include proprietary or confidential information, trade secrets, personally identifiable information, health-related data, privileged communications, and regulatory data. Such data is often subject to preservation due to pending or reasonably anticipated litigation, government investigation, due diligence, or other applicable legal matter, meaning the data is routinely transferred and shared with outside counsel for analysis and support of clients' claims and defenses.

Many law firms provide guidance regarding information governance to clients, however more times than not, firms fail to realize that they too are also responsible for following similar guidelines. Appropriate precautions must be in place throughout a firm to protect the integrity and sanctity of client data, prevent unauthorized access, and to ensure timely remediation. However, firms must also have this data available for litigation response, analysis, and review. Therefore, keeping data entirely offline is rarely an option.

There are several pillars of governance that law firms should consider when examining the handling of both their own data as well as that of clients. As a fiduciary of their clients' data, firms that fail to address these issues will eventually find themselves in an ethical nightmare, that when applied to a partnership creates a considerable problem.

Information Storage, Retention, and Remediation

Organizations must work to ensure that data is protected from physical threats including loss of power, environmental disasters, hardware failures, and theft. Thus, careful planning and selection of datacenter features and location is paramount; some qualities of preferable datacenters include geographically diverse co-location, failover systems, backups of key data, backup power sources, cloud usage, and encryption at rest and in transit.

Various options for hosting data exist, however due to the prevalence of unreliable datacenters, clients are now requesting that their firm disclose information about where and how their data is stored, the protections in place to secure it, and data breach response plans; some sophisticated clients even put law firms through information security audits. Two very core compliance questions often involve a few main categories of inquiry:

1. Industry-Standard Compliance Protocols

As technology advances and attacks become increasingly sophisticated, it is critical that data be secured using industry accepted protections including but not limited to SAS 70[1], SSAE 16[2], and SOC1 – SOC3[3]. While the details of each are extremely complex and beyond the scope of this article, firms should consider seeking compliance with them because they are critical measures of standards.

Another key measure is the "tier" system associated with datacenters, which can be summarized as follows:

Tier	Features	Datacenter Availability	Offline Time per Annum
Tier 1	Non-redundant capacity components (single uplink and servers)	Guaranteeing 99.671% data availability	System will be completely down/offline/no access for almost 29 hours a year
Tier 2	Tier 1 + Redundant capacity components.	Guaranteeing 99.741% data availability	System will be completely down/offline/no access for almost 23 hours a year
Tier 3	Tier 1 + Tier 2 + Dual-powered equipment and multiple uplinks	Guaranteeing 99.982% data availability	System will be completely down/offline/no access for almost 2 hours a year
Tier 4	Tier 1 + Tier 2 + Tier 3 + all components are fully fault-tolerant including uplinks, storage, chillers, HVAC systems, servers etc. Everything is dual-powered	Guaranteeing 99.995% data availability	System will be completely down/offline/no access for around 27 minutes a year

The cost of provisioning services in these tiers varies greatly, which obviously is a critical decision factor for companies and firms alike. Note, of course, that nobody gets to *choose* the downtime other than for scheduled maintenance.

2. Data Availability and Security

As previously mentioned, firms need to provide data to authorized users when necessary. Often, preservation data is only needed when it's time to cull the data for document review or analysis. Beyond that, having an entire preservation copy on the network may not be necessary. If it is online for convenience of reference, firms should consider setting up a VLAN (virtual network) that allows the system to only exist within the firm's physical network and only allow access to specific employees.

Encryption also provides for protection of client data by ensuring that any data coming into or leaving the firm is transported either on encrypted media or via SSL with TLS over the Internet. The proper use of encryption software, such as VeraCrypt protects against inadvertent leakage of data while in transit with common carriers. Accordingly, law firms should train employees to send passwords separately or over secondary communication sources to avoid providing an interceptor with full access to the underlying data.

For data on firm servers, information technology or security professionals should ensure that two-factor authentication (2FA) is used, as it combines a username and password with a second layer of security. Firms may also conduct routine audits to find stale accounts present on the network, and also use "tripwire" software that monitors client evidence repositories and maintains an access trail that allows for alarms to be triggered upon certain events on the evidence.

While a firm may make significant efforts to ensure that data is available when needed, it must also consider the process surrounding secure destruction of data when appropriate. This is a complicated process, requiring the case team to consider whether preservation obligations exist, whether the data may be connected to other matters, and whether a certification of deletion may be appropriate.

Device Management

Risk of theft remains a prevalent issue for laptops and other mobile devices as they usually contain sensitive business information. Once again, the proper use of robust encryption can safeguard data from being disclosed to unauthorized parties.

Although members of a law firm's IT group will traditionally keep an updated inventory of all workstations and devices in use by its employees, they may be unaware of devices received from clients, third parties, or opposing counsel. Proper procedures to account for these devices can help to avoid loss of data, inadvertent destruction, and/or infinite retention of the devices. As part of a firm's device management policy, firm-appointed personnel should carry the responsibility of tracking any such devices, and creating chain of custody forms for original evidence.

Firms should also consider employing Bring Your Own Device (BYOD) policies, which allow employees of the firm to utilize their personal cell phones, tablets, computers, or other devices for use with firm data. Mobile Device Management (MDM) software can help to manage employees who seek to check corporate email on personal cell phones and allows the firm or corporation to reset a device and remove firm or corporate data from the device. Without such software an employee is able to, easily forward company information via a personal mailbox on the device unbeknownst to the company since the email would not be flagged on their email servers as having been sent/forwarded. Citrix, Sudo Security, and Apple offer MDM software.

Phishing and Social Engineering

If an attacker is interested in gaining access to firm information, various attack vectors may be pursued. A highly effective yet very basic attack uses social engineering by impersonating members of an organization (frequently IT), and convincing a user to disclose passwords, documents, and other sensitive information. This method doesn't require the attacker to have detailed knowledge of the underlying systems and relies on the victim to circumvent any security measures, and thus is extremely low risk and carries with it the potential for significant rewards.

Phishing on the other hand relies on the untargeted distribution of fraudulent information to substantial numbers of recipients. A phishing email may instead impersonate a common social networking website demanding that a user reset their password. The link may contain malicious software or direct the recipient to a third-party website to steal their credentials.

The primary method of preventing social engineering and phishing attacks is simply through user education.

Additional Security Considerations

Law firms are increasingly adopting additional security precautions regarding the identification and authentication of its users when accessing documents, networks, and devices. The most basic precaution is having its users regularly create and revise complex passwords.

In order to protect a firm from information theft, a standard process for employee separation should be implemented, involving device deactivation (or at least password resetting), and return of all mobile devices and access cards.

Finally, when an employee is traveling, domestically or internationally, devices should be properly encrypted to prevent the disclosure of information in the case of physical theft. If connecting to a public or potentially insecure network, employees should always endeavor to utilize a VPN connection or through remote desktop environment, such as Citrix.

Ethical Considerations

The American Bar Association Model Rules provide broad guidance regarding ethical obligations. ABA Model Rule 1.1[4] requires competence in *selecting and using technology* and calls for attorneys who lack the necessary technical competence for security to consult with qualified people who have the requisite expertise.

ABA Model Rule 1.6[5] generally defines the duty of confidentiality and broadly extends that duty to "information relating to the representation of a client." It's now commonly accepted that this duty applies to client information in computer and information systems as well. An amendment to this rule added Comment 16[6], which requires reasonable precautions to safeguard and preserve confidential information.

ABA Model Rule 1.4[7], Communications, also applies to attorneys' use of technology and requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent" and also requires notice to a client of compromise of confidential information relating to the client.

These rules set up broad definitions regarding what an attorney should do in relation to holding data and communicating. Some states have taken these broad principles and developed more specific standards. For example, in Arizona, attorneys and law firms are obligated to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. Lawyers in Arizona must also recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult available experts in the field.

Whereas, in California, attorneys have an express duty "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client.[8]" Rule 3-110(A)[9] also prohibits the intentional, reckless or repeated failure to perform legal services with competence.

Massachusetts law, M.G.L. c. 93H[10], is unique in that it applies to "persons who own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts." It requires covered persons to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards." In addition to requiring a risk assessment, the regulation contains detailed

requirements for the information security program and detailed computer system security requirements. Some observers believe that this Massachusetts law will become a model for comprehensive protection of personal information.

Finally, Nevada also has laws that require "reasonable security measures" and encryption[11](NRS 603A.210 and NRS 597.970).

Cloud Storage and Ethics

Aside from the ethics opinions above, the specific issues surrounding the use of cloud storage is a relevant topic for attorneys as cloud storage offers convenience and savings. Thus far, US ethics commissions have determined that it is ethical for lawyers to use cloud computing, with most concluding that lawyers must take reasonable steps to ensure that the firm's confidential data is protected from unauthorized third party access[12]. The ABA also provides a helpful map that delineates cloud computing provisions by state[13].

Conclusion

A security policy is only as strong as its weakest physical or digital link. Law firms must ensure that their information governance policies and strategies consider both its own data and the data of its clients. Although members of a case team may not know the underlying protections and precautions that have been put into place within the firm, they should be able to consult with IT in order to provide those answers.

[1] More information is available at: http://sas70.com/sas70_overview.html

[2] http://ssae16.com/SSAE16_overview.html

[3] https://www.cpa2biz.com/Content/media/PRODUCER_CONTENT/Newsletters/Articles_2012/CPA/Jun/Easy123.jsp

[4] Available at:http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence.html

[5] Available at:http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

[6] Available at:http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html

[7] Available at:http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_4_communications.html

[8] See 1/ Bus. & Prof. Code, § 6068, subd. (e)(1).

[9] Available at: http://rules.calbar.ca.gov/Rules/RulesofProfessionalConduct/CurrentRules/Rule3110.aspx

[10] Available at: https://malegislature.gov/Laws/GeneralLaws/PartI/TitleXV/Chapter93H

[11] Available at: http://www.leg.state.nv.us/nrs/nrs-603a.html and http://www.westernreportingservices.com/NRS597.970.pdf

[12] See generally: North Carolina State Bar Council 2011 Formal Ethics Opinion 6; Massachusetts Bar Association Ethics Opinion 12-03; Oregon State Bar Formal Opinion No. 2011-188; Professional Ethics Committee of the Florida Bar Op. 10-2 (2011); New York State Bar Association's Committee on Professional Ethics Op. 842 (2010); Pennsylvania Bar Association Ethics Opinion No. 2010-060 (2010); and Iowa Committee on Practice Ethics and Guidelines Ethics Opinion 11-01 (2011).

[13] Available at:http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html#

Computer Fraud and Abuse Act

Satisfying the Computer Fraud and Abuse Act's Jurisdictional Requirements Can Be Complicated

By Paul E. Freehling (April 27, 2015)

The parties in a Computer Fraud and Abuse Act case moved for partial summary judgment. Among the issues were whether the plaintiff had incurred the requisite $5,000 in qualifying losses, and whether the complaint was time-barred. The motions were denied, but the court had to do a lot of explaining. *Quantlab Technologies Ltd. v. Godlevsky*, Case No. 4:09-CV-4039 (S.D.Tex., Apr. 14, 2015) (Ellison, J.).

Status of the case

Judge Ellison ruled that the CFAA damages threshold was met. He held that (a) the value of time spent in an internal investigation could be aggregated with (b) sums paid to two consultants to investigate the intrusions and to assist in the prosecution of resulting litigation. He also decided that the statute of limitations began to run when the plaintiff first learned of the supposed CFAA violations, even though the identity of the perpetrator was unknown. And he ruled that claims against an individual whose alleged wrongdoing was mentioned in the body of the initial CFAA count filed in 2009, but who was not named as a defendant in that count until a third amended complaint was filed in 2014, related back to the 2009 filing.

The alleged violations

Quantlab is a financial research firm that claimed to have valuable trade secrets relating to high frequency stock trading programs. In September 2007, six months after the company terminated its employee Kuharsky, Quantlab discovered that its computer network apparently had been accessed without authorization on four separate occasions between March and August 2007. An internal probe indicated that he was the culprit.

Additional investigation prior to filing the complaint

In 2008, Quantlab retained network security consulting firm Grey Hat to ascertain whether Kuharsky could gain future unauthorized access. No conclusions were reached. Later, Quantlab concluded that he had not accessed the company's files after all. Rather, it was his friend Andreev, a Quantlab employee, who acted at Kuharsky's behest and used Kuharsky's home computer.

The pleadings

Quantlab's original CFAA count named Kuharsky as a defendant. Quantlab employee Maravina was not named as a defendant, but she was described as a "sleeper mole" who had assisted Kuharsky in stealing trade secrets and confidential information. She was added as a CFAA defendant in the third amended complaint.

Calculating qualifying losses

1. Qualifying losses relating to Kuharsky. Quantlab calculated that its internal investigation in 2007 took 10-12 hours and cost the company $2,500-3,000. That sum was not enough, however, to satisfy the $5,000 requirement for bringing a CFAA lawsuit. Gray Hat billed the company $13,400 in 2008 for consulting services, but Kuharsky contended that those services did not include investigation of the supposed computer incursion. The court accepted as true the sworn declaration of Quantlab's CEO that Gray Hat was hired in response to Kuharsky's actions. Thus, the requisite qualifying loss total was deemed established.

2. Qualifying losses relating to Maravina. After the complaint was filed, Quantlab hired consulting firm Pathway Forensics and asserted that payment of its $31,900 bill constituted qualifying losses. Maravina insisted that Pathway's assignments concerned litigation, not investigating her role in the 2007 events. Quantlab maintained, however, that the lawsuit work was not included in that bill. The court concluded that since Pathway may have contributed to Quantlab's 2014 decision to add Maravina as a defendant, $5,000 in damages was demonstrated. The court said it was unnecessary to rule on the question of whether all expenses incurred investigating several persons' intrusions can be used in computing the amount of losses attributable to each person's involvement.

Statute of limitations

1. *Kuharsky.* Quantlab moved for summary judgment against Kuharsky. He asserted that the two-year statute of limitations began to run in September 2007. Quantlab argued that it had two years from early 2008 when the company first learned that Andreev, not Kuharsky, had accessed the network. The court said that the motion could not be granted because no evidence had been presented regarding the material question of whether Andreev was authorized to access the network from Kuharsky's home.

2. *Maravina.* Seven years elapsed between the intrusions in 2007 and the first time Maravina was named as a CFAA defendant. She asserted a statute of limitations defense. The court reiterated that the original CFAA count called her a "sleeper mole" and said she was "on notice that the lawsuit concerned the same conduct that now underpins the CFAA claim against her." So, that claim was held to relate back to the 2009 litigation commencement date. Although not mentioned in its recent ruling, an earlier written decision on other motions in the same case stated that she was a named defendant (but not in the CFAA count) in the original complaint, and the court added that she was Kuharsky's wife.

Takeaways

CFAA litigation can be very complex. For example, judges have not consistently ruled on the two primary issues involved in *Quantlab*: (a) the meaning of the statutory requirement of a "loss . . . of at

least $5,000," and (b) the date the statute of limitations regarding a CFAA violation begins to run. Moreover, judicial interpretations of the statutory phrases "without authorization" and "exceeding authorized access" as they relate to prohibited contact with a computer network are sharply divided. Some courts hold that those phrases refer only to hacking by an outsider. Other jurists say the statute also is directed at persons who make unauthorized use of their employer's computer. Both a prospective plaintiff considering filing a CFAA claim, and a defendant who is or may be named, should consult experienced counsel.

CFAA and SCA Do Not Prohibit Creation Of A Fake Facebook Page

By Paul E. Freehling (June 15, 2015)

The defendants in a case pending in Chicago federal court were accused of contravening Facebook's terms of use by accessing its computers in order to create a phony page and then using it to ridicule someone. In *Bittman v. Fox*, Case No. 14 C 8191 (N.D.Ill., June 1, 2015) (Holderman, J.), the court held that those allegations do not state a cause of action under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, or the Stored Communications Act, 18 U.S.C. § 2707.

Summary of the case

In 2013, several persons began voicing complaints to the staff and board of trustees of a public library which permitted patrons to view pornography on the library's computers. The objectors' increasingly strident efforts to persuade library personnel to install filters on the computers were unsuccessful. Moreover, allegedly in response to those efforts, library personnel engaged in what the objectors viewed as violations of the Illinois Open Meetings Act and as harassment. The objectors retaliated by creating a Facebook page on which they mocked the library's spokesperson. She filed a multi-count complaint alleging, among other causes of action, CFAA and SCA violations. The objectors' motion to dismiss the CFAA and SCA counts, and a few other claims, was granted. The remaining counts will be heard by a different judge (because Judge Holderman retired the day the opinion was issued).

Actions by and against the objectors

The objectors attempted to make their views heard at board meetings. The board responded by committing what the objectors viewed as Open Meetings Act violations (in at least one instance, the Illinois Attorney General agreed that the Act had been violated) and refusing in other ways to let the objectors speak their minds. On one occasion, library personnel accused the objectors of illegally disrupting board meetings and summoned the police, but no arrests were made. When the objectors began receiving harassing emails and phone calls at home, which they attributed to library personnel (acting directly or indirectly), the objectors created the fake Facebook page and used it to ridicule the library spokesperson and her floral arrangement business. She sued.

Dismissal of the CFAA and SCA claims

The CFAA and SCA counts allege that the plaintiff was injured by the defendants' violation of Facebook's terms of use, and that the violation constitutes unauthorized access to Facebook's

computer. Her allegations were imaginative, but there appears to be scant authority supporting the view that she stated justiciable causes of action.

In his ruling on the Rule 12(b)(6) motion, Judge Holderman reasoned that the statutes were enacted to protect against hacking, or tampering with, computerized personal and proprietary information. The defendants here "did not access a computer to damage, steal or tamper with" the plaintiff's data. Further, noting that the CFAA is a criminal statute, he cited the rule of lenity and the decision in *U.S. v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), a somewhat similar California case. The court there ruled for the defendant, holding that criminalizing "the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine." Judge Holderman also cited *Matot v. CH*, 975 F. Supp. 2d 1191 (D. Ore. 2013), a decision reaching the same result in a civil lawsuit.

Takeaways

According to *Matot*, the fabrication of fake social media accounts and phony profiles is not uncommon, and sometimes they even have been created by law enforcement personnel. Moreover, users of electronic media have been known to include lies and other fictions in their postings. Judge Holderman cited *Drew* for the proposition that prosecuting someone for accessing social media computers in violation of the media's rules, even as part of a vindictive campaign or one intended to embarrass, "affords too much discretion to the police and too little notice to citizens who wish to use the Internet." Judge Holderman did not mention *U.S. v. Morris*, 928 F.2d 504 (2d Cir. 1991), where the use of electronic media in a manner unrelated to its intended function contributed to a CFAA criminal conviction for unauthorized access to a public website.

In *Bittman v. Fox*, in addition to the dismissed CFAA and SCA claims, several common law causes of action were alleged. The defendants still are charged with defamation, intentional infliction of emotional distress, and interference with prospective economic advantage. The defendants in *Bittman* were not alleged to have achieved a monetary gain by violating an electronic media's rules. If there were such a claim in a different case, that claim might state a cause of action for fraud.

Trading Secrets

Corporate Espionage: Not Your Typical Sports-“Gate”

By Erik Weibust (June 26, 2015)

Generally when one refers to “competitors” in the context of protecting trade secrets, it is in regard to business competitors, not competing sports teams. And usually when the talking heads on sports radio and television are discussing legal issues, they relate to domestic violence or other crimes, concussions, illicit and performance enhancing drugs, or labor disputes (sometimes even non-competes), not to corporate espionage. Recently, however, the worlds of sports and trade secret protection collided on the baseball diamond when the St. Louis Cardinals were accused of hacking into the Houston Astros’ internal computer network and stealing proprietary information.

According to the *New York Times*, Cardinals employees gained access to the Astros’ “internal discussions about trades, proprietary statistics and scouting reports,” which the Astros no doubt would prefer to keep private. Specifically:

Law enforcement officials believe the hacking was executed by vengeful front-office employees for the Cardinals hoping to wreak havoc on the work of Jeff Luhnow, the Astros’ general manager, who had been a successful and polarizing executive with the Cardinals until 2011.

The Astros hired Mr. Luhnow away from the Cardinals in December 2011, and he quickly helped to turn the struggling team into a contender (they currently have the best record in the American League—and the second best record overall, trailing only the Cardinals who are perennial contenders). This allegedly caused Cardinals personnel to be concerned that Mr. Luhnow had taken their proprietary baseball information with him to the Astros (he has denied doing so). Indeed, highlighting the benefits of a trade secret audit, accessing the Astros’ computer system was apparently quite simple and unsophisticated, as Mr. Luhnow purportedly used the same password to access the Astros’ network that he had previously used to access the Cardinals’ network (he has denied this as well). According to the *Times*:

Investigators believe that Cardinals personnel . . . examined a master list of passwords used by Mr. Luhnow and the other officials when they worked for the Cardinals. The Cardinals employees are believed to have used those passwords to gain access to the Astros’ network, law enforcement officials said.

The FBI is investigating and “subpoenas have been served on the Cardinals and Major League Baseball for electronic correspondence.” The Cardinals and/or any employees involved in the hacking could face federal criminal charges, including charges under the Economic Espionage Act (EEA), which deals with theft of trade secrets, the Computer Fraud and Abuse Act (CFAA), which deals with the hacking itself, and perhaps even the Wire Fraud Statute.

Trading Secrets

Charges under the EEA would require prosecutors to prove that the Cardinals: (1) stole or misappropriated trade secret information (as defined by the Uniform Trade Secrets Act); (2) knew that such information was proprietary; (3) knew that such information was stolen or misappropriated; (4) acted with the intent of economically benefitting someone other than the Astros (i.e., the Cardinals); and (5) intended to injure the Astros. Moreover, the prosecution would also have to prove that the trade secrets were "related to or included in a product that is produced for or placed in interstate or foreign commerce," which Major League Baseball (the "product" here) certainly is. A person found guilty of violating the EEA can be fined or imprisoned up to 10 years, or both, and an organization such as the Cardinals that is found guilty can be fined up to $5 million.

Charges under the CFAA would require prosecutors to prove that the Cardinals: (1) accessed a protected computer, (2) without authorization or by exceeding such authorization as was granted; (3) knowingly and with the intent to defraud; and (4) obtained something of value in furtherance of the intended fraud. Penalties under the CFAA also include fines and imprisonment.

Some states have analogous criminal statutes, including both Texas and Missouri, which could be implicated given that the victim of the alleged hacking, the Astros, are located in Houston, and the alleged perpetrators, the Cardinals, are located in St. Louis.

The Astros could also seek civil damages under federal law, including under the CFAA and possibly the Stored Communications Act (if communications were hacked), as well as under state law, including state unfair business practices statutes, trade secret misappropriation statutes, and common law claims of misappropriation, conversion, and the like. Indeed, the Missouri criminal statute discussed above contains a civil cause of action that allows for the recovery of compensatory damages and attorneys' fees where there tampering with computer data, equipment, and users can be proven (including "any expenditures reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, computer service, or data was not altered, damaged, or deleted by the access").

Although it appears, based on the limited facts that have been publicly disclosed to date, that the Astros could have strong civil claims against the Cardinals, it is far more likely that they will simply allow federal officials to pursue any criminal charges they may deem appropriate, and otherwise handle the issue within the confines of MLB's disciplinary process. Indeed, MLB's constitution requires that teams address "[a]ll disputes and controversies related in any way to professional baseball" internally, with the commissioner acting as arbitrator.

Dean Pelletier and Eric Ostroff have very informative blog postings on this topic as well that are certainly worth reading. And we will be sure to provide any updates as they become available.

California Federal Courts Reiterate: Unless Computer Hacked, Computer Fraud and Abuse Act Permits Misuse Of Electronic Information

By Paul E. Freehling (September 15, 2015)

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*en banc*), the court held that the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, prohibits unlawful *access* to a computer but not unauthorized *use* of computerized information. Although that holding represents a minority position, two recent opinions — one in a Ninth Circuit criminal case and one by a California district court in a civil proceeding — indicate that the ruling in *Nosal* still is the law out west.

Recent Ninth Circuit and California district court CFAA cases

Christensen. The 100+ page opinion in *U.S. v. Christensen*, Nos. 08-50531, *et al.* (9th Cir., Aug. 25, 2015), details what the court described as "a widespread criminal enterprise offering illegal private investigation services in Southern California." Six individuals were accused and convicted in the District Court for the Central District of California pre-*Nosal* of computer fraud, bribery, racketeering, wiretapping, identity theft, and more. On appeal, several convictions were affirmed, and some others were remanded but just for resentencing. Of particular interest to readers of this blog, however, all three convictions for violating the CFAA were vacated on the ground that *Nosal* rendered the jury instructions clearly erroneous and prejudicial. A retrial may be possible.

Loop AI Labs. In *Loop AI Labs Inc. v. Gatti*, No. 15-cv-00798 (N.D. Cal., Sept. 2, 2015), the defendants' motion to dismiss certain counts of the amended complaint was granted in part and denied in part. The defendant was Loop AI Labs' former CEO. Although she had left the company and worked for a competitor, she continued to log in to Loop AI Labs' computers. The court ruled that until Loop AI Labs formally revoked her authorization to access the company's computers, she did not violate the CFAA by logging in, regardless of her motive.

Faulty jury instructions in *Christensen*

One of the defendants was a Los Angeles police officer. He was charged with violating the CFAA, among other statutes, by (a) logging in to confidential state and federal law enforcement databases — which he had the right to access — and (b) in exchange for a bribe, providing to two other defendants information they requested from those databases but to which they were not entitled. The prosecutor simply assumed, and did not attempt to prove, that the officer thereby committed a CFAA violation. According to the Ninth Circuit, that assumption was unwarranted after *Nosal* was decided.

By the same token, at trial the three defendants accused of CFAA violations did not object when the court instructed the jurors — before *Nosal* — that they should find a CFAA violation if they determined that a computer had been knowingly accessed with the intent to use the information to commit a fraud. In *Christensen*, the appellate court held that those jury instructions were plainly erroneous in light of *Nosal* and clearly were prejudicial. For these reasons, the CFAA convictions were vacated.

Takeaways

Approximately one-half of the circuit courts of appeal have ruled on the meaning of the phrase "exceeds authorized access" as used in the CFAA. In the circuits where there has not yet been a ruling, obviously, there is uncertainty as to which position the court will adopt.

The majority — so-called liberal — view is exemplified by holdings in cases such as *International Airport Centers, L.L.C. v. Citrin,* 440 F.3d 418, 420-21 (7th Cir. 2006) (CFAA violated by accessing a computer for an unauthorized purpose). *Nosal*, and now *Christensen*, represent the minority (or narrow) position that an individual with authorization to access a computer does not commit a CFAA violation regardless of what the individual does with the information so obtained.

Adding to the confusion, courts are not in agreement over the meaning of *Nosal*. For example, in the recent case of*U.S. v. Shen*, Case No. 4:14-CR-122 (W.D. Mo. Apr. 21, 2015), the facts were somewhat similar to those in *Loop AI Labs*. Citing *Nosal*, the court in *Shen* stated: "There is some disagreement as to whether an employee who properly accesses a computer and then misuses the information can be convicted" of violating the CFAA. The Missouri court added: "However, courts are clear that employees who gain access to a computer through their employment lose authorization once they have resigned or been terminated. Moreover, persons of common intelligence would understand as much." *Id.* at p.4 (citations omitted). As is apparent, the judge who decided *Loop AI Labs* does not concur. Further, there are also federal courts in California who have concurred with the *Shen* reasoning.

Similarly, one cannot be sure that all courts agreeing with the "narrow view" set forth in *Nosal* also would accept the holding implicit in *Christensen* that a corrupt police officer does not exceed his "authorized access" to confidential government data bases when he logs in solely for the purpose of providing other persons, in exchange for a bribe, information to which they have no right. With all this uncertainty, the one thing that is certain is that the Ninth Circuit continues to embrace a very narrow and restrictive view of CFAA liability, in contrast to most of the other circuits in the nation.

Michigan Federal Court Rejects As Dicta Sixth Circuit's Broad Computer Fraud and Abuse Act Interpretation

By Paul E. Freehling (October 12, 2015)

While employee Lehman was employed by Experian and allegedly subject to various employment covenants, he incorporated Thorium, a competitor. After Experian laid him off, he operated Thorium. Experian sued Lehman and Thorium in a Michigan federal court, accusing them of wrongdoing including violations of the federal Computer Fraud and Abuse Act. Holding that the CFAA is intended to criminalize hacking and that Experian's allegations of hacking were oblique at best, the court dismissed most of Experian's claims under that statute.

Status of the case

Because some of Experian's common law causes of action and one of its CFAA contentions were not dismissed, discovery is proceeding. *Experian Marketing Solutions, Inc. v. Lehman*, Case No. 15:cv-476 (W.D. Mich., Sept. 29, 2015).

Background

Experian is part of a world-wide marketing services conglomerate that collects and analyzes business data. At the time he was laid off, Lehman was Experian's executive vice president. He was based in Grand Rapids, Michigan, and was authorized to access the company's computer files. As a condition of his initial hire, and again later in connection with settlement of a claim he brought against the company while still its employee, he executed non-compete, non-solicitation, and confidentiality agreements. He allegedly violated those agreements and the CFAA by creating and operating Thorium and by downloading Experian's confidential information (both while he was an Experian employee and after he was laid off) to a hard drive that company had provided to him. He also was accused of violations by purportedly instructing three Experian employees, whom Thorium later hired, to provide him with data from Experian's computers, and by erasing all information on Experian's hard drive before returning it.

Broad and narrow interpretations of the CFAA

Federal courts are divided on the meaning of the phrases "[access] without authorization" and "exceeds authorized access" as used in the CFAA with respect to computers. Four courts of appeal have interpreted the statute broadly, ruling that the purpose for accessing a computer is relevant in determining whether access was authorized. Two federal appellate courts disagree.

The Sixth Circuit Court of Appeals

The Sixth Circuit has not ruled definitively as to the meaning of those statutory phrases. However, that court seemed to signal that it favored the majority position when it wrote, in a 2011 decision (quoting from a 2009 Ninth Circuit opinion), that "an individual who is authorized to use a computer for certain purposes but goes beyond those limitations . . . has exceed[ed] authorized access." *Pulte Homes, Inc. v. Laborers' Int'l Union of N. Amer.*, 648 F.3d 295, 304.

The ruling in *Experian*

Concluding that the Sixth Circuit has not weighed in definitively on the meaning of "authorized" as used in the CFAA, and that the quote from *Pulte Homes* is mere dicta, the district court found the minority interpretation to be the most satisfying. Since Lehman was "authorized" to access Experian's computers when he downloaded its confidential data before he was laid off, the court held that the CFAA was not violated regardless of what he did with the data. Similarly, the court ruled that the defendants did not violate the statute by obtaining, from three Experian employees who had "authorization" to access its computers, the company's proprietary secrets after Lehman was terminated. Although his continued use of an Experian computer after he was terminated clearly was not "authorized," such use was held to be not actionable under the CFAA because Experian failed to allege that he or Thorium thereby obtained anything of value.

One of Experian's CFAA claims was not dismissed. The allegation that Lehman caused "impairment to the integrity or availability of data" by wiping the hard drive clean before returning it was held to state a statutory violation.

Takeaways

A CFAA claim for unauthorized use of a computer not based on hacking is likely to be dismissed in the Fourth and Ninth circuits. Four other Courts of Appeal — the First, Fifth, Seventh and Eleventh — disagree, holding that the CFAA also prohibits accessing a computer for an unauthorized purpose even though the user has authority to use the computer. Individual district court judges in the circuits that have not ruled have reached varying decisions on this issue. Eventually, either Congress must amend the statute to resolve this inconsistencies or the U.S. Supreme Court may be asked to do so. In the meantime, litigants and their counsel can only guess how those circuit courts which have yet to decide, and the district courts in those circuits, will rule.

Nosal Update: Ninth Circuit Hears Oral Arguments on Password Sharing and Scope of Computer Fraud and Abuse Act

By Amy Abeloff and Robert B. Milligan (October 28, 2015)

On October 20, 2015, a Ninth Circuit panel consisting of Chief Judge Sidney Thomas and Judges M. Margaret McKeown and Stephen Reinhardt heard oral argument from the U.S. Department of Justice and counsel for David Nosal on Nosal's criminal conviction arising under the Computer Fraud and Abuse Act (CFAA). In 2013, Nosal was found to have violated the CFAA by allegedly conspiring to obtain access to company information belonging to his former employer, executive search firm Korn Ferry, through the borrowing of another employee's login password. He was also convicted of trade secret misappropriation under the Economic Espionage Act.

The panel focused most of its questions around one main point of contention between the parties: the interpretation of the "without authorization" language appearing throughout Section (a) of the CFAA. Such a focus makes sense given that the interpretation of this short phrase could completely change the legal landscape surrounding password sharing, not only in professional settings, but also in personal, consensual settings.

Nosal's Points

Counsel for Nosal urged the panel to adopt a limited reading of the CFAA, based on the reasoning laid out in the Ninth Circuit's previous *en banc* opinion (*Nosal I*). *Nosal I* held that the CFAA was an "anti-hacking" statute and did not contemplate, nor criminalize, the misappropriation of trade secrets. As an "anti-hacking" statute, the CFAA, the court held, criminalizes "the circumvention of technological access barriers." In other words, a person cannot be found to have accessed a computer "without authorization" if he did not circumvent a technological access barrier, or "hack" into a computer.

This time around, counsel for Nosal argued that password sharing is not hacking, and therefore, such an action cannot amount to a federal crime. Further, counsel urged the panel to limit its interpretation of the "without authorization" language appearing throughout the Act, so as to prevent the over-criminalization of actions otherwise not prohibited by law (e.g., password sharing over a cloud system, or another consensual password sharing arrangement). Nosal's counsel also argued that the "without

authorization" language be read consistently throughout the Act, so that the same interpretation would apply to both the misdemeanor and felony provisions of the Act.

U.S. Government's Arguments

On the other side of the spectrum lie the government's arguments. Counsel for the government argued that protecting computers with passwords to prevent unintended user access indeed creates a "technological access barrier," and any circumvention thereof (consensual or otherwise) constitutes a violation of the CFAA. Such a broad interpretation was met with raised brows from the members of the judicial panel.

Counsel for the government repeatedly argued that the interpretation of the "without authorization" language should mirror the interpretation in the *LVRC Holdings LLC v. Brecka* case. Per *Brecka*, a person accesses information "without authorization" under Sections (a)(2) and (4) of the CFAA when he has not received permission to use a computer for any purpose, or when the person's employer has rescinded permission to access a computer and the person uses it anyway. In other words, the government's counsel seemed to advocate the criminalization of any sort of password sharing. After receiving some push-back from the panel after making such an argument, counsel suggested limiting this interpretation to the employment context only, but members of the panel shot back because the CFAA includes no such limiting language. The government's counsel argued that the person must have shared or used the password while also knowing it was prohibited by an employer to do so.

With regard to Nosal's trade secrets conviction, the panel pressed the government's counsel for a good portion of her allotted argument time. Counsel argued the record revealed sufficient evidence to establish the element that source lists derive independent economic value for not being generally known by the general public.

Possible Outcomes for Nosal and Beyond

Though the panel did not give a clear indication one way or the other whose side it was likely to advocate in Nosal's case, recent Ninth Circuit precedent may prove enlightening on the topic. In the *U.S. v. Christensen* (9th Cir. 2015) decision, the Ninth Circuit (composed of a panel of different judges than those deciding Nosal's fate) vehemently upheld the holdings in *Nosal I*, despite the different facts of each case. In particular, the *Christensen* panel relied heavily on the *Nosal I* rationale that the CFAA only deals with violations of restrictions on access to information, not restrictions on use. At the very least, *Christensen* demonstrates that the CFAA has been on the Ninth Circuit's radar, even though its rationale may not impact the outcome in *Nosal II*.

Moreover, the panel's surprise at the government's assertion that all password sharing should be subject to criminal sanctions indicates an unwillingness to adopt such an argument. As a previous post hypothesized, the panel's final ruling will likely put to bed the password sharing issue, and limit it to certain situations (on which ground is still unclear), at least in the Ninth Circuit. The ruling will hopefully provide helpful guidance on how to formulate acceptable computer policies prohibiting conduct running afoul of the CFAA. That way, employers and businesses can better protect their trade secrets from escaping the confines of their walls.

Non-Competes & Restrictive Covenants

Appellate Court Holds That Non-Compete Agreement Assigned Pursuant to Bankruptcy Court Order is Enforceable by Assignee

By Paul E. Freehling (January 20, 2015)

Courts are divided on the enforceability by an assignee of a non-compete covenant relating to personal services where the covenant does not state whether it is assignable and the employee does not consent to the assignment.

Status of the case

A non-compete agreement signed by an employee of TSG, Inc., purported to be effective for two years after his termination and to be applicable to the whole of North America. Subsequently, TSG, Inc. was adjudicated a bankrupt. The trustee in bankruptcy assigned the agreement to TSG Finishing, a solvent, wholly-owned operating subsidiary of TSG, Inc., and the employee went to work for the subsidiary. He had the same job title, and performed essentially the same tasks, as before. Two years later, he resigned and accepted a similar position with a competitor. The subsidiary sued him and moved for entry of a preliminary injunction. The motion was denied, but the appellate tribunal reversed, remanded, and directed the trial court to enter the injunction. *TSG Finishing, LLC v. Bollinger*, Case No. COA140623 (N.C. Court of Appeals, Dec. 31, 2014).

The assignor, the assignee, and the employee

TSG, Inc. and its wholly-owned, operating subsidiary TSG Finishing, were in the business of "fabric finishing," applying chemical coatings to textiles in order to provide customers with, for example, the desired color, stiffness, and abrasion resistance. The fabric finishing process was complex and involved trade secrets.

Bollinger was a long-time employee of TSG, Inc. He signed the covenants in 2007 in exchange for a salary increase and a signing bonus.

In 2009, TSG, Inc. filed a Ch. 11 bankruptcy petition. Two years later, the bankruptcy trustee assigned a number of TSG, Inc.'s assets, including the covenants, to TSG Finishing which became Bollinger's employer. His title with each company was Quality Control Manager, and his duties were substantially the same. TSG Finishing was headquartered in Pennsylvania. He worked at a plant in North Carolina. In 2013, he quit TSG Finishing and was employed by a nearby competitor and was given a similar job assignment.

The non-compete

The covenant was silent with regard to assignability. It included a Pennsylvania choice-of-law provision.

Courts are split regarding the enforceability of personal service non-compete covenants assigned without the employee's consent, courts cite the following factors:

1. A covenant assigned simply by operation of law — for example, where the assignor corporation merely changed its state of incorporation or just converted to an LLC — usually is enforced. *See, e.g., Ochsner v. Relco Unisystems Corp.*, Case No. A13-2399 (Minn. Court of Appeals, Oct. 6, 2014), p. 6.

2. The employee may be deemed to have given implied consent if the covenant states that it is binding on the parties' "successors and assigns." If the covenant contains no such words, but the employment agreement of which it is a part contains that language, judicial rulings are not uniform.

3. Courts are divided as to whether enforceability is impacted by the form of the assignment, for example, (a) a transfer to the assignee of all of the assignor's *assets*, as opposed to (b) all of the assignor's *stock*. In either event, enforcement may be less likely if the assignor was not an operating business on the date of the transfer. *See, e.g., Cronimet Holdings, Inc., v. Keywell Metals, LLC*, Case No. 14 C 3503 (N.D.Ill., Nov. 7, 2014) (slip opin. at 11-12).

4. If the assignee and the assignor are virtually identical, and particularly if they are closely affiliated, courts seem less hesitant to enforce assigned covenants. The same is true if the employee's job title, duties and responsibilities are no different after the assignment, especially if the employee received valuable consideration for signing.

5. Judges tend to be sympathetic to employees who may be unable to earn a living if the covenant is enforced. However, judges also sympathize with assignees whose good will, confidential information, and investment would be at substantial risk in the absence of enforcement.

The rulings here

The trial court concluded that the assignee was unlikely to succeed on the merits. Among the primary factors which seem to have led to this result were the absence of a covenant provision *permitting* assignment, the enormous breadth of the covenant's geographic scope, and the court's view that a leading Pennsylvania case, *Hess v. Gebhard & Co.*, 808 A.2d 912, 922 (Pa. 2002) — which involved a sale of the assignor's assets and held that the assignee could not enforce the covenant — was analogous.

On review, the opposite result seems to have been reached primarily because of the extensive amount of time, effort, and expense the assignee (and the assignor) incurred in developing and protecting the trade secrets which were critical to the assignee's business. In the absence of enforcement, the competitor would be able to use that confidential information without making a similar investment. In addition, the appellate judges deemed the *Hess* case to be distinguishable. Also, the covenant did not have a provision *prohibiting* assignment, the assignor demonstrated that there were jobs the employee could perform even if the covenant was enforced, and substantial consideration was given for the covenant at signing.

Takeaways

There can be no certainty regarding the enforceability of a personal services non-compete assigned without the employee's permission. But consent may be inferred by, for example, a "successors and assigns" clause or if the nature of the employment immediately after the assignment is little different from what it was before. If prejudice to the assignee resulting from not enforcing the covenant greatly outweighs the harm to the employee if it is, enforcement is likely.

Trading Secrets

Non-Solicitation Covenant That Is Silent As To Its Scope May Be Unenforceable

By Paul E. Freehling (February 18, 2015)

An employment agreement covenant prohibiting solicitation of co-employees, but not indicating what solicitations were prohibited, has been held to be invalid.

Status of the case

A multi-count complaint filed in the D.C. District Court charged two former employees of the plaintiff with breaches of contract and tort violations. The defendants moved to dismiss. The court held that some of the eight counts stated causes of action, but one count the court did dismiss alleged that the defendants violated their covenant not to solicit the plaintiff's employees. The court held that the covenant was too vague to be enforceable because it did not specifically identify the solicitations that were impermissible. *Base One Technologies, Inc. v. Ali*, Civ. Ac. No. 14-1520 (D.D.C., Jan. 20, 2015).

Base One's business model

Base One was in the business of recruiting and staffing telecommunications and financial information management personnel for clients. The personnel that were recruited became employees of Base One. Each was assigned to work at a particular Base One client according to the client's needs and the employee's skill set.

Non-competition and non-solicitation covenant

The two defendants were hired by Base One to work on an extensive computer-related project for a specific Base One client. They both signed Base One's employment agreements. Those agreements stated that employees are likely to be "the principal intermediary and personal contact" between Base One and the client. Further, recognizing that Base One's employees frequently gain extensive knowledge of the client's business and develop loyalties with the client, the agreements note that clients "might desire to place their IT business directly with" the employees — after the employees' relationship with Base One has ended — rather than with Base One. Accordingly, the agreements mandate that during and for one year after termination of the Base One employment relationship, employees shall not "market any [competitive] type services" to a Base One client the employee was serving, and shall not "solicit, contact, represent, or offer to represent" other Base One employees.

Alleged violation and lawsuit

When the two defendants left the employ of Base One, they immediately went to work for the Base One client they had been serving. Base One filed a complaint which included what the court described as "a veritable cornucopia of claims." Two counts alleged breach of contract. One averred that the defendants violated the non-solicitation covenant by soliciting each other to work for the Base One competitor (the second breach of contract count alleged contravention of the non-compete provision). The defendants' motion to dismiss the former count was granted.

The court's reasons for dismissing the count regarding prohibited solicitation

In the court's view, the wording of the covenant "is so vague and ambiguous as to render it unenforceable. . . . Although the Court can perhaps guess that [Base One] meant to prohibit solicitation or contact for the purpose of employment elsewhere, the provision does not so specify." Noting that the employment agreement contained a New York choice of law provision, and "Particularly in light of New York's general hostility toward restrictive covenants in the context of employment, the Court will not redraft a poorly written, overbroad restraint in order to make it enforceable."

Takeaways

A motion to dismiss, or for summary judgment with respect to, allegations based on a "vague and ambiguous" contract provision might be denied on the ground that the parties' intent regarding the meaning of the provision is an issue of fact to be resolved at trial. *See, e.g., Whelan Security Co. v. Kennebrew*, 379 S.W.3d 835, 846 (Mo. Sup. Court 2012) (summary judgment inappropriate because "the lack of any language regarding the purpose of the employee non-solicitation clause prevents this Court from determining the purpose of the clause as a matter of law. The intent of the parties must instead be determined by the use of parol evidence, creating a factual issue for the trier of fact"). But the *Base One* court went a different route, granting the defendants' Rule 12(b)(6) motion to dismiss the claim relating to a non-solicitation agreement which contained the identical ambiguity as in *Whelan*. The moral of the story is that two courts sometimes issue diametrically opposite rulings when presented with the same question of law.

Geographically Overbroad Non-Competes Held To Be Unenforceable

By Paul E. Freehling (February 26, 2015)

In unrelated decisions, two federal courts recently refused to enforce non-compete covenants in employment agreements that lack reasonable geographic limits.

Status of the cases

In one of the two lawsuits, the employment agreement included a Tennessee choice of law provision. Louisiana courts are more protective of employees than courts in Tennessee. Since the parties had contacts with both states, naturally the ex-employee contended that Louisiana law applied and the former employer disagreed. A Louisiana district court judge sided with the ex-employee, held that the non-compete violated Louisiana law, and granted summary judgment to the ex-employee. *Bell v. L.P. Brown Co.*, Civ. Ac. No. 14-2772 (W.D. La., Feb. 2, 2015).

In the other case, an Arkansas district court judge ruled that the non-compete provision in the parties' employment agreement violated Arkansas law. The former employer sued to enforce the non-compete, but the Eighth Circuit Court of Appeals affirmed the district court's order dismissing the lawsuit. *NanoMech, Inc. v. Suresh*, No. 13-3671 (8th Cir. Feb. 6, 2015).

The covenants

Both companies' covenants purported to be applicable during the employment period and for two years after termination. The temporal limits were not significant issues in either case.

1. *L.P. Brown Co.'s covenant.* It prohibited, "within any U.S. cotton market," (a) competing, directly or indirectly with the company (which was in the cotton and fiber industry), or (b) "becom[ing] employed by or perform[ing] services in any capacity for" any of its competitors.

2. *NanoMech's covenant.* This corporation "researches and develops nanotechnologies." Its non-compete contained the employee's commitment not to "be employed by, or consult in any business which competes with" NanoMech.

L.P. Brown Co.'s choice of law provision

Brown Co.'s principal place of business is in Memphis. Bell, a salesman, lives in Louisiana. He delivered the signed employment agreement to Brown Co. in Memphis, attended several sales meetings there, and picked up his company car and computer in Tennessee. His company-issued cell phone was shipped to him from Memphis. However, he worked out of his home, and his business cards showed his Louisiana address. He was Brown Co.'s only employee in Louisiana. His territory included parts of Louisiana, Tennessee, and two other states.

The court observed that Tennessee "generally upholds what it deems to be reasonable non-competition agreements, viewing [them] as promoting stable business and employment relationships." By contrast, "Louisiana has long had a strong public policy in protecting its employees from restrictions on the common law right to work." Analogizing to a Louisiana judicial ruling relating to a contractual forum selection clause in an employment agreement, the court in*Brown Co.* held that Tennessee law would apply to Bell only if, after the event giving rise to the litigation, he "expressly, knowingly, and voluntarily agreed to and ratified" the choice of law provision.

Contemporaneous with his delivery to Brown Co. of his resignation, Bell asked the company twice to release him from the non-compete (the company refused both requests). In addition, he executed an acknowledgement confirming that he had been reminded of the non-compete. The court held, however, that these acts failed to meet the Louisiana standard for application of Tennessee law because the parties did not discuss explicitly, and Bell did not unequivocally consent to, the choice of law provision.

Nano-Mech's covenant

The Court of Appeals noted that under Arkansas law, which admittedly applied to the covenant, restraints in employment agreements are enforced only if they are "reasonably necessary to secure the interest of the" protected party and are "not so broad as to be injurious to the public interest." NanoMech insisted that Suresh had had extensive access to the company's trade secrets, that it competes with nanotechnology companies around the world, and that there was a risk she would disclose the confidential information if she worked for a NanoMech competitor. The appellate tribunal concluded, however, that an Arkansas court would not enforce a non-compete that contained neither a geographic nor a customer-specific restriction.

Takeaways

These opinions illustrate the importance of drafting employment agreement restrictive covenants that will be enforceable under whatever law is applicable. There is considerable variation among different states' views regarding such provisions. So, a company with operations in a number of jurisdictions should tailor the wording to fit the locale. As these cases demonstrate, "one-size-fits-all" covenants may not be enforceable in every state where litigation concerning them might be filed. Seyfarth Shaw can provide state-by-state guidance regarding the language to use in employment agreements to maximize the likelihood that non-compete, non-solicitation and confidentiality provisions will be enforced.

Beware of the Delaware Choice of Law in Non-Compete Agreements

By Justin K. Beyer and Matthew I. Hafter (March 2, 2015)

Delaware has long been one of the jurisdictions most friendly to the interests of corporations and is the state of incorporation for a significant majority of corporations. While that trend does not seem likely to change, a new Delaware Chancery Court decision should give pause to choice of law decisions of Delaware corporations with multi-jurisdictional work forces and operations in states other than Delaware.

Recent Ascension Case

In *Ascension Ins. Holdings, LLC v. Underwood*, C.A. No. 9897-VCG, 2015 Del. Ch. LEXIS 19 (Del Ch. Jan. 28, 2015) (unpublished), the Delaware Court of Chancery recently ruled that, despite a Delaware choice-of-law and venue provision contained in a non-compete agreement, California law applied to the agreement and under California law the agreement was void as a matter of law. In this case, the plaintiff (Ascension) sought an injunction against a former employee (Underwood) for violating a non-compete provision in an employment agreement entered into around the same time Ascension purchased Underwood's business under an asset purchase agreement.

When Underwood terminated his employment relationship with Ascension, the five-year non-competition period under the asset purchase agreement lapsed. However, the separate non-compete provision of Underwood's employment agreement provided a two-year tail at the end of the employment, which Ascension argued was specifically contemplated during the negotiations when acquiring Underwood's business.

Ascension was incorporated in Delaware, but headquartered in California which is also where Underwood worked. In the employment agreement, parties selected Delaware law to govern. Delaware law generally enforces employee non-competition agreements if reasonable in scope and duration and if they advance a legitimate economic interest of the employer. California, in contrast, has a specific statute that renders a covenant not to compete unenforceable against an employee unless made in connection with his or her sale of substantially all of the assets and goodwill of a business non-competition agreements (Cal. Bus. & Prof. Code Sections 16600, 16601).

Choice of Law Analysis

The Chancery Court conducted a choice-of-law analysis to determine whether Delaware or California law would apply. The court found that the parties' relationship was centered in California, the various contracts were negotiated and entered into there, and the territory in which the defendant employee would be restricted was located there. The court acknowledged that "[u]pholding freedom of contract is a fundamental policy of [Delaware]" but rejected the plaintiff employer's argument that Delaware's interest in that policy trumped California's interest in not burdening its citizens with non-competition covenants. The Delaware court acknowledged that under the applicable California statute the non-

compete in the asset purchase agreement would be enforceable to protect the acquired goodwill, but reasoned that the covenant in the employment agreement was directed to a different employer interest; concluding that the restriction in the employment agreement would be prohibited under California law. It held that "allowing parties to circumvent state policy-based contractual prohibitions through the promiscuous use of [choice-of-law] provisions would eliminate the right of the default state to have control over enforceability of contracts concerning its citizens." On this basis, the Chancery Court denied the employer's motion for preliminary injunction.

Practical Considerations

For Delaware corporations with employees in many states, this case presents a conundrum:

- While there is clearly a value to having a single state law govern its relationship with employees in many states, and Delaware law is comparatively employer-friendly with respect to restrictive covenants, there is a risk that the law of each employee's home state will control unless the corporation has a meaningful connection to Delaware.

- Similarly, a Delaware corporation headquartered in a state with laws on restrictive covenants that are in the middle of the spectrum (enforceable but narrowly construed or with high proof thresholds) might opt for Delaware law because it is more favorable. But in that situation the employer should evaluate the risk that in reaching for the more friendly laws of Delaware it may lose the benefit of even the modestly friendly provisions of its home state and become subject to laws of each employee's state which may render non-competition restrictions completely unenforceable or in other respects may be less favorable that those of the employer's home state.

- In mergers and acquisitions and similar transactions involving the sale of a business, acquirers commonly require restrictive covenants in both the sale agreement and in separate employment agreements. Acquirers should balance the risk that a court in any particular state may reject the choice-of-law provision that selects Delaware compared with the law of the state in which the acquirer has meaningful contacts.

Trading Secrets

Ninth Circuit Jeopardizes Broad "No Re-Hire" Clauses in California

By Robert B. Milligan and Carrie Price (April 13, 2015)

In *Golden v. California Emergency Physicians Medical Group*, a divided Ninth Circuit panel held that a "no re-hire" provision in a settlement agreement could, under certain circumstances, constitute an unlawful restraint of trade under California law.

The Facts

Dr. Golden, a physician, agreed to settle his discrimination claim against his employer, California Emergency Physicians Medical Group ("CEP"). Their oral settlement agreement, later reduced to writing, had Dr. Golden "waive any and all rights to employment with CEP or at any facility that CEP may own or with which it may contract in the future." The district court enforced the parties' settlement over Dr. Golden's objection that this "no-rehire" clause violated Section 16600 of California's Business & Professions Code, which provides that a contract is void if it restrains anyone from engaging in a lawful profession.

The Appellate Court Decision

On appeal, Dr. Golden argued that the "no re-hire" clause was unlawful and that, because it constituted a material term of the settlement, the entire agreement was void, permitting Dr. Golden to pursue his discrimination lawsuit.

The Ninth Circuit panel determined that Dr. Golden might prevail on this argument, and remanded the case to the district court for further proceedings. The panel first found that the validity of the "no re-hire" clause was ripe for determination. The dispute was ripe not because CEP was currently seeking to enforce the "no re-hire" clause against Dr. Golden (it was not), but because Dr. Golden sought to have the settlement agreement voided after his former attorney attempted to enforce the agreement in order to collect attorney's fees. The panel reasoned that "when a litigant resists his adversary's attempt to enforce a contract against him, the dispute has already completely materialized."

The Ninth Circuit panel next addressed the validity of the "no re-hire" clause. Historically, this type of clause, which commonly appears in settlement agreements, has not been viewed as a non-compete clauses, in that a "no re-hire" clause does not keep a former employee from working for a competitor—just the former employer. The *Golden* court, however, took a wider view of Section 16600, reasoning that it applies to *any* contractual provision that " 'restrain[s anyone] from engaging in a lawful profession, trade, or business of any kind' … extend[ing] to any 'restraint of a substantial character,' no matter its form or scope."

To support this broad interpretation, the Ninth Circuit panel majority cited Section 16600's language, statutory context, and case law to reason that Section 16600 applies to any contractual limitation that restricts the ability to practice a vocation. *See, e.g., Edwards v. Arthur Andersen LLP*, 189 P.3d 285

(Cal. 2008); *City of Oakland v. Hassey*, 163 Cal. App. 4th 1447 (2008). The panel majority noted that both *Edwards* and *Hassey* focused on the text of the law—whether the contested clause restrained someone from engaging in a trade, business, or profession—and not specifically whether the clause prevented competition with the former employer. The panel majority concluded that a clause creating a restraint of "substantial character" that could limit an employee's opportunity to engage in a chosen line of work would fall under Section 16600's "considerable breadth."

Of significance is that the Ninth Circuit panel did not rule that the clause was actually void. Instead, the panel majority concluded that the district court would need to do more fact-finding to see if the clause actually created a restraint of a "substantial character" on Golden's pursuit of his profession.

It also is significant that the Ninth Circuit panel majority—mindful that the California Supreme Court itself has not ruled on whether Section 16600 extends beyond traditional non-compete clauses in employment agreements—was merely predicting how it thought the California Supreme Court would rule.

A sharp dissent by Judge Kozinski expressed skepticism that the California Supreme Court would reach the same result as the panel majority, and argued that the settlement agreement should be enforced because the provision put no limits on Dr. Golden's current ability to pursue his profession.

What Is the *Golden* Rule for California Employers?

Golden furnishes no clear guidance as to the continued viability of "no re-hire" clauses in California settlement agreements, for it is unclear how courts will apply the "substantial character" standard. However, it can be expected that plaintiffs' lawyers will closely scrutinize "no-rehire" clauses and that this is even more likely if a clause applies beyond the employee's prior employer to, for example, subsidiaries and affiliates of the employer, or if the employer commands a substantial share of the relevant labor market. But more limited "no re-hire" clauses, for most employers, would not seem to create any restraint that one could reasonably consider to be of "substantial character." And most cases, unlike *Golden*, would not raise the validity of a "no re-hire" clause until there actually is an issue of re-hire—an issue that often never arises as a practical matter. Nonetheless, until the California Supreme Court weighs in, California employers should consider the Ninth's Circuit's decision when drafting settlement agreements that contain "no re-hire" clauses.

Forum Selection Clause in Non-Compete Agreement Unenforceable

By Paul E. Freehling (April 20, 2015)

A contractual provision designating the exclusive venue for filing a breach of contract lawsuit was held to be trumped by a 100-year old statute requiring trial of such cases in the county of residence of at least one party. *A&D Environmental Services, Inc. v. Miller*, Case No. COA14-913 (N.C. App., Apr. 7, 2015).

Summary of the case

A North Carolina statute provides that, absent other applicable law, contract litigation "must be tried in the county in which" one or more plaintiffs or defendants reside when the complaint is filed. The parties' employment agreement relevant to this litigation included a non-compete, not-solicit, and confidentiality provision, and a forum selection clause which stated that any complaint concerning the agreement "shall be brought exclusively in Mecklenburg County, North Carolina" (most likely Charlotte). The employer was headquartered in Guilford County (Greensboro, which is 90 miles from Charlotte). The employee, a resident of Orange County (not far from Greensboro), resigned, went to work for a competitor, and was sued in Guilford County. He moved to dismiss for lack of venue. His motion was denied, and the ruling was affirmed on appeal.

The Appellate Court's Holding

There was no evidence that either party resided in Mecklenburg County, the contractually designated "exclusive" venue. Relying on the statute, as well as a 1921 North Carolina Supreme Court decision (*Gaither v. Charlotte Motor Car Co.,* 182 N.C. 498, 109 S.E. 362) applying the statute in a factually similar lawsuit, the appellate tribunal held that venue in Guilford County was proper. The reasonableness of the statute as applied to the facts was not addressed.

Takeaways

At one time long ago, most courts invalidated forum selection clauses on the ground that the parties have no right to dictate where their disputes may be adjudicated (particularly if the legislature had addressed the issue). Today, the North Carolina statute and courts in a few other states perpetuate that philosophy.

However, a 1972 U.S. Supreme Court decision (*The Bremen v. Zapata Off-Shore Co.,* 407 U.S. 1) criticized such thinking in part because forum selection clauses often provide consistency and certainty. Thereafter, many judges have held that such clauses must be analyzed on a case-by-case basis. When drafting — or being asked to agree to — a forum selection clause, keep the following factors in mind since they may determine whether it will be enforced:

Trading Secrets

- whether the clause identifies the *only* court or courts where the controversy is to be heard or simply refers to a *permissible* adjudicatory forum,
- whether the contract was procured by fraud or duress, and whether the choice of venue is reasonable,
- whether the selected forum has subject matter jurisdiction (for instance, a clause naming a specific federal court will not be enforced in the absence of diversity of citizenship and the jurisdictional amount in controversy, or a federal question),
- whether there is a nexus between the facts underlying the dispute and the location of the contractually designated adjudicator,
- whether the relief requested by the plaintiff is at odds with fundamental policies of either the state of the forum or of the selected venue, and
- whether comity is impacted (for example, if the contractual venue is in another country and was a reasonable selection when the contract was signed, the decision-maker may be inclined to enforce the clause, other things being equal).

Aggressive SEC Enforcement Efforts Regarding Confidentiality Agreements Will Continue

By Ada W. Dolph (April 22, 2015)

In a post-script to the SEC's April 1 cease and desist order penalizing KBR, Inc. for a confidentiality statement that failed to carve out protected federal whistleblower complaints (our alert on it here), SEC Office of the Whistleblower Chief Sean McKessy today made additional comments that suggest public companies as well as private companies that contract with public companies should immediately review their agreements for compliance.

In a webinar sponsored by the American Bar Association titled "New Developments in Whistleblower Claims and the SEC," McKessy commented on the recent KBR Order. Here are the key takeaways:

SEC Rule 21F-17 is "Very Broad"

McKessy stated that he views the SEC Rule 21F-17 as "very broad," and "intentionally so." The Rule provides in relevant part:

(a) No person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement . . . with respect to such communications.

McKessy said that he reads the Rule as stating that "no person shall take *any* action" to impede an individual from communicating directly with the SEC.

Agreement Review a Continued High Priority for the SEC

McKessy stated that this initiative remains a "priority" for him and his office. "To the extent that we have come across this language [restricting whistleblowers] in a Code of Conduct" or other agreements, the SEC has taken the position that it "falls within our jurisdiction and we have the ability to enforce it."

He noted that "KBR is a concrete case to demonstrate what I have been saying," referencing public remarks he has made in the past regarding SEC scrutiny of employment agreements. He stated that the agency is continuing to take affirmative steps to identify agreements that violate the Rule, including soliciting individuals to provide agreements for the SEC to review. Additionally, he reported that the SEC is reviewing executive severance agreements filed with Forms 8-K for any potential violations of the Rule.

The KBR Language is Not a "Safe Harbor"

When asked whether the language required as part of the KBR Order constituted a "safe harbor," McKessy stated that he would "not go that far," and that each agreement will be viewed in context. He described the language in the KBR Order as "certainly instructive" but "not restrictive" and not insulating a company from further scrutiny by the SEC. He also stated that it is "really not appropriate for me to bless any language," and suggested that the same language could be acceptable in one context but not in another depending on the company's approach to encouraging employees to come forward to report alleged securities fraud.

KBR Could Be Applied to Private Companies

McKessy was also asked whether the SEC would apply the KBR Order to private companies under the U.S. Supreme Court's 2014 ruling in *Lawson v. FMR LLC*, 134 S.Ct. 1158 (2014), which expanded Sarbanes-Oxley's whistleblower protections to employees of private companies who contract with public companies.

McKessy stated that the SEC has not officially taken a position on this issue, but in his personal opinion he can "certainly can see a logical thread behind the logic of the *Lawson* decision" to be "expanded into this space [private companies]," and that "anyone who has read the *Lawson* decision can extrapolate from it the broader application."

SEC Not Bound By Agreements Precluding Production of Company Documents

McKessy was asked regarding the SEC's position regarding the disclosure of company documents by whistleblowers in their complaints to the agency. He said that it will "surprise no one that companies have a 100% record" of preferring that company documents not be provided to the SEC. But, "[a]t the end of the day" he stated that any kind of agreement restricting an employee from providing company documents to the SEC is not enforceable against the SEC and companies should not "bank on the fact" that the SEC would "feel bound" by that agreement in any way.

McKessy took a more measured approach with regard to privileged company documents, however. McKessy stated that the SEC is "not interested in getting privileged information" and that the SEC discourages whistleblowers and their counsel from providing privileged information as part of their complaints. He noted that while there are "certain exceptions to privilege," he would "hate to leave the impression that [the agency] is looking to create to create an army of lawyers who can ignore their confidentiality requirements because of the possibility of being paid under our [Dodd-Frank bounty] program."

Next Steps for Companies

McKessy concluded his remarks on this issue by stating that "[t]his is the time for the company to take a look at standard, standing severance and confidentiality agreements."

In short, it is clear that we can expect further SEC enforcement actions in this area. Public companies and private companies that contract with public companies should consult with counsel to review their employment agreements to be sure they will not be the next to be caught in the SEC's crosshairs.

Court, Applying Pennsylvania And California Law, Declines To Enjoin Alleged Violation Of Worldwide Non-Compete

By Paul E. Freehling (May 5, 2015)

A non-competition covenant prohibited employees of Adhesives Research (AR), a company based in Pennsylvania, from performing services for a competitor of AR anywhere in the world for two years after termination. Newsom, AR's western U.S. manager of medical products, worked out of her home in California. When she quit and joined another adhesives manufacturer, AR sued and moved for entry of a preliminary injunction. The court denied the motion.

Status of the case

The covenant contained a Pennsylvania choice of law provision and mandated that litigation be filed in that state. Responding to the motion, Newsom argued that Pennsylvania law was inapplicable and asserted that California law applied. It is less friendly to employers. The court concluded that the worldwide geographic scope was overbroad under both states' legal principles, that blue penciling was impermissible because of AR's unclean hands in attempting to enforce an oppressive covenant, and that in any event the new employer did not compete with AR. *Adhesives Research, Inc. v. Newsom*, Civ. No. 1:15-CV-0326 (M.D. Pa., Apr. 13, 2015) (Caldwell, J.).

The parties

AR makes adhesives used in medical, pharmaceutical, electronics, and other industries. Its headquarters are in Glen Rock, PA, but it sells adhesives all over the world. They are purchased as raw materials and used by customers in making their final products. Except for a few days each year spent at corporate headquarters for meetings and training, Newsom worked from home but communicated frequently with AR in Glen Rock.

The non-compete

In 2012, AR required all of its employees, including Newsom, to sign a non-compete agreement. It prohibited performance of:

"any services similar to the services performed by [the employee] during his employment with [AR], for . . . any business . . . that develops, manufactures or sells any products that compete in kind with . . . any products manufactured, sold or under development by [AR] . . . in any area of the world in which such products are sold by [AR]."

The agreement, which contained a Pennsylvania choice of law provision, included a consent to litigation exclusively in a federal or state court in Pennsylvania and a waiver of a claim or defense that the forum was inconvenient.

Newsom's resignation from AR, and her new employment

Newsom resigned from AR and went to work for Scapa Tapes, a manufacturer of bonding and adhesive products, as a sales executive for the western United States. Unlike AR, Scapa does not sell raw adhesives. Rather, it uses the adhesives in making the other products it sells.
Unenforceability under California and Pennsylvania law. Newsom maintained that California law controls the non-compete covenant as against her even though it specifies application of Pennsylvania law. Without deciding, Judge Caldwell concluded that the covenant is unenforceable under either state's laws.

California. A California statute provides that, with exceptions not applicable here, contractual employee non-compete clauses are void.

Pennsylvania. Courts in Pennsylvania require that restrictions in an employment agreement's non-competition clause must be "roughly consonant" with the employee's duties and must not be unduly burdensome. According to Judge Caldwell, a worldwide ban on Newsom's employment by an AR competitor "is not limited to an area reasonably necessary to protect" AR. He also held that the ban results in a severe hardship to her. Moreover, he concluded that AR had engaged in oppressive overreaching by applying an unlimited geographic scope to an employee whose territory only included one-half of this country, and he ruled that AR had unclean hands. Although Pennsylvania permits blue penciling of unreasonably broad contractual restrictions in some circumstances, the judge stated that AR's unclean hands here preclude the exercise of such judicial discretion in its favor.

The non-competition clause

Judge Caldwell held that AR and Scapia are not competitors. AR manufactures adhesive rolls which it sells to customers for use in their products. By contrast, Scapia does not sell adhesive rolls but, rather, makes and sells goods which contain adhesives. He ruled that the restraint against working for a company that manufactures or sells "any products that compete in kind" with AR's products is overbroad because no prudent prospective employer engaged in a business even remotely similar to AR's would take a chance on hiring a former AR employee.

Takeaways

Employers with workers in more than a single state, who are required to sign a one-size-fits-all non-compete, non-solicitation and/or confidentiality template, run a significant risk that it will not be enforceable in at least some jurisdictions. In addition, inclusion of provisions more protective than necessary jeopardize enforceability. For help in drafting enforceable restrictive employment covenants, consult an experienced trade secrets attorney.

Trading Secrets

Court Affirms California Attorney General's Demand for Confidential Donor List

By Ofer Lion, Douglas M. Mancino, and Christian Canas (June 1, 2015)

Unwelcome news for charities concerned with donor confidentiality

A recent court ruling[1] upheld the position of the California Attorney General (AG) requiring that charities located or operating in California provide a copy of their unredacted Form 990 Schedule B, including the names, addresses and contribution amounts for all donors listed. While the AG has indicated that the information will not be made publicly available, the ruling is unwelcome news for charities concerned about protecting donors' identities. The collection of sensitive donor information from charities appears to be a growing trend by state Attorneys General. Affected charities, including out-of-state charities soliciting or otherwise operating in California should review their donor confidentiality policies and disclosures to ensure that their donors are aware of such requirements.

Regulation of Charities Located or Operating in California

Most California charities and certain out-of-state charities are required to register and file an annual report (Form RRF-1) with the AG's Registry of Charitable Trusts. Religious organizations, educational institutions, hospitals and health care service plans are exempt from this registration and reporting.

A copy of the charity's annual return (Form 990) must be included with the annual report. The AG recently began treating annual reports submitted without Schedule B (or with a redacted Schedule B) as incomplete. Failure to file a complete report generally results in penalties, fees and the loss of California income tax exemption.

Several states, including New York, have a similar filing requirement. Both the California and New York AGs note that their policy is not to disclose Schedule B to the public. However, there is no guarantee that their disclosure policies will not change in the future and it is unclear if the donor information, once in the possession of a state's AG, would be subject to a request for disclosure under that state's public records act.

Schedule B – Donor Disclosure

Schedule B to the Form 990 is used to disclose to the IRS the reporting organization's significant donors (generally those who contribute over $5,000 in cash or property), including their names, addresses, and contribution amounts. Tax-exempt organizations are generally required to make available for public inspection and copying their three most recent annual returns, including copies of all schedules, attachments and supporting documents filed with these returns. Most such returns are posted and publicly available at no cost on third-party websites, such as Guidestar.org.

However, except for private foundations (Form 990-PF filers) and section 527 political organizations, public disclosure of the names and addresses of contributors set forth on Schedule B generally is not required, and the Schedules B of those organizations typically do not appear when posted online.

The Center for Competitive Politics, a Virginia nonprofit registered with the California AG, challenged the AG's unredacted Schedule B filing requirement. It argued that the disclosure violates its and its supporters' First Amendment rights to freedom of association and that certain nondisclosure rules under federal law preempt the state requirement.

The Ninth Circuit affirmed an earlier decision to deny the Center's motion for a preliminary injunction, rejecting the Center's arguments and concluding that the disclosure requirement bears a substantial relation to a sufficiently important government interest and is facially constitutional.[2]

However, the Court left open the possibility that the Center could show a reasonable probability that the compelled disclosure of its contributors' names will subject them to threats, harassment or reprisals that would warrant relief on an "as-applied" challenge. Such a challenge, *Americans for Prosperity Foundation v. Harris*,[3] is pending in the Ninth Circuit. So, the Court may soon carve such an exception out of California's filing requirement, or not.

Out-of-State Charities with a California Presence Subject to Disclosure

Out-of-state corporations that are (1) "doing business" in California for charitable purposes or (2) "holding property" in California for such purposes are subject to the AG's registration and filing requirements, as well as a whole host of other regulations generally applicable to California charities.[4]

"Doing business" is not a defined term, but generally requires that a corporation conduct some systematic or ongoing activity in California. The AG has issued limited examples of activities that, if conducted in the state, would constitute doing business in California, including: (1) soliciting donations by mail, by advertisements in publications, or by any other means from outside of California, (2) holding board or membership meetings, (3) maintaining an office, (4) having officers or employees who perform work, and/or (5) conducting charitable programs. Grantmaking in California, by itself, generally is not considered doing business in California.

The second basis for subjecting an out-of-state charity to the reporting and registration requirements is "holding property" in California for charitable purposes. Unfortunately, the AG's office has not issued guidance on the distinction between holding property for charitable purposes and holding property for investment or other non-charitable purposes other than a brief statement on its website that maintaining "financial accounts or investments at an office of a financial institution located in California" does not constitute doing business in California.

Out-of-state charities that may meet the above requirements and are not currently registered with the AG's Registry of Charitable Trusts may wish to consider contacting local counsel for advice regarding their California operations to avoid or minimize potential penalties.

Conclusion

The recent *Center for Competitive Politics* decision exemplifies what we expect to be a growing trend by state Attorneys General to demand sensitive donor information from charities operating or soliciting in those states. Charities should continue to heed the Schedule B instructions and not include Schedule B in filings with states that do not require it, as those states may inadvertently disclose the charity's donor information to the public.[5]

[1] *Center for Competitive Politics v. Harris*, No. 14-15978 (9th Cir. May 1, 2015).

[2] On May 15, 2015, the Center filed with the U.S. Supreme Court (Justice Kennedy) an application for an injunction to block the disclosure pending the filing and disposition of a petition for a writ of certiorari. In a setback to the Center, the application was denied without prejudice to renewal in light of any further developments.

[3] *Americans for Prosperity Foundation v. Harris*, No. 2: 14-cv-09448-R-FFM (C.D. Cal. Feb. 23, 2015).

[4] For a detailed discussion of California requirements that extend to out-of-state charities, see Mancino, "California Regulation of Out-of-State Charities," 17 Taxation of Exempts 6 (May/June 2006).

[5] Schedule B, Page 5 (General Instructions: Public Inspection), available at http://www.irs.gov/pub/irs-pdf/f990ezb.pdf.

Texas Don't Hold 'Em: Forum Selection Clause Is Unenforceable

By Joshua A. Rodine and Jonathan L. Brophy (June 10, 2015)

California courts generally favor forum selection clauses entered into freely by parties and where enforcement is not unreasonable. This general principle is true even if the forum selection clause is "mandatory" and requires a party to litigate its dispute exclusively in the designated forum. The party opposing enforcement of a forum selection clause ordinarily bears the burden of proving why the clause to which it previously agreed should not be enforced.

Contrary to these general principles, on May 28, 2015, in *Verdugo v. Alliantgroup, L.P.*, the California Court of Appeal held that if a dispute involves unwaivable claims under California's Labor Code, the employer seeking to enforce the forum selection clause bears the burden of showing that litigating the claims in the contractually designated forum "will not diminish in any way the substantive rights afforded … under California law."

The Facts

When Texas-based Alliantgroup hired Rachel Verdugo, she signed an "Employment Agreement." The Agreement provided that any dispute regarding Verdugo's employment had to be brought in Harris County, Texas and that the laws of Texas would govern the dispute.

When Verdugo filed a class action lawsuit alleging Labor Code violations involving unpaid overtime, meal and rest breaks, wage statements, and timely termination pay, Alliantgroup moved to stay the action based on its forum selection clause. The trial court found the forum selection clause enforceable and stayed the action.

The Appellate Court Decision

The Court of Appeal reversed the trial court. It held that Alliantgroup bore the burden of showing that enforcing the forum selection clause would not significantly diminish Verdugo's statutory rights. The rationale for this holding was that the Labor Code claims asserted by Verdugo were unwaivable and the forum selection clause had the potential to operate as a waiver. Alliantgroup thus had the burden to prove that the clause did not in fact significantly diminish unwaivable statutory rights.

The Court of Appeal held that Alliantgroup had failed to meet its burden. The Court of Appeal explained that "a comparison is necessary to determine whether enforcing a forum selection clause and choice of law clause would violate California's public policies embodied in its governing statutes." Because Alliantgroup failed to compare Texas and California law on overtime pay, breaks, and other compensation issues raised by Verdugo's claims, and because Alliantgroup failed to compare the policies underlying Texas and California law, or their respective interests in having their laws enforced, Alliantgroup failed to demonstrate that its forum selection clause was enforceable.

What *Verdugo* Means For Employers

Employers should review their forum selection and choice of law clauses to determine whether they will be able to show that they are enforceable if an employee raises unwaivable Labor Code claims. In this case, the Court of Appeal expressly noted that "Alliantgroup could have eliminated any uncertainty on which law a Texas court would apply by stipulating to have a Texas court apply California law in deciding Verdugo's claims, but Alliantgroup failed to do so." Had Alliantgroup provided that disputes were to be heard in Texas, but that the Texas courts were required to apply California law, the result of the case likely would have been different.

(Editor's note, employees may attempt to use this decision to argue that Business and Professions Code section 16600 is a substantive right to challenge mandatory forum selection clauses contained in non-compete agreements with California employees)

Non-Compete That Grants An Employer The Right To Seek Injunctive Relief No Guarantee That Injunction Will Issue

By Paul E. Freehling (June 12, 2015)

A trial court declined to enter a preliminary injunction in a non-compete covenant case despite a provision in the covenant giving the employer the "right to seek injunctive relief in addition to any other remedy available to it." The decision was affirmed on appeal.

Summary of the case

A 20% owner of a pest control service company (referred to by the appellate court as "Yuma Pest"), his wife and his sister all were employees of the company. In late 2010 or early 2011, in settlement of a dispute the three of them had with Yuma Pest, the 20% ownership interest was relinquished, all three signed non-compete and non-solicitation covenants, they resigned, and they and Yuma Pest executed mutual releases. A few months later, they and several other former employees allegedly began to compete with the company. In June 2012, Yuma Pest sued and moved for issuance of a preliminary injunction. Twenty months later, following an evidentiary hearing, the motion was denied. The Arizona Court of Appeals affirmed. *Security Pest & Termite Systems v. Reyelts*, No. 1 CA-CV 14-0237 (May 14, 2015) (not for publication).

The covenant

In addition to the injunction clause, Yuma Pest's covenant provided that employees would not work in the pest control business within a 50-mile radius of the company's Yuma, Arizona headquarters for two years after termination.

The defendants

Prior to the settlement, Matthew Reyelts was the general manager and a one-fifth owner of Yuma Pest. His wife and his sister were the company's office manager and financial manager, respectively. A new company, RAM Pest Management, opened for business in Yuma five months after the settlement. Two months later, Matthew's wife and sister went to work for RAM. Subsequently, two other Yuma Pest employees, one of whom was Matthew's father, resigned and joined RAM. Matthew, who did not become employed by RAM, formed a company in Yuma known as "Bug Warrior" to provide education and training services related to pest control. Yuma Pest sued all of the above, alleging contract and tort claims.

The injunction hearing

The hearing commenced more than a year after the complaint was filed. By that time, several years had elapsed since the settlement. One of the witnesses at the hearing, Yuma Pest's general manager, testified that although customer cancellations had increased after the settlement, Yuma Pest's revenue did not decline. He added that he could calculate with reasonable certainty the damages the company sustained due to the defendants' competition. Seven months after the hearing began, the court ruled that an injunction was not warranted. It reasoned that (a) Yuma Pest had an adequate remedy at law, and (b) in light of the passage of several years between the alleged violation and the ruling on the motion, the company failed to show the likelihood of irreparable damage.

The decision on appeal

The primary basis for the trial court's judgment that Yuma Pest had an adequate remedy at law was, of course, the general manager's testimony. Further, according to the appellate tribunal, any inappropriate solicitation of Yuma Pest's customers has "already occurred." So, the lower court was held to have concluded correctly that the company failed to show that denial of an injunction would result in irreparable harm.

Takeaways

Yuma Pest's request for a preliminary injunction was problematic:

- *The covenant's mention of a* "*right to seek an injunction*." The lower court reasoned, and the Court of Appeals agreed, that the non-compete did not **require** entry of injunctive relief. Rather, it merely allowed such relief if — in the court's discretion — an injunction was deemed to be appropriate. Consider stating in a non-compete simply that the company has "the right to injunctive relief" in the instance of a covenant violation rather than that the company could "seek" injunctive relief.

- *Adequacy of a legal remedy.* A preliminary injunction often is entered against the violator of a non-compete. The reasoning is, in part, that a monetary award equal to losses already incurred will not suffice to make the injured party whole (for example, absent an injunction future losses also may be caused by the violation). Here, however, the injunction motion was denied partly because (a) the general manager testified that he would be able to compute Yuma Pest's damages with reasonable certainty, and (b) the complaint apparently failed to allege that the company sustained additional harm.

- *Delay*. The appeals court's opinion does not state who was responsible for the lengthy delay between the date Yuma Pest learned of the alleged violations and the date of the ruling on Yuma Pest's injunction motion. The jurists may have concluded that Yuma Pest was not diligent in its pursuit of injunctive relief.

Is An Offer Of At-Will Employment Adequate Consideration For A Non-Compete? Recent Court Rulings Split Three Ways

By Paul E. Freehling (June 30, 2015)

Three very recent decisions reflect the irreconcilable division of judicial authority regarding the adequacy of at-will employment as the sole consideration for an otherwise valid non-compete. *Compare (*a) Standard Register Co. v. Keala, No. 14-00291 (D. Haw., June 8, 2015) (adequate under Hawaii law) ("majority rule"), *with* (b) Hunn v. Dan Wilson Homes, Inc., Nos. 13-11297 and 14-10365 (5th Cir., June 15, 2015) (inadequate under Texas law) ("minority rule"), *with* (c) *McInnis v. OAG Motorcycle Ventures, Inc.*, 2015 IL App. (1st) 130097 (June 25, 2015) (2-1 ruling based on the *Fifield* rule) ("middle ground").

Status of the *Standard Register* case

Several at-will employees of Standard, a distributor of promotional marketing products, executed non-competes and then resigned and went to work for an alleged competitor. Standard sued them. Judge Seabright bifurcated and decided the adequacy-of-consideration issue. Although the non-competes contained an Ohio choice-of-law provision (Standard is an Ohio corporation), he held that Hawaii had the most significant relationship to the parties and the dispute. So, Hawaii law applied.

Hawaii's Supreme Court has not decided whether, under that state's law, "continuing at-will employment is, by itself, sufficient consideration for an otherwise reasonable non-competition agreement entered into during a term of employment (and not at the beginning of employment)." Judge Seabright observed that courts in several states hold that consideration in such a situation is insufficient, but "the clear majority position is to the contrary." The court concluded that "the Hawaii Supreme Court would not require additional consideration beyond continuing at-will employment."

Status of the *Hunn* case

Texas Bus. & Com. Code § 15.50(a), provides that "a covenant not to compete is enforceable if it is ancillary to or part of an otherwise enforceable agreement at the time the agreement is made." Lack, an at-will employee of Hunn's architectural design company, signed a non-compete. Lack transferred to his home computer from the company's computer a copy of confidential plans and specifications relating to a project on which Lack was working for a client of Hunn's (the company permitted employees to take files home to work on them). Then, Lack resigned, was hired by the client, and allegedly used the files to complete the project. Hunn sued Lack for breach of the non-compete, violating the Computer Fraud and Abuse Act, and unlawfully disclosing the company's confidential information to Hunn's client.

The Fifth Circuit held that a contract for at-will employment does not qualify as "an otherwise enforceable agreement" under the Texas statute "because the promise of continued employment in an at-will contract is illusory — neither the employer or employee is bound in any way." Therefore, the non-compete lacked consideration and was unenforceable under Texas law. That court also rejected Hunn's other claims (*see* below).

Status of the *McInnis* case

For three years, McInnis was an employee of OAG, selling Harley-Davison motorcycles. He quit OAG and went to work for a competitor for one day. He then returned to OAG which required him to sign a non-compete and confidentiality agreement as a condition of his re-employment. He resigned 18 months later and resumed employment with the competitor. OAG sued and sought an injunction. It was denied on the ground that the covenant lacked adequate consideration because he was an at-will employee employed for less than two years. A scathing dissent challenged the majority's rationale.

The conflict among the states

The majority position: According to Judge Seabright in *Standard Register*, courts in Maryland, Ohio, Vermont, and Wisconsin reason that an employer's forbearance in exercising a legal right — here, not terminating an at-will employee — is valid consideration for a non-competition covenant and is not illusory. Further, he referenced the Restatement Third of Employment Law (April 2014 Proposed Final Draft), § 8.06 comment *e*, and Reporters' Notes. Comment *e* asserts that "Continuing employment of an at-will employee is generally sufficient consideration to support the enforcement of an otherwise valid restrictive covenant." The Reporters' Notes to comment *e* cite rulings to this effect by courts in more than 20 states.

The minority position: Citing cases from Minnesota, South Carolina, and Washington, Judge Seabright said that several jurisdictions hold that "continued at-will employment, standing alone, is insufficient consideration for a non-competition agreement entered into during current employment." He said that the Restatement Third of Employment Law identifies six jurisdictions, besides those three, that concur with the minority view.

Middle ground: According to Judge Seabright, the Restatement identifies eight states — including Illinois — that endorse a middle ground, namely, that consideration is sufficient only if the employee is retained for a substantial period after the non-compete is signed. A leading Illinois case (there is no Supreme Court decision directly on point) is*Fifield v. Premier Dealer Services, Inc.*, 2013 Ill. App. (1st) 120327, holding that continuous employment for two years or more constitutes reasonable consideration for a restrictive covenant. The majority in *McGinnis* followed that ruling.

Justice Ellis, dissenting, rejected as indefensible a bright-line two-year rule. He insisted that a determination of the adequacy of consideration requires a case-by-case analysis in order to protect "at-will employees from the whim of the employer." Here, in his view, it was relevant that McGinnis signed the covenant at the time he was hired, that the period of McGinnis's post-covenant employment (18 months) was substantial, and that he left OAG voluntarily. The jurist said he could understand the term "additional consideration" in the instance of an existing employee but questioned the logic of requiring "additional compensation" — additional to what? — for a newly hired employee. He also noted that three of the four federal judges deciding post-*Fifield* cases predicted that the Illinois Supreme Court would reject the bright-line rule.

Two other issues in *Hunn*

CFAA. One count of Hunn's complaint against Lack accused him of violating the Computer Fraud and Abuse Act. The appellate tribunal held that since Lack was employed by Hunn when he transferred the files to his home computer, and since employees were permitted to transfer files to their home computers, Lack did not exceed authorized computer access. Therefore, there was no CFAA violation.

Disclosure of trade secrets and other confidential information. Hunn accused Lack of post-employment disclosure of Hunn's confidential plans and specifications. But the Fifth Circuit disagreed because the plans had been disclosed to the client with Hunn's consent — through its agent, Lack — during Lack's employment by Hunn.

Takeaways

1. *Consideration.* Determination of the sufficiency of consideration for a non-compete executed by an at-will employee may turn on which state's law applies. If the relevant facts and circumstances permit, an employer should include a choice-of-law provision designating the law of a state where at-will employment is adequate consideration. However, as the *Hunn* case illustrates, choice-of-law clauses are not always honored.

2. *Confidential information.* An employer who gives employees access to confidential information should require them to sign written commitments (a) to return or delete the information promptly after termination of employment, and (b) under no circumstances to use or disclose the information other than in furtherance of the employer's business.

Non-Compete Injunction Denied, Ninth Circuit Remands For Reconsideration, But District Court Denies It Again, Declines Equitable Tolling

By Paul E. Freehling (July 10, 2015)

As directed by the court of appeals, a district court judge reconsidered his denial of a non-compete covenant case injunction but reached the same result on reconsideration. He also stated why he would not have extended the covenant's expiration date even if he had been inclined to enter the injunction. *Ocean Beauty Seafoods LLC v. Pacific Seafood Group Acquisition Co.*, No. C14-1072 (W.D.Wash., Oct. 30, 2014) (Ricardo S. Martinez, J.), *remanded*, No. 14-35950 (9th Cir., May 8, 2015), *on remand*, (W.D. Wash., June 25, 2015).

Status of the case

Last October, a federal district court judge in Seattle denied a motion for preliminary injunction in a lawsuit alleging violation of a non-competition covenant. The unsuccessful movant appealed to the Ninth Circuit Court of Appeals. Concluding that the lower court had made a number of factual, legal and procedural errors, the appellate court remanded for the district court's reconsideration. Last month, the Seattle judge again declined to issue an injunction order. He also explained why, if he had issued the order, he would not have equitably tolled expiration of the one-year covenant.

Background

When Michael Coulston first became a Pacific Seafood employee in January 2011, he signed a covenant barring him, for 12 months after termination, from engaging in business with a competitor of the company in any "geographic area" in which it does business. The covenant was governed by Oregon law. In July 2014, he left Pacific and went to work for Ocean Beauty. Both companies are seafood processors and distributors on the West Coast. Pacific sued Ocean Beauty and Coulston.

Judge Martinez's initial denial of a preliminary injunction

In his 2014 decision, Judge Martinez determined that Pacific Seafood (a) had failed to demonstrate a likelihood of success on the merits of its claim against Ocean Beauty and Coulston, and (b) had failed to show that it would sustain irreparable harm absent injunctive relief. There was no definition of "geographic area" in the covenant. The judge said it appeared to encompass the entire west coast of the U.S. which he found to be unreasonable since Coulston had a more limited territory. Moreover, Judge Martinez held that Coulston was not shown to have diverted, or was likely to divert, any business to Ocean Beauty based on his knowledge of Pacific's business practices.

The Ninth Circuit's decision

Marked as a "Memorandum" and "Not for Publication," the appellate court's ruling took issue with Judge Martinez's findings, conclusions and denial of Pacific Seafood's motion to supplement the record. According to the appeals court, Coulston's territory while he worked for Pacific was more extensive than the district court indicated and, moreover, Oregon law does not render a covenant automatically unenforceable even if it covers an overly broad territory. Further, Pacific was held to have a protectable interest in information Coulston possessed regarding Pacific's "marketing plans and product allocation." The Ninth Circuit also noted that the trial court seemingly did not appreciate the difference between evidence of *actual* harm and a showing of *a likelihood* of harm. The trial court's denial of Pacific's motion to supplement the record was said to be an abuse of discretion as well. The case was remanded to Judge Martinez for reconsideration. Finally, in a footnote, the appellate court directed the district court, if it grants a preliminary injunction, to consider equitably extending the non-compete's one-year term.

Judge Martinez's second denial of an injunction

On remand, the judge said he "remains unconvinced" that "the geographic scope of the non-compete agreement is reasonable." Further, he stated that the record before him did not persuade him that "there is a substantial risk Ocean Beauty would be able to divert a significant part of Pacific Seafood's business given Mr. Coulston's knowledge" or that he was "likely to divert business to Ocean Beauty based on any such knowledge." So, Judge Martinez again found a failure by Pacific to show that it would suffer irreparable harm in the absence of an injunction.

In light of the Ninth Circuit's footnote, and recognizing that the appellate court might disagree with his second denial of an injunction, Judge Martinez discussed equitable tolling. The issue potentially was relevant because of the imminent expiration of Coulston's one-year non-compete. The judge noted that the Oregon Supreme Court, the Ninth Circuit and many other courts of appeal have declined to extend a covenant that has expired or is about to expire, and he said that the record before him warranted a similar ruling in this case.

Takeaways

Counsel drafting, seeking to enforce, or defending against an effort to enforce, a non-compete should consider the following:

- *Equitable tolling*. A non-competition agreement often expresses the parties' intent that the employer shall be entitled to an extension of the injunction period equal to the length of time during which the ex-employee engaged in illicit competition. The non-compete in the *Ocean Beauty* litigation did not include such a provision. Arguably, Pacific Seafood's request for tolling asked the court to amend the covenant by adding a term to which Coulston had not consented. But a contrary contention could be made: assuming the covenant was enforceable, failure equitably to toll would deprive Pacific of the benefit of its bargain which was for 12 months' freedom from Coulston's competition. A party seeking equitable tolling should present persuasive, admissible evidence justifying an extension of the non-compete period.

- *Geographic scope and time limit of the non-compete*. Larger and longer are not necessarily preferable when it comes to the area and temporal provisions set forth in a restrictive covenant. If excessive, they may cause unenforceability. Geographic scope and time limit terms may approach, but they should never exceed, the maximums that are *reasonable* under the circumstances.

Trading Secrets

- *Be gracious to a judge whose prior opinion has been remanded for reconsideration*. Judge Martinez emphasized that he disagreed with the appellate court's order, and he did not take kindly to what he viewed as Pacific Seafood rubbing his face in the remand order. His second opinion expressed annoyance — to say the least — at what he called Pacific's "rejoic[ing] in reiterating the numerous 'errors' found by the Ninth Circuit." He also took "exception to the tone" of Pacific's briefs and Pacific's "apparent lack of respect for this Court and its prior findings." If Pacific wanted to generate sympathy for its legal position, understatement might have been more effective. However, he might have reached the same result in any event.

50 State Non-Compete and Trade Secret Desktop Reference

By Robert B. Milligan (July 22, 2015)

Seyfarth Offers 2015-2016 Edition of 50 State Desktop Reference: 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 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's one-stop Desktop Reference surveys the most asked questions related to the use of covenants and intellectual capital protection in all fifty states. For the company executive, in-house counsel, or HR professional, we hope 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 in hard copy or eBook format (compatible with PCs, Macs and most major mobile devices). The eBook is fully searchable and offers the ability to bookmark useful sections and make notations for easy future reference.

To request the 2015-2016 Edition of 50 State Desktop Reference in eBook or hard copy, please click the button below:

Request eBook now

Trading Secrets

No Economic Recovery Available For Breach Of A Non-Compete Set Forth In A Distributorship Agreement Which Bars Damages Awards

By Robert B. Milligan and Paul E. Freehling (July 27, 2015)

Where a freely negotiated contract between two sophisticated companies included a provision barring an award of monetary relief for breach of contract, the court will enforce the provision as written and award no economic damages. *CH2O, Inc. v. Meras Engineering, Inc.*, No. 45728-8-II (Wash. App. Court, July 21, 2015) (unpublished opinion).

Status of the Case

A non-exclusive distributorship agreement between CH2O, a California water treatment company, and Meras, a Washington State competitor, provided for CH2O's sales of specified products to Meras for resale to certain of its *existing* customers. The agreement's non-compete clause prohibited sales by Meras of products similar to those made by CH2O but manufactured by its competitors. Further, Meras was required to refer to CH2O inquiries regarding, and requests for, CH2O's products from *potential* customers. Section 9 of the agreement stated that neither of the parties would be liable to the other for economic damages arising out of a breach of the agreement. CH2O sued Meras in a Washington state court, seeking economic damages for breach of contract, for allegedly selling products similar to CH2O's products to CH2O's customers. The lower court granted summary judgment to Meras. CH2O appealed. A few days ago, the state's appellate court affirmed.

CH2O's Contentions

CH2O maintained that the lower court's interpretation of Section 9 rendered other contractual obligations illusory. For example, Section 6(a) obligated Meras to use its best efforts to sell the identified CH2O products to designated California customers. Section 13 contained a *force majeure* provision, disclaiming liability of one contracting party to the other for events beyond the parties' control. Further, CH2O contended that the court's interpretation of Section 9 was inconsistent with Section 18 which provided for an award of costs and attorneys' fees for a prevailing party in a dispute concerning the agreement. CH2O insisted that Section 9 only excluded one party's liability to the other with respect to third party claims brought against one of them by, for example, customers.

The Ruling on Appeal

The appellate court agreed with Meras that Section 9 contained an express, unambiguous and universal waiver of the parties' liability to each other for economic damages resulting from a breach of the agreement, regardless of what caused the damages. But a lawsuit for breach of contract was not precluded so long as only noneconomic recovery — for example, asking for specific performance or a declaratory judgment — was sought. Consistent with the court's effort to reconcile Sections 9 and 18, it

said that by means of Section 18 the parties carved out from the damages exclusion recovery of attorneys' fees and costs for prevailing in a contract action seeking only equitable relief.

CH2O maintained that the court misconstrued the parties' intent as to the meaning of Section 9. Finding Section 9 to be unambiguous, the court declined to interpret it based on evidence outside the four corners of that section. (Interestingly, however, the court went on to surmise that perhaps the reason for Section 9's exclusion of monetary damages was that, as business partners, the companies "depend on each other's financial stability to execute a successful business strategy.")

Takeaways

Although Section 9 might appear to be strange, it left little room for interpretation. The appeals court found that both companies engaged in drafting and negotiating their contract. Therefore, the court concluded that Section 9 should be enforced precisely as written. The lesson is that a party acts at its peril by assuming that a contract provision will be interpreted by a court to incorporate terms not actually included.

These two companies have litigated against each other before. Meras' employment of several CH2O's employees, who allegedly were subject to non-compete agreements with CH2O, was the subject of Northern District of California court rulings in August 2012 and January 2013. In that litigation, Meras and the employees sued in California, seeking a determination that the non-competes were void (separately, CH2O sued the employees in Washington to enforce the agreements). The California federal court held that because the employees' non-compete clauses required litigation in a Washington court construing the clauses under Washington (not California) law, the California lawsuit must be dismissed. That holding was the subject of a Seyfarth Shaw blog in February 2013.

Court Decries Ambiguity Of Terminology Used In Non-Compete Agreement And Injunction

By Paul E. Freehling (August 10, 2015)

A preliminary injunction was entered against a fired executive of a roofer who, immediately after he was discharged, went to work for an alleged competitor. The district court held, and the Seventh Circuit agreed, that his non-compete and non-solicit agreements were overbroad and confusing, but that some injunctive relief nonetheless was warranted in this case. *Turnell v. CentiMark Corp.*, No. 14-2758 (7th Cir., July 29, 2015).

Summary of the Case

Turnell joined CentiMark, a national roofing product and servicing company, as a laborer and rose to Senior Vice President and Midwest Regional Manager. Contemporaneously with one of his promotions and salary increases, he signed non-compete and non-solicit agreements required of management-level personnel. He was terminated 25 years later for alleged misconduct and immediately was hired by Woodward, a small Chicago-area roofer. CentiMark sued Turnell for breach of contract, and he sued the company for employment discrimination. The company moved for entry of a preliminary injunction. Applying Pennsylvania law (the agreements so specified as CentiMark is incorporated and headquartered there), the district court judge blue-penciled the covenants and enjoined him but only to the extent she determined to be "reasonably necessary" to protect CentiMark. Recently, on Turnell's interlocutory appeal, her ruling was affirmed.

The Covenants

Both the non-compete and the non-solicit lasted for two years after termination. Both provided for tolling during any period of competition.

The non-competition provision prohibited engaging "in any competing business" to that of CentiMark. "Competing business" was defined as selling the same or "similar" products to those sold by CentiMark. The geographic scope of the provision was wherever he had "operated" as a CentiMark employee.

The non-solicitation clause forbad soliciting "competing business" both from CentiMark's customers or suppliers, and from its "prospective customers or suppliers." The term "prospective customers" was defined as anyone "contacted" by CentiMark during specified periods. The clause contained no geographic limit.

The District Court's Rulings

CentiMark asked the district court judge to bar Turnell from performing any work for Windward, but she deemed that request unreasonable. However, she also declined to enter the order Turnell sought which would have invalidated the covenants altogether as overbroad and oppressive.

Even though CentiMark's and Windward's sales territories and roofing product lines were far from identical, the district court held that the companies were competitors. But the court modified the prohibition in the non-solicitation clause against marketing to CentiMark's "prospective customers" who CentiMark has "contacted." Her reasons, as summarized by the Seventh Circuit, were that the prohibition was "too vague (what kinds of contact count?), too broad (what relationship can CentiMark legitimately seek to safeguard with a prospect it merely called a few years ago?), and impractical (Turnell cannot know everyone his former employer contacted)." Instead, the injunction ordered him, for two years from the date of issuance, not to sell, attempt to sell, or help to sell products or services related to "commercial roofing." Even though his territory had covered the entirety of four states and only parts of three others, the injunction applied to any actual customer of CentiMark as of the date he was fired who was located anywhere in those seven states. CentiMark was required to post a $250,000 bond.

Opinion on Appeal

The Seventh Circuit explained that the only issues on appeal were (a) the likelihood of CentiMark prevailing in its effort to enforce the covenants, and (b) the balance of potential harms to the parties. Turnell did not challenge on appeal the scope of the injunction, just the fact that it was issued at all. So, some of the panel's comments concerning the ambiguity of scope terms used in the covenant might seem to be dicta. However, in a footnote the panel *directed* the district court judge to consider those comments if she chose "to modify the preliminary injunction" and "when and if [she] issues a permanent injunction."

Noting that Pennsylvania jurists have discretion to blue-pencil but also to refuse to enforce an oppressive covenant, the appeals court stated that "Not every overbroad covenant is oppressive . . .. In many cases, overbreadth has a more benign cause (such as poor drafting)." Here, the covenants' purported coverage of products and services "similar" to CentiMark's was acceptable although it "might benefit from more precision (what counts as similar?) or a narrower focus (similar products do not necessarily compete)." The restriction to locales where Turnell "operated" as a CentiMark employee also was criticized as imprecise but acceptable, and he was "free to work in other product and geographical markets."

In the Seventh Circuit's view, the district court judge "could have narrowed Turnell's restrictive covenants even further than [she] did." For example, the prohibition against selling "'commercial roofing' is too broad, as CentiMark sells a more specific [product:] commercial flat single-ply roofing." Further, the injunction need not have pertained to the entirety of seven states because, with respect to three of them, Turnell's territory only encompassed a portion. But, recognizing that the covenants were executed a quarter-century earlier, and that neither the company nor Turnell could have anticipated precisely what the two of them would be doing many years later, the appeals court held that the covenants were "overbroad but not oppressively so." In sum, the district court judge "exercised [her] equitable discretion under Pennsylvania law to blue pencil the restrictions . . . and properly concluded that CentiMark has a strong chance of enforcing them, as narrowed." Finally, "the balance of harms favors Turnell, if at all, only slightly. It is not enough to overcome CentiMark's likelihood of success on the merits."

Takeaways

The lesson of this case is that employers and their attorneys should take care in choosing the words and phrases used in restrictive covenants. The terms "competing business," "similar products," places where an employee "operated," "prospective customers," and potential customers who were "contacted" all were held to be ambiguous. Further, two companies are not necessarily "competitors"

just because they have some product overlap. Also, trying to extend the reach of a covenant beyond the territory where the employee actually worked may make a covenant unenforceable. A court, particularly one in a jurisdiction that does not permit blue-penciling, might conclude that the former employer's use of vague terms such as these renders a non-compete or non-solicit so oppressive as to warrant its invalidation.

Effective Carve-Outs to Seek Injunctive Relief from the Court in Arbitration Provisions

By Alex Meier (August 12, 2015)

Christopher Pike: "That's a technicality."

Spock: "I am a [lawyer], sir. We embrace technicalities."

Star Trek Into Darkness

Arbitration is no longer the final frontier. Instead, arbitration is often the first and only forum for resolving disputes. The business community has embraced arbitration as an alternative method of dispute resolution, but sophisticated parties still maintain a preference favoring court resolution of disputes involving preliminary and injunctive relief.

What someone *wants* and what someone *agrees to*, however, can vary drastically. Including an arbitration carve-out for preliminary injunctive relief is extremely common, but will the court honor it?

This issue arises at the intersection of two different provisions in an arbitration agreement: the carve-out to an arbitration provision and the delegation provision. The carve-out typically excludes certain disputes from arbitration, such as:

- Example: "The Parties agree to resolve any dispute, controversy or claim that arises during the course of the Parties' Agreement. If the Parties are unable to resolve a dispute, the dispute, *other than a dispute relating to the breach of the confidentiality provision* of this Agreement, shall be subject to final and binding arbitration by a single arbitrator."

- Example: "Any dispute arising out of or in connection with this Agreement shall be referred to and finally resolved by arbitration before a single arbitrator. The foregoing, however, *shall not* preclude the parties from applying for any preliminary or injunctive remedies available under applicable laws for any purpose."

The delegation provision is a statement by the parties about *who decides* whether a dispute is arbitrable, usually indicated by:

- A statement expressly reserving questions about the scope of arbitration for the arbitrator.

    - Example: "Any dispute arising out of or in connection with the arbitration provision of this Agreement, including any questions *regarding its existence, validity or termination*, shall be referred to and finally resolved by the arbitrator."

- Incorporating the Rules of the American Arbitration Association ("AAA") or another arbitration organization's rules that reserve disputes over the scope of an arbitration provision for the arbitrator.

    - Example: "The Parties agree that any dispute regarding the interpretation or enforcement of this Agreement shall be resolved by binding arbitration *according to the rules of the American Arbitration Association*."

So what happens if an arbitration provision includes both a carve-out for preliminary injunctive relief and a delegation provision? According to several recent cases in the Eleventh Circuit, everything goes to arbitration, even claims expressly carved out by the parties.

The anomaly occurs because of the order in which the court must address what it has the authority to decide and what is reserved for the arbitrator.

The court begins by assessing whether questions about the *scope or applicability* of the arbitration provision may be addressed by the court. The default setting is that the court retains the authority to decide "questions of arbitrability." The parties, however, have the ability to reassign that authority from the court to the arbitrator. Doing so means that the arbitrator decides whether a dispute should be in arbitration *and* the merits of any dispute subject to arbitration.

The delegation provision trumps any carve-out. If questions of arbitrability are reserved for the arbitrator, then the court cannot address claims within the carve-out unless both parties agree that the carve-out claims may be brought in court.

But any dispute about whether a claim is arbitrable or carved out obliterates the court's authority to address the claim because questions of arbitrability must be heard by the arbitrator.

A recent case in the Northern District of Georgia demonstrates how a delegation provision stopped a former employer from enforcing non-compete and non-disclosure provisions against a former employee.

In *Cellairis, Inc. v. Duarte*, Case No. 2:15-cv-101-WCO (N.D. Ga. 2015), a cell phone kiosk franchisor filed a preliminary injunction to enforce non-compete and non-disclosure provisions against a former employee. The agreement contained an arbitration clause that sent everything to arbitration except for a few disputes where irreparable harm could result, like a confidentiality or non-compete violation.

But the agreement also contained a delegation provision, which unequivocally provided that *all disputes* over the scope of the arbitration clause must be decided by the arbitrator.

Even though the franchisor had some very compelling evidence that its former employee was competing in the same industry and violating the scope of the non-compete agreement, the court found that it lacked the authority to enjoin the employee because the arbitrator had to first decide whether a request for preliminary injunctive relief qualified as a "request for preliminary injunctive relief."

Because the franchisor overlooked the effect of the delegation provision on its ability to bring an action in court, the franchisor wasted time and money seeking relief the court could not provide. Instead, after several weeks, the franchisor left the court with nothing more than an order to initiate arbitration proceedings.

Trading Secrets

NOTES FOR THE CAPTAIN'S LOG

- If your agreements contain carve-outs in any form *and* either incorporate the AAA Rules *or* expressly delegate questions of arbitrability to the arbitrator, consider placing a "carve-out" in the delegation provision allowing the court to decide whether a dispute falls within the arbitration carve-out.

- If you are involved or about to be involved in a dispute over an agreement with this issue, it may be more cost-effective and efficient to simply start in arbitration and decide scope issues in that forum. Otherwise, you run the risk of spending precious time arguing about whether the court can even consider your request for relief in the first place–let alone decide it.

Webinar Recap! State Specific Non-Compete Oddities Employers Should Be Aware Of

By Michael Baniak and Paul E. Freehling (August 20, 2015)

We are pleased to announce the webinar "State Specific Non-Compete Oddities Employers Should Be Aware Of " is now available as a podcast and webinar recording.

In Seyfarth's sixth installment, attorneys Michael Baniak and Paul Freehling 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. As trade secrets and non-compete laws continue to evolve from state to state in piecemeal fashion, companies should continually revisit their trade secrets and non-compete strategies in light of the evolving legal landscape and legislative trends.

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

- Enforceability of non-compete, non-solicit, and confidentiality covenants in employment agreements depends primarily on the applicable statutes, and pertinent judicial decisions and conflict of laws principles, regarding (a) the acceptable breadth of such covenants, and (b) appropriate balancing of the legitimate business interests of employers, employees, and the public; enforceability requires constant vigilance in updating the covenants as the law, business and employment evolve, often very rapidly.

- Because each jurisdiction's version of the Uniform Trade Secrets Act as enacted — it has been adopted in one form or another in the District of Columbia and each of the 50 states except New York and Massachusetts– is unique, all relevant jurisdictions' versions must be analyzed.

- Oddities in the law of restrictive covenants include the following: (a) hostility in a few states to non-competes and/or non-solicit covenants in general, (b) in some states (whether by statutory provision or judicial fiat), certain employees are exempt from such covenants, (c) there are disparities in various courts' willingness to "blue pencil," reform, or invalidate covenants deemed overbroad as written, and (d) there are variations in different courts' views as to whether only actual disclosure, or also threatened or inevitable disclosure, of trade secret or confidential information will be enjoined.

Trend In The Courts: It's Getting Harder To Obtain Preliminary Injunctions In Restrictive Covenant Cases

By Paul E. Freehling (November 19, 2015)

In recent weeks, courts almost routinely have been denying preliminary injunctive relief in cases alleging violation of non-compete and similar employment agreements. Three examples: *Burleigh v. Center Point Contractors*, 2015 Ark. App. 615 (Oct. 28, 2015); *Evans v. Generic Solution Engineering, LLC*, Case No. 5D15-578 (Fla. App., Oct. 30, 2015); and *Great Lakes Home Health Services Inc. v. Crissman*, No. 15-cv-11053 (E.D. Mich., Nov. 2, 2015).

Status of those cases

In each of those cases, injunctions were denied or, if granted by a lower court, the order was reversed.

Burleigh. When he was employed in 2012 by Center Point, a general commercial construction company, Burleigh had more than 10 years of experience in construction in northwest Arkansas. His title was operations manager and estimator. He signed non-compete (two years, within a radius of 50 miles from Bentonville, Arkansas), non-solicitation, and confidentiality covenants. In 2014, he resigned and formed, with a friend, a competitor of Center Point.

Center Point sued Burleigh. His motion to dismiss the complaint was denied, and Center Point sought a preliminary injunction. The trial court granted the injunction including two additions to the non-compete agreement: (a) the court required Burleigh to give Center Point notice of and details concerning any prospective business activity that would compete with activities in which he was engaged on or before the date he resigned, and (b) Center Point was ordered to post a $50,000 bond. He appealed.

The Arkansas Appellate Court reversed and remanded. It held that Center Point failed to demonstrate a likelihood of success on the merits. According to the court, there was no evidence that Center Point provided Burleigh with any "special training," "proprietary formulas," "trade secrets," "confidential business information," or "a secret customer list." Further, Center Point did not show that he learned anything at Center Point that would give him an unfair advantage in the bidding process. Therefore, "Center Point did not have a legitimate interest to be protected by agreement, and the non-compete agreement only shielded Center Point from ordinary competition."

Evans v. Generic. In order for a former employer to prevail in a suit under Florida law based on a non-competition covenant, enforcement of the covenant must be shown to be necessary in order to protect the former employer's "legitimate business interests." Reaching a decision similar to that in *Center Point*, the Florida Appellate Court held that the former employer failed to make the requisite showing.

The former employer, Tech Guys, builds online sales and marketing systems. It does not have employees, preferring instead to retain independent contractors. One of them was Chinn who had signed a restrictive covenant prohibiting, for two years after termination of his relationship with Tech

Guys, work for current or former Tech Guys clients. While working for Tech Guys, Chinn assisted one of its significant clients, RRI, which had a three-year non-exclusive contract for services.

When Chinn left Tech Guys, he and another ex-Tech Guys independent contractor — but one who had not signed restrictive agreements — formed a competitor. After RRI's contract with Tech Guys expired, RRI offered to continue to use Tech Guys (although not exclusively). The offer was declined. When RRI became a client of Chinn's new company, Tech Guys sued Chinn and his company and obtained a preliminary injunction.

The defendants appealed, and the appellate court reversed. According to the appellate tribunal, the "facts are insufficient to support the trial court's finding of a substantial business relationship in need of protection."

Great Lakes Home. Great Lakes is a home-health and hospice provider. Crissman was vice-president for operations and planning in Michigan. At the time of her employment, she signed non-competition, non-solicitation, and confidentiality covenants. Pursuant to the agreements, she promised that for two years after termination, she would not divert or attempt to divert from Great Lakes business opportunities in any county where Great Lakes was Medicare-certified on the date she was employed by Great Lakes.

Eighteen months after leaving Great Lakes, Crissman accepted a position with a competitor. Her responsibilities included work in various states but not in any county where Great Lakes does business. Great Lakes sued her and sought a preliminary injunction. Judge Rosen authored a detailed must-read opinion, clearly laying out Michigan law on the subject and explaining in detail why injunctive relief was denied.

Confidentiality. Great Lakes contended the court could presume that Crissman disclosed Great Lakes' confidential information. Crissman rebutted the presumption by submitting a signed and sworn denial that she had made any improper disclosures and describing in detail the firewall established with her new employer that precluded any disclosures.

Non-compete. Great Lakes argued that Crissman was liable for non-compete covenant violations because of her employment by a competitor that was servicing areas where Great Lakes operated. There was no allegation that Crissman, personally, violated the covenant. The parties agreed that her new employer did provide services competitive to those offered by Great Lakes even though there was no evidence that she participated. The court concluded that Great Lakes' interpretation of the covenant would preclude her "from working in *any* capacity, in *any*location, with a competitor as defined in the Agreement" (emphasis in the original). That interpretation was held to violate Michigan law which provides that "'non-competition agreements must be tailored so that the scope of the agreement is *no greater than is reasonably necessary* to protect the employer's legitimate business interests'" (quoting from an earlier Michigan district court case but adding the emphasis).

Extension of the non-compete agreement. Judge Rosen observed that enforcement of the non-compete agreement would require extending its duration since, by its terms, it expired in August 2015. Although conceding that Great Lakes had been diligent in seeking injunctive relief, he pointed to Michigan law restricting extension of such covenants to "the most extreme circumstances." Here, he held, there was "no clear 'flouting' of the Agreement or bad faith." Accordingly, Great Lakes had failed to demonstrate a likelihood of success on the merits.

Takeaways

These cases, and other similar recent decisions, indicate that courts are reluctant to enter preliminary injunctions for alleged violations of employment agreements. Even if the non-compete time period and geographic area are reasonable, a mere showing that the ex-employee went to work for a competitor during that period and within that area may no longer be sufficient. Rather, the moving party seemingly will have to demonstrate clearly that the ex-employee him- or herself caused damages by poaching significant customers, hiring away invaluable workers, or disclosing highly confidential information.

Trading Secrets

Do Non-Competes Really Stifle Tech Innovation?

By Dawn Mertineit and Dallin Wilson (November 20, 2015)

As has been well-chronicled in this blog, Massachusetts and many other states (and even the federal government) have been grappling with proposed legislation that would ban or severely limit non-competes in employment contracts. Proponents of bans on non-competes claim that they stifle innovation in the technology sector by preventing skilled employees from using their unique talents to start new businesses or helping young, developing companies introduce new products or technology to the market. However, a debate continues to rage regarding whether there is any evidence that non-competes negatively impact technology innovation.

As we've discussed on this blog, Hawaii recently passed legislation that specifically prohibits non-competes "in any employment contract relating to an employee of a technology business." The Hawaii legislature stated that non-competes impose a "special hardship on employees of technology businesses" and "unduly restrict future employment opportunities for technology workers and have a chilling effect on the creation of new technology businesses within the State by innovative employees." In fact, the legislation specifically references "academic studies [that] have concluded that embracing employee mobility is a superior strategy for nurturing an innovation based economy."

But do "academic studies" actually support such a position? The results are mixed. Some studies have found that high employee mobility and short job tenure is positive for productivity in firms that spend on R&D, based on a variety of factors (including the spread of knowledge by mobile employees, greater incentives to create knowledge, and more dynamic labor markets). On the other hand, another study found that companies in non-compete jurisdictions that enforced non-competes enjoyed reduced research and development costs through knowledge retention and investment in human capital. Similarly, another study found that banning non-competes in the biotechnology industry would actually harm research productivity. In short, there is no consensus on the impact non-competes have on innovation and productivity.

Non-compete opponents also point to the decline in innovation within Massachusetts' Route 128 area during the 1970s, while at the same time Silicon Valley was having relative success. While one study concluded that California's ban on non-competes was a factor in the success of Silicon Valley over Route 128, other commenters haven't been quite as sure. For example, Matthew Max, an MIT professor focused on tech innovation and entrepreneurship, thinks that it's premature to conclude that the elimination of non-competes results in more innovation. Similarly, in her book,"Regional Advantage," AnnaLee Saxenian argues that Silicon Valley's advantage was primarily caused by cultural and structural differences between the East Coast and West Coast, resulting in Silicon Valley developing a decentralized but cooperative industrial system, while Route 128 came to be dominated by independent, self-sufficient corporations.

Recent growth in the technology sectors of various cities and states also challenges the assertion that the presence of non-competes stifles innovation. Some of the fastest growing tech sectors are in states that enforce non-competes, including Utah's Wasatch Front; Austin, Texas; and the research triangle in

North Carolina. Commenters suggest that these locations have certain characteristics that make them more attractive than Silicon Valley to tech companies such as better infrastructure, more business-friendly state and local governments, and lower costs of doing business.

Although the Hawaii legislature was satisfied that non-competes limit mobility and stifle innovation, others have not been convinced, particularly those that do not share Hawaii's unique geography, which makes it particularly difficult for employees on one particular island to find non-offending jobs without leaving the island completely. As states continue to debate the impact of non-competes on tech innovation and the economy as a whole, perhaps more empirical studies will provide guidance one way or the other. Until then, it seems that the debate will continue in statehouses throughout the country.

Pennsylvania Supreme Court Rules That Continued Employment Is Not Sufficient Consideration for Non-Competes Entered Into After the Employment Relationship Has Begun

By Paul E. Freehling and Robert B. Milligan (November 20, 2015)

In a landmark ruling of first impression, the Pennsylvania Supreme Court recently held that an employer's non-competition covenant, which included the employee's pledge not to challenge the covenant for inadequate consideration, is unenforceable unless it is accompanied by a change in job status or some other significant benefit. *Socko v. Mid-Atlantic Systems of CPA, Inc.*, Case No. 3-40-2015 (Nov. 18, 2015), *aff'g* 2014 Pa. Super. 103 (May 13, 2014), which affirmed 2012 WL 12248901 (Pa. Com. Pl., Oct. 17, 2012).

The non-competes

Socko was a salesman for Mid-Atlantic, a basement waterproofing company. In 2007 and 2009, he signed two-year employment agreements each of which contained a non-competition covenant for two years after termination. In 2010, Mid-Atlantic required him to sign a third non-compete. It was more restrictive, expressly superseded the other two, and prohibited competition for two years anywhere Mid-Atlantic did business.

The lawsuit

Shortly after resigning in January 2012, Socko became employed by a competitor. When Mid-Atlantic provided to the new employer a copy of his third non-compete covenant, Socko was discharged. He sued Mid-Atlantic and sought, among other relief, a declaratory judgment that the covenant was unenforceable for lack of consideration.

Pennsylvania's Uniform Written Obligations Act ("UWOA")

Pennsylvania's Uniform Written Obligations Act ("UWOA") provides that an agreement in writing "shall not be invalid or unenforceable for lack of consideration if the writing also contains an additional express statement, in any form of language, that the signer intends to be legally bound." Significantly, Socko's third non-compete contained the parties' express commitment to be "legally bound."

Lower courts' rulings

Relying on a 1991 Pennsylvania mid-level appellate decision which invalidated a restrictive covenant executed by an employee who received no benefit other than continuing employment, the trial court held that Socko's covenant was invalid. Mid-Atlantic appealed, but to no avail. The appellate tribunal observed that a contract without benefit to one of the parties but signed under "seal" has been deemed to be invalid for lack of adequate consideration. The court reasoned that an agreement's inclusion of

the intent "to be legally bound" language in the UWOA provided Socko with no benefit more valuable than a seal. Therefore, the covenant was unenforceable for lack of consideration. Mid-Atlantic appealed to the Supreme Court.

Arguments in the Supreme Court

Mid-Atlantic stressed that, as a matter of law, the UWOA barred Socko from challenging the validity of the covenant for inadequate consideration. Asserting that the statute is unambiguous and contains no exceptions, Mid-Atlantic insisted that the lower courts' rulings in Socko's favor effectively constituted amending the UWOA, thereby legislating under the guise of statutory interpretation. Socko countered that Mid-Atlantic's contentions ignored the public policy inherent in decisions invalidating restrictive covenants executed after the commencement of employment without substantial benefit to the employee.

The Supreme Court's affirmance, with one Justice dissenting

Majority decision. The Court said that **an exchange of consideration** is crucial to the enforceability of all contracts. Moreover, the analysis of non-compete covenants in the employer-employee context is unique and requires rigorous scrutiny. Therefore, since the UWOA does not provide expressly that it applies to employment-related covenants, it cannot reasonably be interpreted as abrogating the need for benefits to a continuing employee executing a non-compete. (**This decision does not alter the pre-existing rule that new employment is adequate consideration for a non-compete.** *See, e.g.,* II Malsberger, "Covenants Not to Compete" 4249-55 (10th ed. 2015) (citing *Geisinger Clinic v. Di Cuccio*, 606 A.2d 509, 513 (Pa. Super. Ct. 1992).)

Dissent. One justice, agreeing with Mid-Atlantic, emphasized that the statute is unambiguous, contains no exemptions, and clearly was made applicable to Socko's employment agreement by inclusion of the "legally bound" phrase. In the justice's view, Socko forfeited his right to challenge the agreement for lack of consideration.

Takeaways

First, the decision reaffirms that Pennsylvania law mandates payment of significant consideration to a continuing employee who signs a non-compete. Otherwise, the covenant is not enforceable. Similarly, the Adequacy of the consideration for a non-competition promise recently has attracted some courts' attention. *See, e.g., Fifield v. Premier Dealer Services,* 993 N.E.2d 938 (Ill. App., 1st Dist., 2013), and its progeny.

Second, the Pennsylvania Supreme Court seems to have emasculated the present version of the UWOA insofar as it pertains to restrictive covenants signed by employees who receive no benefits. Perhaps the State's legislature will try to overrule the *Socko* decision by amending the UWOA. The statute's title, *Uniform* Written Obligations Act, appears to be a misnomer because it is the law only in Pennsylvania.

Third, Socko apparently was not a high level Mid-Atlantic employee who possessed the company's trade secrets, or an employee who had been trained by the company at considerable expense. Thus, by attempting to enforce the non-compete, Mid-Atlantic was likely seeking to avoid ordinary competition. Perhaps different facts would have led to a different result.

Fourth, employers with employees in Pennsylvania who have asked existing employees to sign non-competes or are considering doing the same, should evaluate whether consideration was or will be provided for the non-compete to ensure enforcement.

Trading Secrets

Webinar Recap! Enforcing Non-Compete Provisions in Franchise Agreements

By Erik Weibust (November 25, 2015)

Happy Thanksgiving. As a thank you to our valued readers, we are pleased to announce the webinar "Enforcing Non-Compete Provisions in Franchise Agreements" is now available as a podcast and webinar recording.

In Seyfarth's ninth and final installment in its series of Trade Secrets Webinars, Seyfarth attorneys John Skelton, Erik Weibust and Anne Dunne focused on how to implement and enforce covenants against competition in the franchise context. A franchisor's trade secrets, confidential information, and goodwill are often among its core assets, and implementing and enforcing covenants against competition are a common, and effective, means of protecting such business interests.

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

- For Franchisors, non-compete provisions, especially post-termination restrictive covenants, are an important part of the franchise relationship because franchisees are given access to a franchisor's confidential information and trade secrets and upon the termination, expiration or non-renewal of the franchise agreements, franchisors have a vested interest in preventing the use of such information in a competitive business and in protecting the integrity of the franchise network and their goodwill.

- The enforceability of non-compete provisions are most often litigated in the context of a request for a preliminary injunction and thus franchisors need to be able present evidence to establish (1) all of the necessary elements, especially that the franchisor will suffer irreparable harm to its legitimate business interests and good will if the franchisee violates the terms of the agreed upon non-compete, and (2) that the restrictions are reasonable in time and scope.

- The enforceability of non-compete provisions varies significantly by state and thus national franchisors must ensure that restrictive covenants are drafted to comply with the various definitions of legitimate business interests and protected goodwill and the different Blue Pencil, Red Pencil and Reformation rules.

Texas Federal Court Rules "Anti-Competitive" Employment Covenants Do Not Raise Federal Antitrust Question

By Jesse M. Coleman (November 30, 2015)

In a case solely comprised of state-law claims to enforce employment covenants, a United States District Judge in the North District of Texas ruled last week in *Leica Microsystems Inc. v. Hernandez et al.*, No. 3:15-CV-2531-D, 2015 WL 7424770 (Nov. 23, 2015) that a defendant's characterization of the plaintiff's complaint as conduct violating federal antitrust laws was insufficient to establish federal jurisdiction.

The plaintiff, an alleged global leader in anatomical pathology solutions, sued a former employee and his new business after terminating the former employee for cause. The plaintiff alleged the former employee's new business competed against the plaintiff's business in violation of the former employee's employment agreement. The plaintiff's claims included breach of contract and trade secret misappropriation. The plaintiff also sought an injunction prohibiting defendants from, e.g., using the plaintiff's confidential information and using that information to contact the plaintiff's customers.

All parties agreed that the plaintiff's claims comprises solely state-law causes of action. The former employee nonetheless consented to removal of the case (the party removing the case had been dismissed with prejudice) and argued against the plaintiff's motion to remand. The former employee argued that federal question jurisdiction existed because, according to the former employee, plaintiff's complaint "is asking the state court to enforce [the plaintiff's] anti-competitive practices, in direct violation of the Sherman Anti-Trust Act ("Sherman Act"), 15 U.S.C. §§ 1 and 2." Specifically, the former employee argued that the plaintiff raised federal issues in its complaint by admitting that it had engaged in exclusionary, monopolistic conduct that violated federal antitrust law. Moreover, the defendant argued that plaintiff's ability to recover any of the damages it sought hinged on whether its conduct is a violation of federal antitrust law. Accordingly, according to the defendants, "substantial federal issued act[ed] as a cloud over the entire proceeding."

Judge Sydney A. Fitzwater held, however, that "[a]lthough defendants rely on various 'federal issues,' none is necessary to determine any of [the plaintiff's] state-law claims." Judge Fitzwater held that at most, the defendants had "identified a federal-law defense, i.e., that [the plaintiff] cannot obtain certain injunctive relief because awarding such relief would constitute an unreasonable restraint on trade or a monopoly." This federal-law defense, the judge held, was insufficient as a matter of law to create federal-question jurisdiction. Accordingly, the judge remanded the case and awarded the plaintiff fees and expenses, holding that the removal was unreasonable.

Non-Disclosure Agreement Enforceable Although Unlimited In Time And Area

By Paul E. Freehling (December 14, 2015)

A salesman for a medical device manufacturer signed a confidentiality covenant at the time he was hired. A dozen years later, he resigned and went to work for a competitor. The former employer sued him in an Ohio federal court. Because the covenant had neither temporal nor geographic limitations, the trial court invalidated the covenant and dismissed the breach of contract claim. The appellate court reversed, holding that no such limits are required for a confidentiality agreement. *Orthofix, Inc. v. Hunter*, Case No. 15-3216 (Nov. 17, 2015).

Status of the case

Orthofix's complaint alleged trade secret misappropriation, breach of non-compete and confidentiality covenants, and tortious interference with sales contracts. The company sought $1.6 million in lost profits. The trial court entered judgment in favor of Orthofix on the tortious interference claim (awarding $62,000 in damages) but found for the defendant with regard to trade secret misappropriation and breach of contract. In a recent decision not recommended for publication, the Sixth Circuit Court of Appeals (a) held that the confidentiality covenant was enforceable, (b) determined that the defendant violated it by using and disclosing Orthofix's confidential information, and (c) remanded the case for calculation of breach of contract damages.

Background

Orthofix makes and sells orthopedic medical devices. Hunter, who had no prior experience selling those products, worked for Orthofix for 12 years. The same day he resigned, he went to work for an Orthofix competitor. According to the appellate court, he possessed on his computer and in his memory confidential information such as Orthofix's customer list, sales and pricing data, and physician schedules, preferences, and prescribing habits. He used and disclosed this information by introducing his former customers to his new employer and providing their buying history.

The non-disclosure agreement

Hunter's non-disclosure agreement with Orthofix stated that he would "never use or disclose any confidential information which [he] acquired during the term of [his] employment with the corporation." The term "confidential information" was defined as anything "pertaining to [Orthofix's] business or financial affairs . . . developed by [Orthofix] at considerable time and expense, and which could be unfairly utilized in competition with the corporation." The parties agreed that Texas contract law applied (Orthofix is headquartered in Texas).

Trial court's decision

The lower court concluded that Orthofix could not maintain a breach of contract claim for misuse of "confidential information." That court reasoned that under Texas law, the only proprietary data

qualifying as "confidential information" would be trade secrets protected by the Ohio Uniform Trade Secrets Law. However, the court determined that there weren't any. Accordingly, the court said the covenant would be deemed to constitute a non-compete and was unenforceable because it was missing duration and territorial limitations.

Ruling on appeal

The Sixth Circuit applied the following very different analysis.

(a) A confidentiality covenant that prohibits the use and disclosure of "general skills or knowledge" is invalid under Texas law as an unreasonable restraint on trade. Here, however, the covenant protected "confidential information," not "general skills or knowledge."

(b) A covenant that applies to data that is "valuable, not readily available, and acquired at great expense and effort" is valid in Texas. That is how "confidential information" was defined in the covenant here, and that is the kind of data Hunter used and disclosed. Therefore, the covenant is enforceable. The absence of duration and geographical limits does not change this result.

(c) A covenant that protects "trade secrets," as defined under applicable state law, might also be valid. However, in light of the appeals tribunal's ruling regarding "confidential information," that court found no need to review the trial court's decision that Orthofix did not have any "trade secrets" as defined in the Ohio Uniform Trade Secrets Act.

Takeaways

The enforceability of a confidentiality covenant in an employment agreement without time or geographical limitations may turn, at least in part, on how the information that may not be disclosed is defined. Precluding dissemination of "general skills and knowledge" may constitute an invalid attempt to restrain trade. But, a covenant that prohibits the use or disclosure of narrowly tailored and carefully defined "confidential information" may be enforceable.

The Sixth Circuit observed that "confidential information" under Texas law includes memorized data. In a minority of states, courts hold that a non-disclosure agreement is not violated by revealing a prior employer's proprietary data which the ex-employee only committed to memory.

Although not an issue in *Orthofix*, a judge might decline to enjoin an ex-employee's disclosure or use of a former employer's "confidential information" if the information is deemed to be stale. In that event, disclosure or use may be unlikely to injure the movant.

Legislation

Don’t Tweet On Me! Montana and Virginia Become Latest States to Pass Social Media Privacy Legislation

By Adam Vergne and Chuck Walters (May 21, 2015)

Following a national trend, Montana and Virginia have become the nineteenth and twentieth states to enact laws restricting employer access to the social media accounts of applicants and employees.[1]

Virginia’s law, which takes effect on July 1, 2015, prohibits requesting (or requiring) the disclosure of usernames and/or passwords to an individual’s social media account. In addition, the law prohibits any requirement to change privacy settings or add a manager to the “friend” or contact list associated with a particular social media account. In addition to prohibiting the disclosure of usernames and passwords, under Montana’s new law, which took effect April 23, 2015, an employer is prohibited from requiring the disclosure of any information associated with a social media account or requesting an employee or applicant access a social media account in the presence of the employer. As is common with such legislation, both statutes contain an anti-retaliation provision that prohibits an employer from taking any adverse actions against individual that exercise his or her rights under the law.

Notably, these statutes apply only to *personal* social media accounts meaning accounts opened on behalf or at the request of the employer are not protected. Employers are also still free to view information contained in personal social media accounts that is publically available. Virginia’s law also includes an exception that permits employers to request login information if the employer has a “reasonable belief” the account is “relevant” to a “formal investigation or related proceeding” concerning the violation of a federal, state, or local law.

As the legal landscape associated with social media accounts continues to evolve, employers should review their policies and procedures to ensure compliance with all relevant statutory provisions.

[1] In 2012, Maryland became the first state to enact social media privacy legislation. Since that time, Arkansas, California, Colorado, Illinois, Louisiana, Michigan, Nevada, New Hampshire, New Jersey, New Mexico, Oklahoma, Oregon, Rhode Island, Tennessee, Utah, Washington, and Wisconsin have enacted similar legislation.

Trading Secrets

Connecticut Governor Signs New Social Media Privacy Legislation

By Daniel P. Hart (May 29, 2015)

As we have frequently reported in this blog, social media privacy issues increasingly permeate the workplace. For example, earlier this year, Montana and Virginia joined a growing number of states in enacting laws restricting employer access to the social media accounts of applicants and employees. With Governor Dannell Malloy's approval of similar legislation in Connecticut on May 21, the Constitution State has now become the latest state to follow this trend.

Connecticut's law (Public Act 15-6) becomes effective October 1, 2015 and is generally similar to social media privacy laws enacted in other states. Under the new Connecticut law, employers may not:

- Request or require that an employee or applicant provide such employer with a user name and password, password or any other authentication means for accessing a personal online account;
- Request or require that an employee or applicant authenticate or access a personal online account in the presence of such employer;
- Require that an employee or applicant invite such employer or accept an invitation from the employer to join a group affiliated with any personal online account of the employee or applicant; or
- Fail or refuse to hire any applicant as a result of his or her refusal to (A) provide such employer with a user name and password, password or any other authentication means for accessing a personal online account, (B) authenticate or access a personal online account in the presence of such employer, or (C) invite such employer or accept an invitation from the employer to join a group affiliated with any personal online account of the applicant.
- In addition, like social media privacy laws in other states, the new Connecticut law has an anti-retaliation provision stating that employers may not "discharge, discipline, discriminate against, retaliate against or otherwise penalize any employee who (A) refuses to provide such employer with a user name and password, password or any other authentication means for accessing his or her personal online account, (B) refuses to authenticate or access a personal online account in the presence of such employer, (C) refuses to invite such employer or accept an invitation from the employer to join a group affiliated with any personal online account of the employee, or (D) files, or causes to be filed, any complaint, whether verbally or in writing, with a public or private body or court concerning such employer's violation of [the law]."

- The new law authorizes aggrieved employees and applicants to file complaints with the Connecticut Labor Commissioner, who is required to conduct an investigation and may hold an evidentiary hearing. Remedies and penalties for violation of the statute include recovery of attorneys' fees and costs by the aggrieved employee or applicant, back pay, rehiring or reinstatement, reestablishment of employee benefits, and civil penalties.

- Despite the somewhat onerous penalties that employers can face for violations of the statute, the new law does contain some important exceptions. Under the statute, employers are not prevented from:

- Conducting an investigation for the purpose of ensuring compliance with applicable state or federal laws, regulatory requirements or prohibitions against work-related employee misconduct based on the receipt of specific information about activity on an employee or applicant's personal online account,

- Conducting an investigation based on the receipt of specific information about an employee or applicant's unauthorized transfer of the employer's proprietary information, confidential information or financial data to or from a personal online account operated by an employee, applicant or other source;

- Monitoring, reviewing, accessing or blocking electronic data stored on an electronic communications device paid for, in whole or in part, by an employer, or traveling through or stored on an employer's network, in compliance with state and federal law; or

- Complying with the requirements of state or federal statutes, rules or regulations, case law or rules of self-regulatory organizations.

As other states join the growing chorus of states enacting social media privacy laws, we will continue to report of the latest developments. In the meantime, employers should review their policies and procedures to ensure that they are up-to-date with the latest legislative enactments.

The Sounds of Silence: Non-Compete Reform Efforts Largely Absent in Massachusetts Legislature

By Katherine Perrelli, Erik Weibust, and Dawn Mertineit (June 5, 2015)

Last summer was a busy time for legislators in Massachusetts mulling over non-compete reform. As we reported here and here, several competing bills were in play as the legislative session drew to a close, including a compromise bill that was passed in the state Senate but ultimately failed to advance in the House. You may even recall that then-Governor Deval Patrick introduced a billthat would have banned *all* non-compete agreements in Massachusetts, with a few very limited exceptions, which also failed to go anywhere. In keeping with what appears to have become a perennial tradition in Massachusetts, the legislative session ended with a whimper, at least with respect to non-compete reform, although Governor Patrick introduced a watered-down version after the legislative session ended, which also stalled.

Fast forward nearly a year, and the subject of non-compete reform (and the adoption of the Uniform Trade Secrets Act, which was also a hot topic last year) is largely absent from the halls of the statehouse, with none of the pending bills having even made it to a committee hearing. Many see this relative silence as a function of Governor Charlie Baker's (presumed) more moderate stance on non-competes as compared to his predecessor, who was a staunch advocate of doing away with non-competes altogether. Indeed, much like his fellow candidates at the time, Governor Baker was relatively tight-lipped during his campaign on the topic of non-competes.

As reported by Massachusetts Lawyers Weekly (password required), Governor Baker has made two appointments recently that have observers pondering whether he is in fact *opposed* to non-compete reform. First, shortly after the election, Governor Baker appointed attorney Andrew P. Botti to his transition team subcommittee on jobs and the economy. Botti has been an outspoken critic of then-Governor Patrick's bill proposing to ban non-competes in the Commonwealth, largely on behalf of the Smaller Business Association of New England.

More recently, and perhaps more significantly, in April, Governor Baker appointed Paul T. Dacier, the executive vice president and general counsel of EMC Corporation, to be the chairman of Baker's Judicial Nominating Commission. EMC has earned a reputation as being a strong supporter of non-compete agreements, and as those familiar with some of the leading non-compete cases in Massachusetts know, EMC has frequently sought to enforce its non-compete agreements in the courts. Some have speculated that Governor Baker's appointment of Dacier is a sign that the governor is directly opposed to non-compete reform.

Not surprisingly, those in Governor Baker's camp have denied that these appointments have any hidden meaning, with Botti pointing to Governor Baker's desire to tackle more urgent issues, such as

the performance of the MBTA during this year's record-breaking winter and the state budget. Even supporters of non-compete reform, such as Representative Lori Ehrlich, have largely attributed the lack of progress to disagreements between the state House of Representatives and Senate regarding committee rules, not lack of support from the Governor's Office. However, Rep. Ehrlich did note that Dacier's appointment "is certainly a concern."

So, as we head into the dog days of summer (most welcome after the winter), it appears that non-compete reform is not at the top of the legislative agenda in Massachusetts. As always, we will keep you informed of any significant developments.

Trading Secrets

Democratic Senators Propose Federal Legislation to Ban Use of Non-Compete Agreements with Low-Wage Employees and to Require Advance Notice to Potential Employees of Requirement to Sign Non-Compete

By Robert B. Milligan (June 8, 2015)

U.S. Senators Al Franken (D-Minn.) and Chris Murphy (D-Conn.) proposed federal legislation last week to ban the use of non-competes for low-wage employees and require companies to provide advance notice before asking potential employees to sign non-competes. Senators Elizabeth Warren (D-Mass.) and Richard Blumenthal (D-Conn.) are cosponsors of the bill.

The stated purpose of the legislation, entitled the Mobility and Opportunity for Vulnerable Employees (MOVE) Act, is "to prohibit employers from requiring low-wage employees to enter into covenants not to compete, to require employers to notify potential employees of any requirement to enter into a covenant not to compete, and for other purposes."

In a prepared statement Franken said, "Forcing lower-wage workers to sign 'non-compete agreements' makes it harder for these workers to find new jobs and stay employed. Agreements like these stifle fair competition and harm workers. We need to challenge this practice, and change the law to protect people who are simply trying to make ends meet. Our bill will fix this issue by removing unnecessary employment barriers that hurt everyday Americans."

"Non-compete agreements hidden in low-wage worker contracts deliberately trap these workers in low-paying jobs – and that's unacceptable," said Murphy, in his prepared statement. "I worked hard on this bill because I believe that if you're making less than $15-an-hour, the government has a moral duty to stop companies from exploiting your hard work by preventing you from using your skills and experience to work your way up. The MOVE Act helps low-wage workers by opening new doors and providing them the freedom to pursue better career opportunities."

Murphy also claims that research shows that employers force anywhere from 8-15% of low-wage workers to sign non-compete agreements in an effort to dissuade those workers from seeking better, higher-paying jobs within the same industry.

Trading Secrets

The MOVE Act will ban the use of non-compete agreements for employees making less than $15 an hour, $31,200 per year, or the minimum wage in the employee's municipality, and will require employers to notify prospective employees that they may be asked to sign a non-compete agreement.

Covenant not to compete is defined in the MOVE ACT as:

"an agreement (A) between an employee and employer that restricts such employee from performing

(i) any work for another employer for a specified period of time;

(ii) any work in a specified geographical area; or

(iii) work for another employer that is similar to such employee's work for the employer included as a party to the agreement . . . ."

It also requires employers to post notice of the Act in a conspicuous place on the premises.

Section 4 of the MOVE ACT provides that:

In order for an employer to require an employee, who in any workweek is engaged in commerce or in the production of goods for commerce (or is employed in an enterprise engaged in commerce or in the production of goods for commerce) and is not a low-wage employee, to enter into a covenant not to compete, the employer shall, prior to the employment of such employee and at the beginning of the process for hiring such employee, have disclosed to such employee the requirement for entering into such covenant.

Under the MOVE ACT, the Secretary of Labor shall impose a civil fine of $5,000 with respect to any employer who violates the ban or notice requirement an amount not to exceed $5,000 for each employee who was the subject of such violation. Employers will also be fined $5,000 for failure to post the appropriate notice. In determining the amount of any civil fine, the Secretary shall consider the appropriateness of the fine to the size of the employer subject to such fine and the gravity of the applicable violation.

Based upon the proposed statutory language of "covenant not to compete," it is unclear whether it applies to non-competition agreements alone or non-solicitation agreements and other restrictive covenants (e.g. non-disclosure) as well.

Additionally, it requires virtually every employer in the United States to provide advance notice to prospective employees prior to using a "covenant not to compete," which as indicated above may mean more than just a non-compete agreement.

Also, it is unclear whether the notification requirement governs non-compete agreements introduced with existing employees who are later asked to sign such agreements. Additionally, it appears that the proposed legislation requires that employers ensure that employees' compensation exceeds the minimum threshold of being considered a low-wage worker throughout their employment or run the risk that the non-compete violates the law, even if the agreement was valid at execution.

The proposed legislation also assumes that wages and salary is the key factor in determining whether a non-compete should be enforceable.

The enforceability of non-compete agreements has typically been governed by state law with state courts determining the reasonableness of such covenants.

At first blush, one wonders whether this legislation is really necessary and whether state courts are actually enforcing non-compete agreements against “low-wage workers” and whether employers are actually trying to use and enforce such agreements. Also, one also wonders whether any existing non-compete agreements with “low-wage workers” in reality limit employee mobility or whether this is legislation in search of a problem.

The proposed legislation does serve as a reminder to employers to conduct a survey of their current restrictive covenant agreements and protection plans and ask themselves the following questions:

- What legitimate interests are they trying to protect in their agreements?
- Are they using the right agreements with the right employees?
- Are there some employees that they need to ask to sign non-competes and others that they don’t?
- Should they consider using non-solicit agreements instead?
- Does continuing employment constitute sufficient consideration for the agreements? Or is new consideration required? If so, what is sufficient consideration?
- Are the time duration and geographical restrictions contained in the agreements sufficiently tailored?

We will continue to closely follow this legislation and provide an update on any material developments.

Video Interview: Discussing the MOVE Act with LXBN TV

By Robert B. Milligan (June 18, 2015)

https://youtu.be/8iZi-bZrod0

Following up on my post weighing on the MOVE Act, which stands to impact non-compete agreements for low-wage employees if enacted, I had the opportunity to discuss the subject with Colin O'Keefe of LXBN. In the interview, I discuss the basics of the potential legislation and whether or not it has a chance of passing.

Trading Secrets

Hawaii Bans Non-Compete and Non-Solicit Agreements with Technology Workers

By Robert B. Milligan (July 6, 2015)

Hawaii joined the small list of states that prohibit certain non-compete agreements with employees.

On June 26, 2015, Hawaii's governor David Ige signed Act 158 which voids any "non-compete clause or a non-solicit clause in any employment contract relating to an employee of a technology business."

The Act defines "technology business" as one that "derives the majority of its gross income form sale or license of products or services resulting from its software development or information technology development, or both." It excludes any business that is part of the broadcast industry or any telecommunications carrier. "Information technology development" is defined under the Act as "the design, integration, deployment, or support services for software" and "software development" is defined as "the creation of coded computer instructions."

The Act defines a "non-compete clause" as one that "prohibits an employee from working in a specific geographic area for a specific period of time after leaving work with the employer."

"Non-solicit clause" is defined as one that "prohibits an employee from soliciting employees of the employer after leaving employment with the employer." Curiously, there appears to be an open issue as to whether customer non-solicit provisions are covered by the new Act, though proponents of the Act may argue that customer non-solicits are covered under the "non-compete clause" language.

The stated purpose of the Act "is to stimulate Hawaii's economy by prohibiting non-compete agreements and restrictive covenants that forbid post-employment competition for employees of technology businesses."

In passing the bill, the Hawaii legislature found:

[R]estrictive employment covenants impede the development of technology businesses within the State by driving skilled workers to other jurisdictions and by requiring local technology businesses to solicit skilled workers from out of the State. Eliminating restrictive covenants for employees of technology businesses will stimulate Hawaii's economy by preserving and providing jobs for employees in this sector and by providing opportunities for those technology employees to establish new technology companies and new job opportunities in the State.

A restrictive covenant not to compete with a former employer imposes a special hardship on employees of technology businesses as these highly specialized professionals are trained to perform

specific jobs in the industry. Because the geographic area of Hawaii is unique and limited, non-compete agreements unduly restrict future employment opportunities for technology workers and have a chilling effect on the creation of new technology businesses within the State by innovative employees.

Hawaii has a strong public policy to promote the growth of new businesses in the economy, and academic studies have concluded that embracing employee mobility is a superior strategy for nurturing an innovation-based economy. In contrast, a non-compete atmosphere hinders innovation, creates a restrictive work environment for technology employees in the State, and forces spin-offs of existing technology companies to choose places other than Hawaii to establish their businesses.

The effective date of this law is **July 1, 2015**. It does not affect any existing non-compete or non-solicitation clauses in employment contracts for technology businesses prior to July 1, 2015.

Non-competes with other Hawaii employees remain enforceable as long as they pass a reasonableness analysis under Hawaii law. The legislature found in the new Act "that employer trade secrets are already protected under the [sic] federal Uniform Trade Secrets Act and under section 480-4(c)(4), Hawaii Revised Statutes; therefore, the benefits to the employer from non-compete or non-solicit agreements are duplicative and overreaching protections that may unreasonably impose undue hardship upon employees of technology businesses and the Hawaii economy." The existing Act permits non-disclosure covenants with employees. Accordingly, employers should still use those covenants, even with technology workers.

Companies conducting business in Hawaii in the technology sector should review their employment contracts to determine whether they need to revise their agreements to comply with this new law.

Alabama Revises Non-Compete Statute In Effort to Provide Additional Clarity

By Eric Barton (July 14, 2015)

On June 11, 2015, Alabama's Governor signed into law legislation that revises the state's non-compete statute, which is found in Section 8-1-1 of the Code of Alabama. The effective date for these changes is **January 1, 2016**. As summarized below, these revisions represent the Alabama legislature's attempt to "clarity" portions of the non-compete statute by codifying several recent judicial decisions that interpreted the previous version of Section 8-1-1.

Just like its predecessor, the revised statute begins by setting forth a general ban against ***any*** agreements that restrict someone from engaging in "a lawful profession, trade, or business of any kind." That said, in "order to preserve a protectable interest," the new law then details six exceptions to that general ban:

1. When the "agent, servant, or employee holds a position uniquely essential to the management, organization, or service of the business."

2. "An agreement between two or more persons or businesses or a person and a business to limit commercial dealings to each other."

3. "One who sells the good will of a business may agree with the buyer to refrain from carrying on or engaging in a similar business and from soliciting customers of such business within a specified geographic area . . . subject to reasonable time and place restraints. Restraints of one year or less are presumed to be reasonable."

4. "An agent, servant, or employee of a commercial entity may agree with such entity to refrain from carrying on or engaging in a similar business within a specified geographic area so long as the commercial entity carries on a like business therein, subject to reasonable restraints of time and place. Restraints of two years or less are presumed to be reasonable."

5. "An agent, servant or employee of a commercial entity may agree with such entity to refrain from soliciting current customers, so long as the commercial entity carries on a like business, subject to reasonable time restraints. Restraints of 18 months or for as long as post-separation consideration is paid for such agreement, whichever is greater, are presumed to be reasonable."

6. "Upon or in anticipation of a dissolution of a commercial entity, partners, owners, or members, or any combination thereof, may agree that none of them will carry on a similar commercial activity in the geographic area where the commercial activity has been transacted."

For the first time, the new law now defines "protectable interest," which includes the following:

1. Trade secrets (as defined by Alabama law).
2. "Confidential information, including, but not limited to, pricing information and methodology; compensation; customer lists; customer data and information; mailing lists, prospective customer information; financial and investment information; management and marketing plans; business strategy, technique, and methodology; business models and data; processes and procedures; and company provided files, software, code, reports, documents, manuals, and forms used in the business that may not otherwise qualify as a trade secret but which are treated as confidential to the business entity, in whatever medium provided or preserved, such as in writing or stored electronically."
3. "Commercial relationships or contacts with specific prospective or existing customers, patients, vendors or clients."
4. "Customer, patient, vendor, or client good will associated with any of the following: (1) An ongoing business, franchise, commercial, or professional practice, or trade dress. (2) A specific marketing or trade area."
5. "Specialized and unique training involving substantial business expenditure specifically directed to a particular agent, servant, or employee; provide that such training is specifically set forth in writing as the consideration for the restraint."

Several other key revisions include:

1. "Blue penciling" is now codified, allowing a court (if it so chooses) to void an overly broad or unreasonable in duration restraint and reform it to "preserve the protectable interest or interests."
2. The new law provides the following remedies for breach of a non-compete agreement as follows:
    - "Such injunctive and other equitable relief as may be appropriate with respect to any actual or threatened breach."
    - "The actual damages suffered as a result of the breach or lawful liquidated damages of provided in the contract."
    - "Any remedies available in contract law, including attorneys' fees or costs, if provided for in the contract or otherwise provided by law."
3. The new law states that the party who opposes enforcement of a non-compete agreement must establish that such enforcement would cause them undue hardship. Previously, the plaintiff had the burden of proving the ***lack*** of undue hardship.
4. The new law does not abolish the "Professional Exemptions," which includes doctors, physical therapists, lawyers, CPAs, and veterinarians.

In light of these forthcoming changes, it is imperative that Alabama employers carefully review their non-compete agreements before January 1, 2016 and update them as necessary to conform with the new law. In particular, employers should carefully review the time durations included in their non-compete agreements, as well as how they define their protectable interests, in order to avoid having a non-compete agreement held invalid. Please do not hesitate to contact us if you have any questions or wish to discuss further.

Trading Secrets

U.S. Congress To Again Consider Private Right of Action for Trade Secret Misappropriation

By Marcus Mintz (July 30, 2015)

On July 29, 2015, with bipartisan support, congressional leaders in both the House and Senate, including Senator Orrin Hatch (R-UT) and Representative Doug Collins (R-GA), introduced a bill to create a federal private right of action for the misappropriation of trade secrets. The proposed legislation, titled the "Defend Trade Secrets Act of 2015" ("DTSA"), follows a failed attempt just last year to pass the "Defend Trade Secrets Act of 2014."

Announcement of the proposed legislation was joined by a letter of support on behalf of the Association of Global Automakers, Inc., Biotechnology Industry Organization (BIO), The Boeing Company, Boston Scientific, BSA | The Software Alliance (BSA), Caterpillar Inc., Corning Incorporated, Eli Lilly and Company, General Electric, Honda, IBM, Illinois Tool Works Inc., Intel, International Fragrance Association, North America, Johnson & Johnson, Medtronic, Micron, National Alliance for Jobs and Innovation (NAJI), National Association of Manufacturers (NAM), NIKE, The Procter & Gamble Company, Siemens Corporation, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, United Technologies Corporation and 3M. The joint letter expressed the need for a private right of action to supplement the existing Economic Espionage Act of 1996 ("EEA"), which only provides for criminal sanctions in the event of trade secret misappropriation.

If passed, the proposed DTSA will grant a private right of action for misappropriation of trade secrets under federal law. The DTSA is largely consistent with the Uniform Trade Secrets Act ("UTSA"), which has been passed in some form in almost all states. The DTSA defines "misappropriation" consistently with the DTSA, and provides for similar remedies, including injunctive relief, compensatory damages, and exemplary damages and the recovery of attorneys' fees in the event of willful or malicious misappropriation.

The DTSA differs from the UTSA in several important aspects. First, the DTSA allows for an ex parte seizure order. A plaintiff fearful of the destruction or hiding of its trade secrets would be able to take proactive steps to recover its trade secrets prior to giving any notice of a lawsuit. The proposed seizure protection goes well beyond what a court is typically willing to order under existing state law. Second, the DTSA's limitations period is five years compared to just three under the UTSA. Third, the DTSA allows for the recovery of treble exemplary damages versus double under the UTSA. Fourth, the DTSA contains no language preempting other causes of action that arise under the same common nucleus of facts, unlike the UTSA. Finally, the DTSA allows for federal jurisdiction of a misappropriation claim, provided the plaintiff can demonstrate a connection between the trade secret and interstate commerce. In sum, the DTSA provides significant measures for a plaintiff compared to the UTSA.

Trading Secrets

The DTSA offers significant protections to trade secret holders and will create a uniform legal framework across the United States. Now, all stakeholders will need to wait and see whether the DTSA of 2015 is able to become law where prior legislative efforts failed.

Trading Secrets

Latest Update on Federal Trade Secrets Legislation

By Robert B. Milligan and Amy Abeloff (August 26, 2015)

With increased activity regarding proposed federal trade secrets legislation expected next month and for the remainder of the fall Congressional session, Seyfarth Shaw's dedicated Trade Secrets/Non-Compete group has created a resource which summarizes the proposed legislation, outlines the arguments in favor of and against the legislation, and provides additional 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 federal legislation, the arguments on both sides of the debate, and our most current resource links.

How Are Trade Secrets Currently Protected?

Trade secrets are legally protectable information and can include a formula, pattern, compilation, program, device, method, technique or process. To meet the most common definition of a trade secret, a trade secret has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being generally known. Examples of trade secrets include, plans, designs, negative information, computer software, customer lists, non-public financial information, cost and pricing information, manufacturing information, confidential information about business opportunities, and certain personnel information.

Trade secrets are generally protected by state law under a particular state's adoption of 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 and social media 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?

On July 29, 2015, with bipartisan support, Congressional leaders in both the House and Senate, including Senators Orrin Hatch (R-UT), Christopher Coons (D-DE) and Representative Doug Collins (R-GA), introduced bills to create a federal private right of action for the misappropriation of trade secrets. The identical bills are HR 3326 and S. 1890 and they were referred to their respective judiciary committee. The proposed legislation, titled the "Defend Trade Secrets Act of 2015" ("DTSA"), follows an unsuccessful attempt just last year to pass the "Defend Trade Secrets Act of 2014."

The proposed legislation would authorize a private civil action in federal court for the 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 proposed legislation features amendments from the 2014 bill and seeks to do the following: 1) create a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act; 2) provide parties pathways to injunctive relief and monetary damages to preserve evidence, prevent disclosure, and account for economic harm to companies; and 3) create remedies for trade secret misappropriation similar to those in place for other forms of intellectual property.

The DTSA has some similarities with the Uniform Trade Secrets Act. The DTSA defines "misappropriation" consistently with the DTSA, and provides for similar remedies, including injunctive relief, compensatory damages, and exemplary damages and the recovery of attorneys' fees in the event of willful or malicious misappropriation.

The DTSA, however, differs from the UTSA in several important aspects. Most notably, it opens the federal courts to plaintiffs for trade secret misappropriation cases. The DTSA also allows for an ex parte seizure order. A plaintiff fearful of the propagation or dissemination of its trade secrets would be able to take proactive steps to have the government seize its trade secrets from the defendant prior to giving any notice of the lawsuit to the defendant. The proposed seizure protection goes well beyond what a court is typically willing to order under existing state law. Next, the DTSA's statute of limitations period is five years compared to just three under the UTSA. Additionally, the DTSA allows for the recovery of treble exemplary damages versus double under the UTSA. Finally, the DTSA contains no language preempting other causes of action that arise under the same common nucleus of facts, unlike the UTSA.

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. Legislation to create a civil cause of action for trade secret misappropriation in federal court has failed in at least three previous attempts.

Recent scholarly articles in the Gonzaga Law Review and Fordham Law Review have suggested 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, nation states, 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 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.

Another case involved the sentencing of a former DuPont employee who allegedly conspired with a South Korean company, Kolon Industries, to misappropriate trade secrets involving Kevlar, a well-known synthetic fiber product produced and sold by DuPont. Kolon Industries allegedly put a plan in place to recruit former DuPont employees so Kolon could create a product to compete with Kevlar without putting the time, effort, and expenditures into developing its own product. The former employee, even though he signed a non-disclosure agreement while at DuPont, allegedly retained DuPont documents upon his departure and turned them over to Kolon when they recruited him. Upon finding out about this scheme, the FBI investigated Kolon, and five of its executives were indicted for

committing trade secret theft. Kolon plead guilty and was sentenced to pay $85 million in penalties and $275 million in restitution.

There is also significant harm caused by economic espionage committed by insiders. An employee of a large U.S. futures exchange company recently 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 FBI has recently launched a nationwide awareness campaign and released a short film based upon an actual case, The Company Man: Protecting America's Secrets, aimed at educating anyone with a trade secret about the threat and how they can help mitigate it. The film illustrates how one U.S. company was targeted by foreign actors and how that company worked with the FBI to address the problem.

From the perspective of many of those in favor the legislation, 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 in our global economy. 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, including what are reasonable secrecy measures. Some states have found a novelty requirement for information to be considered a trade secret and some are more protective of customer lists than others. 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. Obtaining service of process and discovery can be extremely difficult or impossible under the current system.

Proponents and Sponsors of the Bills

Announcement of the proposed legislation on July 29, 2015 was joined by a letter of support on behalf of the Association of Global Automakers, Inc., Biotechnology Industry Organization (BIO), The Boeing Company, Boston Scientific, BSA | The Software Alliance (BSA), Caterpillar Inc., Corning Incorporated, Eli Lilly and Company, General Electric, Honda, IBM, Illinois Tool Works Inc., Intel, International Fragrance Association, North America, Johnson & Johnson, Medtronic, Micron, National Alliance for Jobs and Innovation (NAJI), National Association of Manufacturers (NAM), NIKE, The Procter & Gamble Company, Siemens Corporation, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, United Technologies Corporation and 3M. The joint letter expressed the need for a private right of action to supplement the existing Economic Espionage Act of 1996 ("EEA"), which only provides for criminal sanctions in the event of trade secret misappropriation.

In 2014, two similar trade secret bills were introduced and received support from various constituents.

The Heritage Foundation 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 with the PRATSA bill. A diverse set of companies and organizations supported the 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, National Association of Manufacturers, and the National Chamber of Commerce.

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. From their perspective, 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 legislation 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 ex parte seizure.

The former head of the Patent Office, David Kappos, came out in favor of the 2014 House 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

Last August, 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 submitted an Opposition Letter to the 2014 bills. The professors cited 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.

Shortly after the introduction of the bills in July 2015, law professors, David Levine and Sharon Sandeen, wrote a new letter to Congress setting forth seven differences between the 2014 bills and the 2015 bill while still contesting the arguments of the bill's supporters. The seven differences include: 1) the wrong is defined differently; 2) the *ex parte* civil seizure still remains but with apparently more stringent standards; 3) new encryption language has been added; 4) new concerns about employee mobility; 5) trade secrets are described as not intellectual property; 6) the reporting of trade secret theft

abroad is unclear as to whether it means “theft” or “misappropriation;” and 7) “Sense of Congress” provision, which presumes trade secret theft is always “harmful.” They believe that the recently introduced legislation does not ameliorate the problems it seeks to fix.

Current Status Of Proposed Legislation

Both bills have been introduced into their corresponding judiciary committee. HR 3326 and S. 1890 were sent into committee on July 29, 2015. We expect Congress to address the proposed legislation after the Labor Day recess.

For additional news and resources, please click here.

U.S. Senate To Hold Hearing On Impact of Trade Secret Theft

By Robert B. Milligan and Amy Abeloff (December 1, 2015)

Tomorrow at 10:00 a.m. EST, the United States Senate Judiciary Committee will hold a hearing concerning trade secret theft entitled "Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm."

The hearing will feature some of the key supporters of the bill known as the Defend Trade Secrets Act (DTSA). The DTSA currently has over 100 bipartisan Congressional supporters in the House and Senate, including chief sponsors Senators Orrin Hatch (R-Utah) and Chris Coons (D-Del.), who believe the bill will help combat trade secret theft and will provide trade secret theft victims with effective legal recourse in federal court. As it stands, victims presently only have civil legal remedies for trade secret theft at the state level, which can pose challenges to victims to effectively pursue their claims and obtain just remedies. In this particular hearing, the Senate Judiciary Committee will consider the Chinese cyber theft of U.S. corporate trade secrets and other assets.

Despite the support the bill has received, it has been met with some opposition from some academics. Recently, several professors have written Congress in opposition to the DTSA, arguing that the adoption of the bill would be nothing more than trouble. Some of the potential issues cited included chilling innovation in the U.S., increased legal fees associated with litigating trade secret actions, and overall negative economic growth.

Many in the business community and private legal practice, however, have voiced their support for the bill. Senator Hatch has indicated his desire to have the Defend Trade Secrets Act passed this year but whether Congress will act on that ambitious schedule remains to be seen.

The Trading Secrets Blog will be live tweeting the Senate Judiciary Committee's hearing concerning trade secret theft tomorrow, December 2, at 10:00am EST/7:00am PST from @tradesecretslaw and @tradesecretlaws. A live stream of the hearing will be available tomorrow as well.

For more information on the Defend Trade Secrets Act, please see our dedicated page which explains the proposed legislation, its history, the proponents and opponents, and provides a collection of resource materials.

Update on the Senate Judiciary Committee's Hearing on the Protection of Trade Secrets

By Robert B. Milligan and Amy Abeloff (December 2, 2015)

Earlier today, the Senate Judiciary Committee held a hearing regarding the protection of trade secrets through the creation of a federal civil cause of action, which would allow trade secret victims to sue for trade secret misappropriation in federal court.

Senator Chuck Grassley opened the hearing, outlining the importance of protecting the "lesser known but increasingly important form of intellectual property:" trade secrets. Grassley emphasized the hefty financial losses U.S. companies have faced due to the theft of their trade secrets. He noted that the total value of trade secrets in the U.S. is approximately $5 trillion with annual losses owing to trade secret theft amounting to over $3 billion. Senator Patrick Leahy dovetailed off of Grassley's comments, voicing his support for the protection of trade secrets; especially protection for small businesses, like those in his home state of Vermont, with valuable trade secrets.

After the introductory statements, the four witnesses that appeared at the hearing were announced: Karen Cochran, Chief IP Counsel at E.I. DuPont de Nemours and Co.; Tom Beall, VP and Chief IP Counsel at Corning Corp.; James Pooley, Principal at James Pooley, PLC; and Professor Sharon Sandeen, Hamline University School of Law. Professor Sandeen was the only witness in opposition to the adoption of a uniform, federal trade secret law, namely, the DTSA.

Cochran voiced DuPont's support of the DTSA, especially in light of trade secret theft it recently faced with regard to its Kevlar products. We discussed this case in our latest trade secret law update. Cochran noted two benefits to adoption of the DTSA: 1) victims of trade secret theft would have access to federal courts; and 2) future trade secret dissemination and/or destruction would be curbed.

Beall testified that one of its most successful products has been unprotected under patent law for many years, but its trade secrets help keep its version of the product at the top of the market. He also voiced Corning's support of the DTSA based on the fact that state trade secret laws are not harmonized, litigating in many different states actually increases litigation costs, and service of process on a trade secret thief is difficult, if not impossible at times.

Professor Sandeen stated the DTSA would cause more problems than it would solve. She said the DTSA, especially its seizure provision, would open the door to abuse and hikes in litigation costs.

The final witness, Pooley, who rather vehemently disagreed with the opposition's point of view, stated that because the DTSA's proposed narrow application, risk of litigation abuse would be low because restraining orders and injunctions are normally difficult to win. Pooley also acknowledged that despite the adoption of the Uniform Trade Secrets Act (UTSA) by 48 states, each state has its own variations, which affects time and monetary costs in terms of obtaining required orders and serving out-of-state defendants. Moreover, Pooley noted that small businesses would not be at risk of harm under the DTSA as opposers to the bill have argued, but instead would benefit because they, too, need recourse in dealing with theft of its trade secrets nationwide.

Some questions the various senators posed throughout the hearing inquired into the alleged existence of "trade secret trolls," application of the DTSA domestically and abroad, and risk of harm of the ex-parte seizure provision of the DTSA. Sandeen argued that there is indeed a "trade secret troll" threat in abusive litigation tactics; and that those ready and willing to litigate over misappropriation of trade secrets in federal court are essentially "trolls" in a manner similar to patent trolls. However, Pooley disagreed, noting the differences between protections available under patent law versus trade secret law. Those in support of the DTSA cited the increase in international cyber theft, and noted that state courts do not have jurisdiction over foreign culprits as the law currently stands. Though, it bears noting, that the supporters recognized that the DTSA would not necessarily address this rampant international cyber espionage.

Beall cited a real-life example that happened to Corning in which an individual fled the country with company trade secrets, but Corning was unable to prosecute under state trade secret law due to jurisdictional issues. Had a federal cause of action been in place, Beall implied, Corning would have been able to restrain the individual from leaving the country, and would have been able to retain its trade secrets.

Besides the supporters appearing at the hearing today, the bill is also supported by a robust industry coalition that includes Adobe, AdvaMed, the Alliance of Automobile Manufacturers, the Association of Global Automakers, Inc., Biotechnology Industry Organization (BIO), The Boeing Company, Boston Scientific, BSA | The Software Alliance (BSA), Caterpillar Inc., Corning Incorporated, Eli Lilly and Company, General Electric, Honda, IBM, Illinois Tool Works Inc., Intel, The Intellectual Property Owners Association (IPO), International Fragrance Association, North America, Johnson & Johnson, Medtronic, Micron, National Alliance for Jobs and Innovation (NAJI), National Association of Manufacturers (NAM), NIKE, Pfizer, Philips, The Procter & Gamble Company, SAS, Siemens Corporation, Software & Information Industry Association (SIIA), U.S. Chamber of Commerce, and United Technologies Corporation. This coalition wrote a letter today to Senators Coons, Flake, and Hatch saying:

Trade secrets are an essential form of intellectual property. Trade secrets include information as broad-ranging as manufacturing processes, product development, industrial techniques, formulas, and customer lists. The protection of this form of intellectual property is critical to driving the innovation and creativity at the heart of the American economy. Companies in America, however, are increasingly the targets of sophisticated efforts to steal proprietary information, harming our global competitiveness.

Existing state trade secret laws are inadequate to address the interstate and international nature of trade secret theft today. Federal law protects trade secrets through the Economic Espionage Act of

1996 (“EEA”), which provides criminal sanctions for trade secret misappropriation. While the EEA is a critical tool for law enforcement to protect the clear theft of our intellectual property, U.S. trade secret owners also need access to a federal civil remedy and the full spectrum of legal options available to owners of other forms of intellectual property, such as patents, trademarks, and copyrights.

The Defend Trade Secrets Act will create a federal remedy that will provide a consistent, harmonized legal framework and help avoid the commercial injury and loss of employment that can occur when trade secrets are stolen. We are proud to support it.

Supporters of the DTSA voiced concern over the loss of proprietary information, especially abroad, and noted how a federal cause of action would give them, as well as all U.S. companies with trade secrets, easy access to federal court to address the theft.

Senator Hatch believes a vote on the DTSA should happen immediately. “Both Republicans and Democrats can agree that this bill is a win for American property rights and innovation,” Hatch said. “Why wouldn’t we move this bill now?” Senator Coons echoed Hatch, saying “[w]e need this bill now more than ever as more and more American companies are losing jobs and revenue because they lack the ability to defend their trade secrets under federal civil law.” Currently, the DTSA has 92 co-sponsors in the House and 15 in the Senate. Given the wide support from industry leaders as well as bipartisan members of the Judiciary Committee, there appears to be a chance that the DTSA will be voted on this year.

International

Trading Secrets

Opposition Emerges to EU Trade Secrets Directive

By Daniel P. Hart (February 23, 2015)

By any measure, the past few weeks have been eventful in Europe. Given the number of challenges facing European lawmakers — from continued hostilities in Ukraine, to last-minute negotiations over Greek debt, to anti-terrorism measures — it's unlikely that trade secrets protection is at the top of anyone's agenda in Brussels or Strasbourg. Still — as we have previously reported here — the European Commission's proposed directive to protect trade secrets remains an important item on the European Parliament's agenda for this year. As we have argued, the proposed directive (if enacted) will substantially alter the legal landscape in Europe regarding trade secret protection and may enhance cross-border certainty within the EU by requiring all member states to provide certain minimum standards of protection for trade secrets.

Despite widespread support for the proposed directive, opposition to the proposal has now emerged. Recently, the European Public Health Alliance ("EPHA"), a coalition of public health NGOs, patient groups, health professionals, and disease groups, voiced its opposition to the directive. In a joint statement opposing the directive, EPHA argues that the current version of the proposed directive contains:

- "An unreasonably broad definition of 'trade secrets' that enables almost anything within a company to be deemed as such";
- "Overly-broad protection for companies, that could sue anyone who 'unlawfully acquires, uses or discloses' their so-called 'trade secrets'"; and
- "Inadequate safeguards that will not ensure that EU consumers, journalists, whistleblowers, researchers and workers have reliable access to important data that is in the public interest."

The EPHA joint statement further argues that, under the proposed directive, (1) companies in the health, environment and food safety fields could refuse compliance with transparency policies even when the public interest is at stake; (2) the right to freedom of expression and information could be seriously harmed; and (3) the mobility of EU workers could be undermined. Based on these concerns, the EPHA joint statement concludes that "this unbalanced piece of legislation would result in legal uncertainty" and that "unless radically amended by the Council and European Parliament, the proposed directive could endanger freedom of expression and information, corporate accountability, information sharing—possibly even innovation—in the EU." Accordingly, the EPHA urges the EU Council and the European Parliament to radically amend the directive by "limiting the definition of what constitutes a trade secret and strengthening safeguards and exceptions to ensure that data in the public interest cannot be protected as trade secrets."

Trading Secrets

As we have previously noted in this blog, many features of the proposed directive, including its definition of "trade secrets," are similar to provisions in the Uniform Trade Secrets Act, which the majority of U.S. jurisdictions have adopted. Interestingly, in its joint statement, the EPHA observes that the text of the proposed directive "is strongly supported by multinational companies" and notes that industry coalitions in the EU and US have been lobbying for similar proposed trade secrets legislation in the U.S. Congress (which we have previously discussed in this blog). Although the U.S. Congress did not enact neither of the trade secrets bills introduced last year, trade secrets protection also remains an important item on the agenda in Congress — though, as with the proposed EU directive, the proposed U.S. trade secrets legislation also has its opposition.

It is not yet clear how much support, or opposition, the proposed EU trade secrets directive has in the European Parliament. We will continue to monitor progress of both the proposed EU directive and proposed legislation in the U.S. and will report on developments in this blog as they occur.

Webinar Recap! International Trade Secret and Non-Compete Law Update

By Daniel P. Hart, Ming Henderson, and Wan Li (April 23, 2015)

We are pleased to announce the webinar "International Trade Secret and Non-Compete Law Update" is now available as a podcast and webinar recording.

In Seyfarth's third installment of its 2015 Trade Secrets Webinar series, Seyfarth attorneys 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 and China compared to the United States. This webinar provided valuable insight for companies who compete in the global economy and must navigate the legal landscape in these countries to ensure protection of their trade secrets and confidential information, including the effective use of non-compete and non-disclosure agreements

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

International…local law compliance is key

One size does not fit all! Requirements for enforceable restrictive covenants vary dramatically from jurisdiction to jurisdiction. However, there are some common requirements and issues regarding enforceability based on the region (e.g. in Europe, see below). Bearing in mind non-compete covenants across the world 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.

The general approach to restrictive covenants in Europe, is that the restrictions should not go further than is reasonably necessary to protect the employer's legitimate business interests. This restrictive approach is a continuing trend across Europe. For example, there is a recent prohibition in the Netherlands on non-compete clauses in fixed-term contract unless justified by the special interests of the company. In practice, this means that employers should particularly focus on the duration and scope (in terms of geographical coverage and the employee's own personal activities) of the restrictions and be mindful of any local payment obligations when preparing restrictive covenants (e.g. in France and Germany). Europe is also making an attempt to remedy the uneven levels of protection and remedies in relation to trade secrets. The draft EU Directive for trade secret protection is currently making its way through the legislative process with no firm timeline for adoption.

In addition to local or regional nuances, employers should take advantage of other contractual and/or tactical mechanisms as a "belt-and braces" approach, such as, claw-backs and forfeiture of deferred compensation (where permitted), use of garden leave provisions, and strategic use of forum selection and choice-of-law provisions. Employers operating in the U.S. should also consider strategic use of mandatory forum selection and choice-of-law provisions in restrictive covenant agreements with U.S.-based employees.

Practical measures should also be taken to protect 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…do not miss the deadline

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.

Recent case law shows that French Courts are strict when it comes to the interpretation of the non-compete clauses and the possibility to waive the non-compete clause. If an employer misses the relevant contractual deadline to release an employee from their non-compete, the financial compensation will be due for the entire period. Similarly, if the employer waives the non-compete prematurely, the Courts will consider the waiver as invalid.

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 automatically include a confidentiality clause in employment agreements to strengthen the protection of the company's data post-termination. Good news for employers, the French High Court recently confirmed that, unlike non-compete covenants, a confidentiality clause does not require any financial compensation.

United Kingdom…less is NOT more

Restrictive covenants are potentially void as an unlawful restraint of trade! 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. by geographical scope) and is specific to the commercial environment. Unlike in some European jurisdictions, payment will not 'rescue' an unenforceable restriction. In addition, the English Courts tend to have an unforgiving nature when it comes to poor drafting even if the intention of the parties is obvious. Employers should therefore 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", which is narrowly defined, 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. Often the physical protection of confidential information is underestimated

(e.g. encrypting data, installing passwords, secure storage, etc.), which can be a more effective and a less costly approach for employers in the long-term. Employers should therefore also seek to retain physical control of such information in order to reduce and limit unwanted disclosure and misuse.

China …. stay atop an evolving regulatory system

In China, employers should ensure that they have a non-compete agreement with the employee at the time of employment, so that the employer can decide whether to enforce or not to enforce the non-compete agreement for a period of post-employment.

In addition, employers should ensure that documents are marked with 'confidential', or that other measures are taken to protect confidential information. Otherwise, remedies may not be available under the Chinese law for breach of confidential obligations. Employers should also review and update rules and policies regarding confidentiality and security arrangements. Pre-employment vetting of R&D staff is also essential to prevent unexpected breach or non-compliance with trade secret and IP rights.

As a notable (and relatively recent) development, Injunctive relief for trade secret infringement is available in Shanghai and Anhui.

Trading Secrets

Update on Trans Pacific Partnership's Potential Impact on Trade Secret Law

By Eric Barton (October 16, 2015)

As the 2016 presidential race moves into the debate phase, one issue sure to get more and more attention is the proposed Trans Pacific Partnership ("TPP"). In simplest terms, the TPP is a proposed trade agreement between twelve Pacific Rim countries, including the United States, concerning a wide variety of matters of economic policy. Together, the countries account for 40 percent of world economic output. After years of negotiations, an agreement was recently reached on October 5, 2015 after marathon talks in Atlanta, Georgia.

Before negotiations ever began, each of the TPP countries signed confidentiality agreements promising to maintain the secrecy of the negotiations, including the specific terms and provisions being debated. As a result, even though a "deal" has been reached, the exact terms of that deal remain a mystery. That said, before the TPP can become official, the text of the agreement has to be signed and ratified in accordance with the procedures of each of the twelve countries involved. In the United States, that means Congress must accept or reject the TPP within 90 legislative days once the deal is formally submitted for review. According to Politico, many expect Congress to vote on the bill either during the Summer of 2016 or in the lame-duck session after the 2016 elections.

The final terms of the TPP will obviously need to be provided to Congress before any vote can be taken. In the meantime, however, WikiLeaks has been publishing purported "drafts" of the TPP on a regular basis since 2013. According to these leaked materials, the TPP will include a chapter on intellectual property covering copyright, trademarks, and patents, as well as trade secrets. These disclosures are consistent with a public statement from Office of the United States Trade Representative, indicating that each of the TPP countries have agreed that they will "provide strong enforcement systems, including, for example, civil procedures, provisional measures, border measures, and criminal procedures and penalties for commercial-scale trademark counterfeiting and copyright or related rights piracy. In particular, TPP Parties will provide the legal means to prevent the misappropriation of trade secrets, and establish criminal procedures and penalties for trade secret theft, including by means of cyber-theft […]."

One recently leaked "draft" of the TPP includes language requiring TPP signatories to follow the trade secret language found in the Agreement on Trade Related Aspects of Intellectual-Property Rights (commonly referred to as "TRIPS"), which is essentially the same as the trade secret language in the Uniform Trade Secret Act. The leaked documents also indicate that the TPP will move many aspects of trade secrecy into the realm of criminal law, which would obviously be a fairly fundamental change to the focus of current trade secret law, where it is generally treated as a purely civil matter. That said,

only when the “official” TPP is finally revealed will we be able to analyze its actual terms. Based on the leaked versions, though, several groups have already begun publishing highly critical commentaries on the TPP’s various proposals for handling intellectual property rights.

It will also be extremely interesting to see how the TPP’s provisions regarding trade secrets interacts with the proposed Federal Trade Secret Legislation recently introduced in the United States’ House and Senate. For more on that, please follow this link to Seyfarth’s ongoing updates. Suffice it to say, 2016 is already shaping up to possible be a watershed year for trade secret legislation on multiple fronts.

Trading Secrets

Proposed US and EU Trade Secrets Laws Progress but Unlikely to be Enacted This Year

By Daniel P. Hart (October 30, 2015)

There's no doubt that protection of trade secrets is a major concern for most businesses operating in today's global economy. As we have previously discussed, a few years ago CREATe.org and PwC US released a report that highlighted how far-reaching and deeply challenging trade secret theft is for companies operating on a global scale. Notably, in their report, CREATe.org and PwC estimated that trade secrets theft costs anywhere between 1-3% of the GDP of the United States and other industrial economies.

To address the threat to the trade secrets of US businesses, earlier this year Senators Orrin Hatch (R-UT) and Christopher Coons (D-DE) introduced the "Defend Trade Secrets Act of 2015" (S. 1890) in the United States Senate, while Rep. Doug Collins (R-GA) introduced an identical version of the same bill (H.R. 3326) in the United States House of Representatives. As we discussed here, if enacted, the Defend Trade Secrets Act would provide a civil cause of action in federal court to private litigants 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." In addition, the bill seeks to (1) create a uniform standard for trade secret misappropriation by expanding the Economic Espionage Act; (2) provide parties pathways to injunctive relief and monetary damages to preserve evidence, prevent disclosure, and account for economic harm to companies; and (3) create remedies for trade secret misappropriation similar to those in place for other forms of intellectual property.

Both bills have garnered widespread bipartisan support and are currently pending review by the Judiciary Committees in each chamber. As of publication of this blog post, the Senate bill has 10 cosponsors (6 Republicans, 4 Democrats), while the House bill has 62 cosponsors (42 Republicans, 20 Democrats). Given the bi-partisan and bi-cameral nature of the bills, many commentators have predicted that the Defend Trade Secrets Act of 2015 stands a very strong chance of becoming law. Nevertheless, given the current status of the bills in committee, it is unlikely that either bill be scheduled for a floor vote by the end of the year. Staff on Capitol Hill report that, while the House's bill's sponsors hope to see committee action by Christmas, the Chairman of the House Judiciary Committee has only committed to moving the legislation, not to a specific time frame. The Senate bill likewise currently has no scheduled date for Judiciary Committee action.

Meanwhile, across the Atlantic, the European Commission's proposed Directive to protect trade secrets has now crossed most procedural hurdles necessary for a first reading in the European Parliament. As we discussed here, the proposed Directive (if enacted) would substantially alter the legal landscape in Europe regarding trade secret protection and would require all member states to

provide certain minimum standards of legal protection for trade secrets. Earlier this year, the European Parliament's Committee on the Internal Market and Consumer Protection and Committee on Industry, Research and Energy both reviewed the proposed Directive and published their comments and recommended amendments to the proposal. The Parliament's Committee on Legal Affairs subsequently published its own report, which includes the other committees' reports and a draft resolution for vote by the European Parliament.

In its draft resolution, the Committee on Legal Affairs accepted some of the amendments proposed by other committees, particularly amendments to address concerns that the proposed Directive could have an anti-competitive impact or could be used to chill free expression. Among other proposed amendments, the Committee on Legal Affairs has made the following amendments:

- Adding language to clarify that the Directive "does not provide any ground to trade secret holders to limit the use of experience and skills honestly acquired by employees in the normal course of their employment or to add any restriction for employees to occupy a new position, to those provided for in their employment contract, in compliance with relevant Union and national law;"

- Adding language to emphasize the importance of trade secrets protection for small and medium-sized enterprises ("SMEs");

- Adding language to clarify that the measures and remedies provided under the Directive should not restrict whistleblowing activity and the safeguard the freedom of the press;

- Changing the statute of limitations for trade secrets misappropriation claims to three years (the Commission's original text proposed a limitations period of "at least one year but not more than two year after the applicant became aware, or had reason to become aware, of the last fact giving rise to the action");

- Amending the Directive's remedies for protection of trade secrets during litigation to ensure that "those restrictions should not be such as to prevent at least one person from each of the parties and their respective legal representatives from having full access to all the documents in the file" (in contrast, the Commission's original text was written broadly enough to permit "Attorneys' Eyes' Only" protective orders like those commonly used in litigation in the U.S.).

With the publication of a draft resolution, the proposed directive now awaits a vote in the European Parliament upon the conclusion of additional negotiations between the Parliament and the Council of the European Union (which has already reached an agreement on a general approach for establishing a new legal framework for the protection of trade secrets). Staff of the European Commission in Brussels have reported to us that the Council and the Parliament are attempting to reach an agreement that would permit adoption of the proposed directive on a first reading in the Parliament. Currently, the European Parliament is expected to vote on the initiative around March 2016, but the precise date for a first reading has yet to be determined.

We will continue to track developments on both sides of the Atlantic as these proposed measures continue to be considered in the U.S. Congress and in the European Parliament.

Trading Secrets

Dan Hart is a Partner at Seyfarth Shaw's Atlanta office and will be presenting "Protection of Trade Secrets in the US, EU, and Other Countries" at the International Technology Law Association's 2015 European Conference, which will be held in London from November 4-6. More information about the conference can be found here.

Trading Secrets

Australia Non-Compete Update: the Difference Between Winning and Losing Restraint Litigation is Often Good Housekeeping

By Michael Tamvakologos and Justine Giuliani (December 11, 2015)

An enforceable restraint of trade can be a key business asset. Or some might think about it as an insurance policy. The capacity to preserve customer connections, protect confidential information and discourage key executives from setting up their own business or moving to a competitor can be critical to information rich businesses operating in a competitive market. Ensuring the currency of your restraint provisions is an important exercise in risk management.

Experience in this area demonstrates one key distinction which separates cases where restraints are successfully upheld and those where compromise outcomes are achieved. In successful cases, typically, the restraint provision has been drafted quite neatly around the key protectable interests. When seeking to enforce a restraint, an employer will be required to show there is a protectable interest capable of supporting the restraint. This is the first limb of the test for enforceability. The scope, duration and geographical operation of the restraint are logically tied to the protectable interest (see our map below). An employer will need to make out each of these elements to meet the second limb of the test.

This success can be attributed to the practice of regularly revisiting the questions of which key executives or employees should be subject to restraints, and how those restraints should operate. The yearly promotion, pay rise or management re-shuffle cycles are perfect opportunities to update restraint provisions. Often, this is when operational changes (such as the make-up of roles) become effective, so restraints can be tweaked to align with these changes. A promotion or pay rise can be tied to a new contract or restraint provision. Instead of adopting a one-size-fits-all approach when an employee first joins the business, employers can increase the likelihood that a restraint will be enforceable by showing it was the subject of specific negotiation during the employment.

Trading Secrets

What does the Trans Pacific Partnership mean for IP in Australia?

By Justine Turnbull and Cassie Howman-Giles (December 15, 2015)

The Trans Pacific Partnership Agreement ("TPP) between twelve Pacific Rim counties, including Australia and the United States, was finally made public on 5 November.

The text of the Agreement will now be reviewed by various parliamentary committees before Parliament votes on legislation to implement the Agreement in Australia, likely to be in February or March next year. If the implementing legislation is passed in Australia and the other signatory countries, the Agreement will be ratified and come into force. It is expected that it could take up to two years before the Agreement comes into force in all 12 signatory countries.

The intellectual property provisions of the TPP Agreement are contained in Chapter 18. Chapter 18 includes a number of measures designed to protect intellectual property rights, many of which reflect Australia's current intellectual property laws. However, a number of concerns have been raised including by the Australian Competition and Consumer Commission (ACCC), Australia's competition regulator, in its submissions to the Productivity Commission. The ACCC is concerned that some of the provisions in Chapter 18 may "*tilt the balance in favour of IP rights holders to the detriment of competition and consumer*s". In addition, the ACCC has warned that the investor-state dispute settlement provisions (which give foreign companies the right to sue the Australia government for introducing laws which harm their interests) "*risk impeding domestic reforms in the public interest*".

The biggest change to intellectual property law in Australia which will result if the Agreement is implemented in its current form is Australia would be required to implement criminal procedures and penalties for acts including the unauthorised misappropriation of trade secrets. Currently in Australia the only action which can be taken against a person or company who misappropriates trade secrets is a civil claim for breach of confidence. The Agreement also does not make clear what defences will be available to those alleged to have misappropriated trade secrets which is concerning for journalists and whistleblowers.

At this stage, it is still a case of wait and see. Various bodies are expected to conduct further analysis on the provisions of the Agreement to determine the likely impact on Australia. Also, depending on Parliament's assessment of the implementation legislation, the Agreement may need to be renegotiated or side letters entered into to address any issues.

Proposed EU Trade Secrets Directive Crosses Another Hurdle with "Provisional Agreement" Between Council and Parliament

By Daniel P. Hart (December 21, 2015)

As regular readers of this blog will note, we have been tracking progress of the European Commission's proposed Directive to protect trade secrets as it has made its way through the European Union's complicated legislative process over the past several years. Last week, the proposed Directive crossed yet one more procedural hurdle with a "provisional agreement" on the Directive reached by the European Council (represented by the Luxembourg presidency) and representatives of the European Parliament.

The European Commission first proposed the Directive in November, 2013 to provide greater and more consistent protection of trade secrets throughout the EU's 28-Member States. Earlier this year, the European Parliament's Committees on Internal Market and Consumer Protection and Industry, Research, and Energy published comments and proposed amendments to the Directive. The Parliament's Committee on Legal Affairs subsequently issued a draft Legislative Resolution that adopted some (but not all) of the amendments proposed by the other committees. The provisional agreement now clears the way for a vote in the European Parliament next year.

Although the text of the provisional agreement is not currently available, a press release issued by the European Council provides a general overview of the terms. As expected, the proposed Directive will provide that EU member states must ensure that adequate civil procedures and remedies are available to redress illegal acquisition, use, and disclosure of trade secrets without undermining fundamental rights and freedoms or the public interest. Consistent with concerns raised (and amendments proposed) by the Parliamentary committees that previously reviewed the proposed Directive, the Council and representatives of the European Parliament agreed that the proposed Directive (i) will protect whistleblowers, (ii) will not place any limitations on investigative journalism, (iii) will not place any restrictions on workers in their employment contracts, and (iv) will not affect employees' rights to enter into collective bargaining agreements.

In addition, the press release suggests that the Council and representatives of the Parliament have reached an agreement about the limitations period for claims of trade secret misappropriation. The Legal Affairs Committee's draft resolution from earlier this year provided that "Member States shall ensure that actions for the application of the measures, procedures and remedies provided for in this Directive may be brought within three years after the date on which the applicant became aware, or

had reason to become aware, of the last fact giving rise to the action." While this three-year limitations period is longer than the Commission's original text (which proposed a limitations period of "at least one year but not more than two years), it is still somewhat short by comparison to the existing limitations period in some EU member states. (For example, in the UK, a common law claim for breach of confidence or breach of contract is six years.) Based on the European Council's press release, it is now clear that the Council and representatives of the European Parliament have agreed on a limitations period that "**will not exceed six years**."

The press release is less clear on the protections that will be available to trade secrets during litigation. The Commission's original text provided that:

Member States shall also ensure that the competent judicial authorities may, on a duly reasoned application by a party, take specific measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of the legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret. The measures referred to . . . shall at least include the possibility: (a) to restrict access to any document containing trade secrets submitted by the parties or third parties, in whole or in part; (b) to restrict access to hearings, when trade secrets may be disclosed, and their corresponding records or transcript. In exceptional circumstances, and subject to appropriate justification, the competent judicial authorities may restrict the parties' access to those hearings and order them to be carried out only in the presence of the legal representatives of the parties and authorised experts . . .

In other words, the original text contemplated "Attorneys' Eyes Only" protective order like those that are typically used in trade secrets cases in the U.S.

In contrast, in its draft Legislative Resolution, the Legal Affairs Committee watered down this language with the following proposed language that would appear to eliminate true ""Attorneys' Eyes Only" protective orders:

The measures referred to . . . shall at least include the possibility: (a) to restrict access to any document containing trade secrets or alleged trade secrets submitted by the parties or third parties to a limited number of persons, in whole or in part ***provided that at least one person from each of the parties***, and, where appropriate in view of the proceedings, their respective lawyers and/or legal representatives, are given access to the document in full; (b) to restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed, and their corresponding records or transcript to a limited number of persons,***provided that it includes at least one person from each of the parties***, and, where appropriate in view of the proceedings, their lawyers and/or legal representatives . . .

Unfortunately, the Council's press release does not explain how the provisional agreement resolves this conflict but states only that "[w]here necessary, confidentiality of trade secrets will also be preserved during the course of and after the legal proceedings."

Now that the provisional agreement has been reached, the Parliament and Council will conduct a legal-linguistic review of the text. Once that process has been completed, the proposed Directive will then be submitted to the full European Parliament for approval. Currently, the European Parliament is expected to vote on the initiative around March 2016, but the precise date for a first reading has yet to be

determined. If enacted, Member States will be required to enact national law consistent with the Directive within two years.

We will continue to track progress of the proposed Directive, as well as the proposed Defend Trade Secrets Act in the U.S. Congress (which currently has 20 co-sponsors in the Senate and over 100 co-sponsors in the House). In the meantime, companies on both sides of the Atlantic should review their current procedures for protecting trade secrets to ensure that they can fully take advantage of these proposed laws if enacted next year. For practical tips on ways to maximize protection of trade secrets in the workplace, please check out the best practices highlighted in our 2014 webinar series.

Trading Secrets

Leveraging Employment Restraints to Protect Business Assets

By Michael Tamvakologos (December 18, 2015)

When a key employee subject to an employment restraint leaves a business to join a competitor, fast decisions need to be made to protect client goodwill or guard against misuse of confidential information.

The more leverage an employer has against the former employee and his or her new employer, the better the prospects of negotiating a sensible solution quickly or, failing that, taking successful legal action.

Set out below is a summary of the key legal touch points:

SEYFARTH SHAW

TAKING ACTION–LEGAL TOUCH POINTS

Retrieving emails and other company information	*Document preservation and collection* *Information technology hardware and server review* *Opponent document preservation requests*
Seeking undertakings/agreement from former employee/new employer as to future conduct	*Pre-litigation discovery* *Discovery/subpoena* *Anton Piller orders*
Obtaining information from former employees or third parties	*Using court rules* *Discovery and subpoena* *Preliminary discovery orders*
Stopping the conduct	Ex parte Interlocutory Final Injunctive relief
Recovering losses	Liquidated damages Lost client profits "At-risk" client profits Legal costs – Former employee or new employer?

TACTICAL

- Who to sue?
- Where to sue?
- Orders – Restraining/ Confidentiality
- Usual undertaking as to damages
- Timing
- Negotiation
- Litigation entry and exit strategy

PROTECTING BUSINESS GOODWILL

- ☑ Client contact and support transition program
- ☑ Employee communications
- ☑ Market communications
- ☑ Media strategy

Proving loss

One issue that looms large in these situations, particularly where the decision taken is to start legal action, is proving that the business has suffered financial loss. Often, there are no immediate financial losses in the wake of the employee's departure. It may be some time before conduct in breach of the restraint hits the business' bottom line. The easier it is to prove loss, the more confident will be the decision to proceed with a damages case.

Some employers try to side step this difficulty by including a "liquidated damages" clause in the restraint provision. Such a clause specifies up front the financial damage that will be caused to the employer if the restraint is breached. For example, in the accounting profession, it is not uncommon to see liquidated damages provisions which describe likely losses as two, three or even four times annual revenue, for a particular client if that client was to move their business because of breach of the employment restraint.

In theory, it is easier to prove loss where a liquidated damages provision is included in the contract because the former employee and the employer have agreed up front what the damage will be if the restraint is breached. It also provides a clear starting point for negotiations if the dispute takes that path.

But in practice, there's more to it than that:

- Liquidated damages provisions can be attacked on the basis that they are a penalty under law and unenforceable.

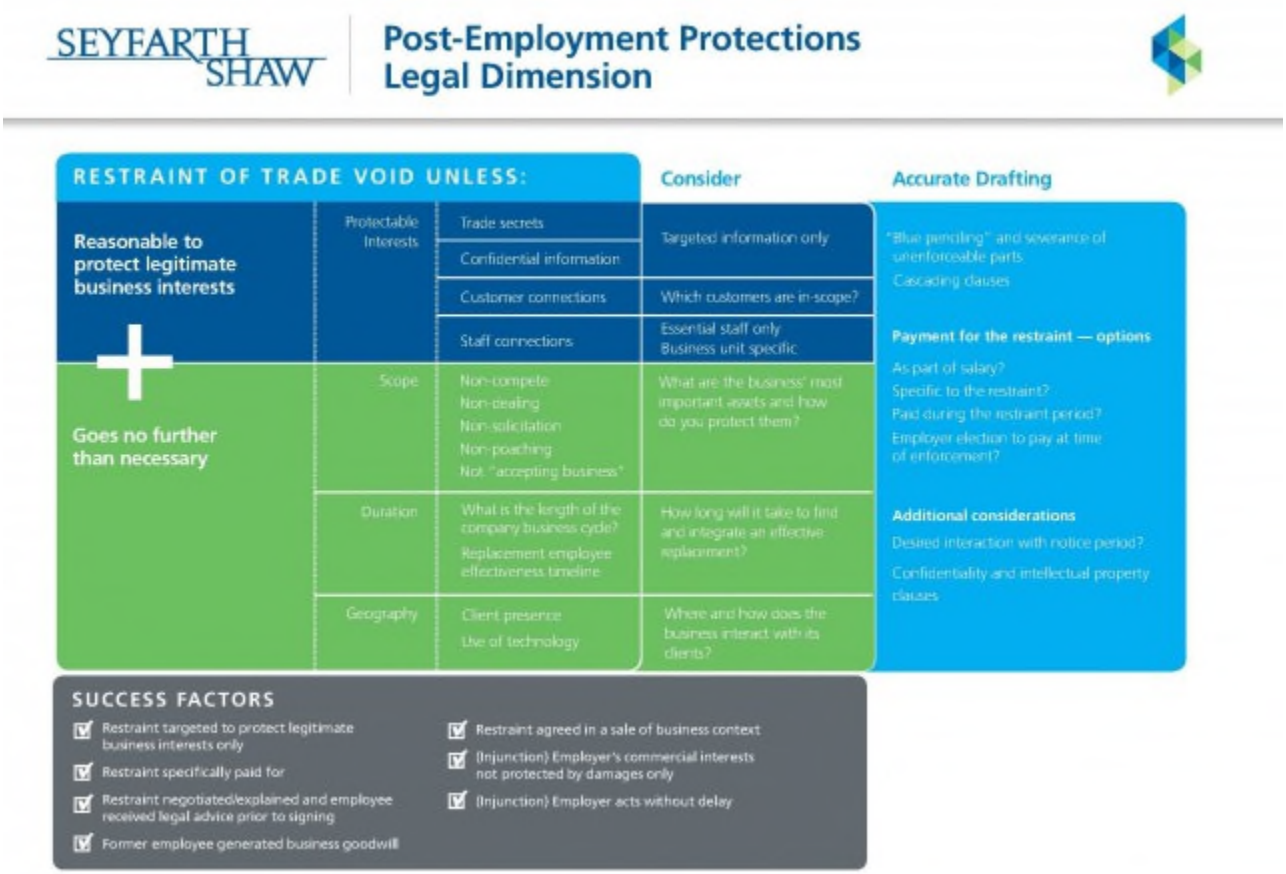
- Courts may be reluctant to give the employer an injunction to stop an actual or threatened breach of the restraint if it appears that damages will be an adequate remedy. Liquidated damages provisions arguably suggest that damages will be adequate (and more easily assessed) if in fact the former employee has breached their employment restraint.

Is it worth including a liquidated damages provision in an employment restraint?

A lot turns on what is accepted practice in the particular industry and which assets of the business are being protected (our restraint map below shows the key protectable interests). If a liquidated damages provision is to be included in the contract, it is important to draft the provision carefully so that it is (a) enforceable and (b) doesn't cut down the other options available to an employer (such as a court-ordered injunction to stop the breach).

This will ensure that the leverage the business needs is there when it is needed most.

Trading Secrets

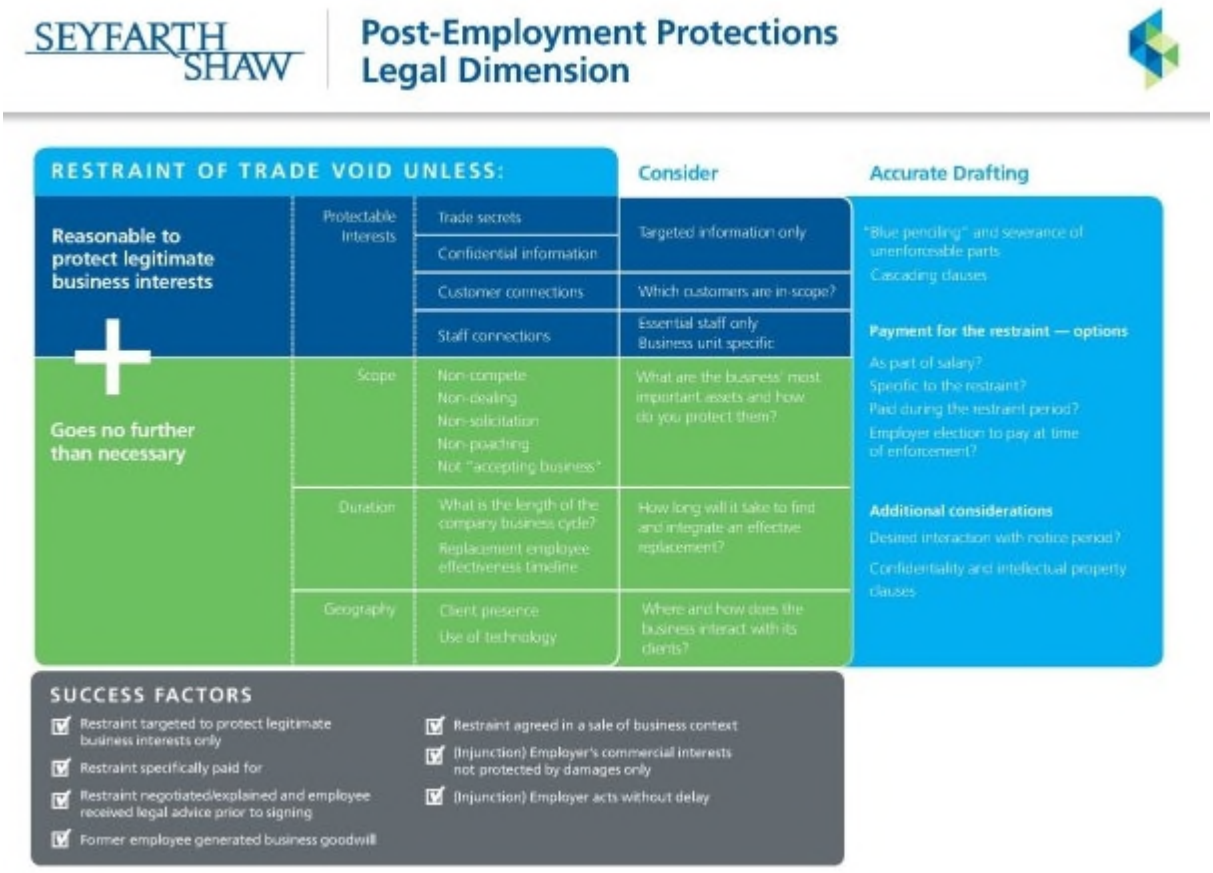


Trading Secrets

Drafting and Litigating Post-Employment Restrictive Covenants in Australia – Tailoring Your Restraint to Ensure the Right Fit

By Michael Tamvakologos and Justine Giuliani (December 22, 2015)

We will now look at the different types of post-employment restrictive covenants, and work through a checklist of questions employers should ask themselves when drafting a restraint to make sure it's the right fit.



A good restraint is not about creating the ultimate "catch all" provision. Rather, it requires a series of good choices to be made that protect the most important business assets. Whilst Australian and English courts have on occasion upheld "cascading" restraints (which might, for example, operate for 12, 9 or 6 months, whichever time period a court finds is enforceable) in practice, cascading restraints can lead to business uncertainty. This is because it is not clear when the employee leaves which time period will be enforceable.

Trading Secrets

Think commercially first and about the legalities second

The starting point is to ask, what is the restraint trying to protect? These are the assets of the business that would be most vulnerable if a particular employee left. In order for a restraint to be enforceable, it must be reasonable to protect a legitimate business interest. Australian courts have recognised that an employer's trade secrets, confidential information, customer or client connections, and staff connections are all protectable interests that are capable of supporting a restraint.

What legal tools can you use?

The next question is, what is the most effective way to protect the identified interest? This is about choosing a restraint that is targeted because the wider the restraint, the less likely it is that a court will consider it reasonable to protect this interest. Broadly, there are four different types of restraint that can be used either as a stand-alone provision, or in combination.

Non-compete

A pure non-compete restraint is the most difficult to enforce because it prevents an employee from working for a competitor of the former employer in any capacity.

An employer can increase the likelihood that a non-compete restraint will be enforceable if they can show it was the subject of specific negotiation (either at the time the employment contract was entered into, or during the employment), or it is accompanied by provisions for payment tied to the period of the restraint to minimise financial disadvantage to the employee whilst he or she is out of the employment market.

A non-compete restraint can be used where other forms of protection would be inadequate to protect the employer's interest. This may occur where an employee possesses specific confidential information obtained during the course of their employment, or more commonly where they acted as the face of the business and the custodian of key client relationships. The courts have recognised that a standard confidentiality clause or non-solicitation restraint may not provide adequate practical protection in these circumstances.

Non-solicitation

A non-solicitation restraint is designed to protect customer connections or the goodwill of the business by preventing an employee from enticing away customers or clients of their former employer. As a rule, a non-solicitation restraint should be restricted to customers or clients with whom the employee had a meaningful relationship, or provided services on a continuing basis. This is because a restraint which applies to all customers or clients of the business, including those with whom the employee had no contact, is likely to go beyond what is reasonably necessary to protect the employer's interest.

Non-dealing

A non-dealing restraint prevents an employee from accepting instructions or business from former clients where it is the client who makes the approach or initiates contact. This type of restraint has its advantages, including that it overcomes the problem of proving actual solicitation by a former employee – often a contentious point in litigation.

Non-poaching

As the name suggests, a non-poaching restraint prevents an employee from poaching other employees of their former employer. Employers should discriminate between employees who are critical to their business and those who are not, and draft the restraint so that it applies to this specific class. The case law shows that a restraint on employment that casts the net too wide and prohibits the solicitation of any employee right down to the "tea lady" is unlikely to be enforceable.

Finally, employers should test the restraint by looking for, and addressing any areas of potential vulnerability. These are the points of attack an opponent might raise if the enforceability of the restraint is ever tested in court. For example, providing an employee with an explanation of the restraint and the reasons for it, and giving him or her the opportunity to obtain legal advice before committing to the restraint, feature in a number of cases where a restraint was upheld (see the "success factors" in our map above).

Updating the restraint

Like any piece of valuable equipment, a restraint needs to be routinely maintained. Where an employee changes position, or the business diversifies its services or product lines or takes on particularly important clients, the restraint should be updated. This could be done, for example, by way of a contract refresh tied to the annual pay review or promotion cycle.

Putting in place a system to administer effective restraint provisions will ensure that you have a targeted restraint in place at the time you need it most, when business assets are at risk.

Please contact any of our partners to discuss the relevant legal touch-points or to access our unique online post-employment restraint solution. We encourage you to leave a comment below.

Trading Secrets

Restraint Payments in Australia – Compliance Issues

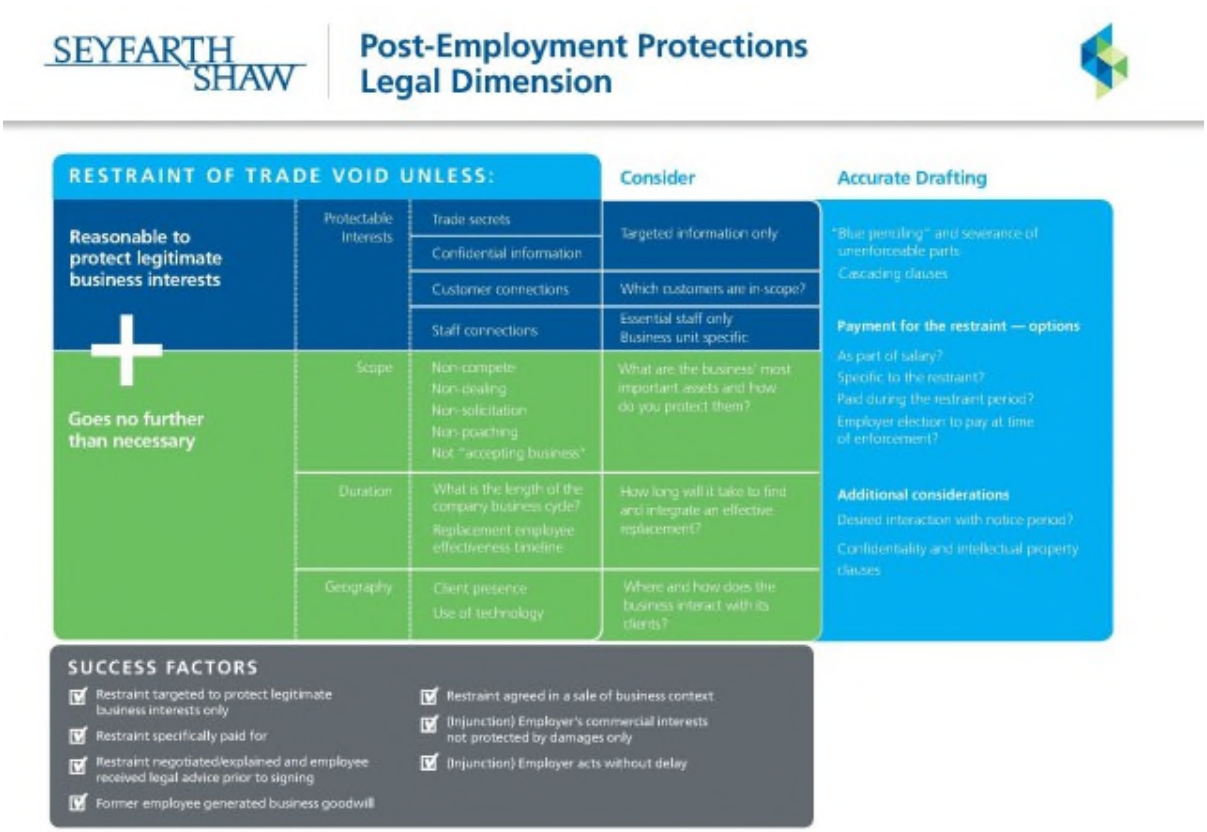
By Michael Tamvakologos and Justine Turnbull (December 28, 2015)

In the latest of our series of post-employment protection blog posts, we consider the compliance and regulatory issues that need to be thought through when drafting an effective post-employment restraint in Australia.

How will any restraint payment be structured?

The threshold question is what kind of payment (if any) to make in return for the agreement of an employee not to engage in particular activities, such as working for a competitor, soliciting business from clients, etc. The best option will depend on the particular circumstances.

Payment could be part of normal salary. There could be a separate lump sum payment which is paid when the agreement is made or at the time the restraint is called on. Alternatively, an employer might wish to drip feed monthly payments during the restraint period. There are a number of ways to structure the arrangements that best suit the business and the employee concerned.



It is also possible for no specific payment to be made in return for the restraint. However, at a practical level, paying an individual not to engage in certain activities such as working for a competitor or poaching staff might mean the obligations are more likely to be complied with. For example, an executive who is not "out of pocket" during the restraint period is less likely to need to take the risk of working for a competitor.

From a purely legal perspective payment does not guarantee enforceability. When the payment is made and the quantum are discretionary matters to be taken into account by a court asked to enforce a restraint. In our experience, it is very helpful to be able to point to payment in return for agreement to be restrained.

Payment for a restraint will, of course, raise a number of regulatory disclosure, approval and tax issues.

"Gardening leave" compared to a post-employment restraint

At the outset it's important to distinguish between:

- payment of salary during a period of notice of termination where the employee is not required to work, which is referred to commonly as "gardening leave" because the employee cannot commence working for another employer but can engage in leisure activities such as gardening (**Notice Payments**); and

- additional payment/s made after termination of employment in return for the former employee's agreement to be prevented from engaging in certain activities such as working for a competitor or approaching their former clients, suppliers or colleagues (**Restraint Payments**).

Notice Payments will not raise the same issues as Restraint Payments. However, neither payment will guarantee the legal enforceability of the restrictions but will merely be a factor that a court may consider in deciding whether the restrictions are reasonable. The argument is that the payment will go some way to addressing the public policy concern about restraints to the effect that they should not deprive a person of their ability to earn a living.

Termination benefits requiring shareholder approval

In the case of certain executives (broadly "Key Management Personnel" as defined in the *Corporations Act 2001* and directors) Restraint Payments may also require the approval of shareholders in general meeting if they are in connection with termination of employment or the transfer of any undertaking or property of the company. This is because the corporations legislation in Australia specifically deems a payment that is made as part of "a restrictive covenant, restraint-of-trade clause or non-compete clause" a benefit that requires shareholder approval.
Whether such approval is required must be determined on a case by case analysis. Generally, Notice Payments will not be caught by this requirement.

Board determination of "reasonableness" of the payment

For some executives a company's board of directors may also have to determine whether a Restraint Payment is "reasonable" in the context of the limits on payments to related parties under the corporations legislation. This is an issue that should be considered at the time a restraint provision is drafted and agreed. If a benefit is not considered reasonable then it will require shareholder approval.

External advice may need to be taken by a board to assist its determination of whether a proposed payment is reasonable.

Disclosure

Corporations legislation and the Listing Rules of the Australian Securities Exchange impose obligations on companies to make disclosures about executive pay, including Restraint Payments and Notice Payments, in certain circumstances. Whether a payment is ultimately disclosed publicly may be a relevant consideration in deciding whether the payment is commercially acceptable to both the executive or employee and the company. On this basis any potential disclosure obligations should be considered at the time of drafting and agreeing payment obligations for restraints.

Taxation

Finally, the tax treatment of a Restraint Payment may be different to the tax treatment of a Notice Payment, depending on whether the Restraint Payment is categorised as an employment termination payment or a capital payment. Specific consideration of this issue will also be required.
Well-drafted restraints of trade are a necessary and reasonable business tool and can be highly effective to protect business interests. To be enforceable, and to prevent side issues becoming a problem, the above matters need to be carefully thought through at the time the restraint is drafted and agreed.

Social Media and Privacy

Trading Secrets

Privacy & Security Are Back on the Agenda in DC

By John Tomaszewski (January 14, 2015)

The plethora of security incidents in the news have once again put security front and center of the international agenda. Predictably, this has triggered a number of responses from governments around the world. Some of these responses seem to have been ill-considered. However, one of the more comprehensive responses came out of the US President's address to the Federal Trade Commission last week. A series of laws were proposed to address the increasing risks which are confronting individual security and privacy rights.

The President's remarks at the FTC gives some valuable insight into where the US regulatory environment may end up in the next year or so. As a part of this analysis, one should focus on two very different agendas: Privacy and Security. These issues, while similar, are very different. Case in point, the UK PM's comment around banning encryption could well result in increased security. However, it will absolutely damage individual privacy (and arguably also damage commercial security).

Security Breach Notification

President Obama has proposed a national standard for security breach notification. This is not the first time this proposal has been placed on the legislative agenda. While this is a step in the right direction, as is always the case, the devil is in the details.

One of the most challenging issues to deal with regarding a security breach is "what data" is impacted, and "does it matter"? In essence, the definition of "personal information" and the "harm" v. "access" triggers are the primary headache for those dealing with whether or not they have to provide notice. Elsewhere in the world, "personal information" is very broadly defined. Historically, the limiting definition of "personal information" was supposed to avoid over-notification. As has been pointed out, this does not seem to have worked.

Practically, it would be more useful to standardize the notice trigger around the concept of "harm". This would operate to make the definition of "personal information" far less important. In effect, if there is a reasonable likelihood of harming someone with the information breached, a notice would be required. This "harm" concept is a well-established principle of tort law, and one that most lawyers are quite capable of dealing with when given the necessary facts. Removal of a variable always makes a solution more efficient, and the use of a results-driven variable such as "harm" should help avoid any unintended consequences which result in an imprecise definition of "personal information". Let's hope the Administration moves in this direction.

Another component which is concerning is the timing requirement around breach notification. While there have been instances of companies being slow to notify impacted consumers, notice is only going to be useful when you actually know what data was compromised, what was the source of the compromise, and who was responsible for the compromise. While a company may know it was

breached, it may take well over 30 days to determine the scope and reasons for the breach. Without a clear understanding of the scope and reasons for a breach, an arbitrary 30-day notice requirement may lead to additional notice-fatigue. If this legislation is to be actually useful, there will need to be a considered discussion as to when the 30 day clock starts ticking; as well as when that clock can be stopped. Almost all the State breach statutes have a tolling period for law enforcement investigations. Hopefully, any national standard will at least have the same limitation.

Consumer Privacy Bill of Rights

Several years ago, the Obama administration presented a Consumer's Privacy Bill of Rights as part of the US endorsement of the APEC Cross Border Privacy Rules System. There are 7 high-level principles contained in the Privacy Bill of Rights. These are: Transparency, Respect for Context, Individual Control, Focused (read: limited) Collection, Accuracy, Security and Accountability. As is usually the case, the high-level principles sound fine at first blush. However, the way they are implemented may have serious unintended consequences. For example, anti-fraud, development of new services, and IP protection are all activities which may become more challenging if the Individual Control principle does not include appropriate limitations. Additionally, some espouse a baseline set of obligations, regardless of individual choice, should be in place. Others point out that individuals often don't have the time or expertise to exercise control in a meaningful way. Consequently, an over-broad reliance on Individual Choice may actually reduce the privacy protections of individuals.

Remedies

Along with the Privacy Bill of Rights, careful consideration will need to be taken around remedies. Some proposals for law have included private rights of action for violations of privacy. The current trend is to rely on the FTC or State Attorney's General to enforce privacy rights. Regardless of one's position on this issue, it is going to be a significant policy driver, with significant impacts to innovation and business growth. Policy makers and legislators will need input from their constituencies to avoid unintended negative consequences growth.

In anyone's analysis, Privacy and Information Security are going to be hot topics on the agenda for the foreseeable future.

How Far Does the "Internet of Things" Reach?

By John Tomaszewski (February 5, 2015)

With the FTC's 2015 report "Internet of Things: Privacy & Security in a Connected World" ("Report") the idea that more than just computers and phones are able to connect to the Internet. In fact, the Report states that the "IoT explosion is already around us." This is true, and the Report goes on to describe some of the more interesting things that can be connected to the Internet which most of us don't think about (e.g. smart health trackers, smoke detectors, and light bulbs). However, how vast is the actual IoT? And what does that mean to businesses?

As security professionals will tell you, if it has an IP address, it is a potential access point to your network. As such, it is a potential place where a hacker can find a way into your network and then "elevate permissions" into more sensitive parts of a network. This seemed to the be way that several recent large hacks occurred. Thus, the internet of things represents a potential security hole if one doesn't consider all the different devices which can be hacked.

So – what is out there which has the ability to acquire an IP address (and thus is a hacking risk)?

These we know about:

- Desktop Computers
- Laptops
- Tablets
- Smartphones

But what about:

- Copy machines
- Printers
- Fax machines
- VoIP enabled Phones
- Televisions
- Bluetooth headsets

- cash registers (Point-of-Sale terminals generally)
- Handheld barcode readers
- Smart thermostats
- Keycard readers (for doors)
- Security cameras
- Light bulbs
- Environmental control panels
- Lab equipment
- Medical diagnostic equipment
- Warehouse inventory scanners
- The fridge in the break room
- Personal fitness monitors
- Wristwatches (iWatch)
- Armbands
- Glasses

And maybe even…

Shirts and other clothes.

As each one of these neat bits of technology start to take hold companies which allow them into the physical range to connect with the corporate network will need to have a strategy to manage the security risks inherent in all of them.

It's not going to get any easier…

Aspects of Private Social Media Groups May Be Protectable Under Illinois Trade Secret Law

By Christopher Baxter (May 28, 2015)

In Illinois federal court, a plaintiff alleged aspects of their LinkedIn group were trade secrets misappropriated by the defendant. The defendant moved to dismiss for failure to state a claim. The court denied the motion in part and granted in part, ruling that portions of social media groups may be protectable under the state's trade secret law. *CDM Media USA, Inc. v. Simms*, Case No. 14-cv-9111 (N.D. Il., Mar. 25, 2015) (Shah, J.).

Summary of the case

This case concerns the ownership rights to private social media groups. The plaintiff, CDM Media USA, created a private LinkedIn group for CIOs and other IT executives interested in CDM events. The defendant, Robert Simms, was the point person for this group while he was employed at CDM. When Simms resigned from CDM, he allegedly refused to return the group's membership list and communications to CDM and later allegedly used the materials to compete against CDM by attempting to solicit CDM's current and potential customers and vendors. CDM filed suit alleging, among other things, violation of the Illinois Trade Secrets Act. Simms filed a motion to dismiss for failure to state a claim. The court denied the motion with respect to the group's membership list but granted the motion with respect to "confidential information" contained in the group.

Legal standards under the Illinois Trade Secrets Act

A claim under the Illinois Trade Secrets Act requires the plaintiff allege (1) they have a trade secret (2) that was misappropriated (3) using the defendant's business. "Trade secret" under the act requires the information sought to be protection derive economic value from its secrecy and that the information be subject to reasonable efforts of secrecy and confidentiality.

The Court's ruling

Regarding the group's membership list, the Court denied the motion to dismiss stating there was too little known about the contents, etc. of the group at the present stage of litigation to rule on the issue as a matter of law, without further factual inquiry. However, the Court granted the motion to dismiss regarding the "confidential information" contained in the group stating CDM's blanket allegations, i.e., that the LinkedIn group contained confidential information, were insufficient. According to the Court, the plaintiff must allege certain messages or classes of messages contain trade secrets and what it is about the messages that satisfy the trade secrets definition.

Trading Secrets

Takeaways

Whether or not membership lists of private social media groups are protectable under Illinois trade secret law will likely depend on the privacy/confidentiality measures employed to protect to information and whether the information economic value from its secrecy. Regardless, it is safe to say that in no circumstances will a public group's membership list be protectable because they lack a fundamental tenet of trade secret law, i.e., the information must be "secret." Moreover, information contained within a private social media group, such as messages, may be protectable. However, for protection to exist, information within the group desired to be protected must be identified with some specificity and have independent economic value.

Webinar Recap! Employee Social Networking: Protecting Your Trade Secrets in Social Media

By John Tomaszewski, Eric Barton, and Daniel Joshua Salinas (June 9, 2015)

We are pleased to announce the webinar "Employee Social Networking: Protecting Your Trade Secrets in Social Media" is now available as a podcast and webinar recording.

In Seyfarth's fourth installment of its 2015 Trade Secrets Webinar series, Seyfarth attorneys addressed the relationship between trade secrets, social media, and privacy.

As a conclusion to this well-received webinar, we compiled a list of key takeaway points, which are listed below.

- *Social Media Privacy Laws are on the Rise.* At least 20 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 "nonpersonal" accounts and on suspected data theft or workplace misconduct. To learn more, please see our *Social Media Privacy Legislation Desktop Reference*.

- *Safeguard Your Trade Secrets.* Protecting your company's valuable confidential information and trade secrets from disloyal employees is a very different exercise than keeping strangers and competitors locked-out. This exercise is further complicated by inconsistent privacy legislation, which can vary wildly from state-to-state. 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?

- *Social Media and BYOD.* Social media is an extension of the trend to combine work, and non-work related activities within the same platform. Just like smartphones allow you to engage in both work, and non-work related emailing, the social media platforms continue to drive the conflation of personal and employee activity. As a result, a holistic approach needs to be taken in managing the employee. Otherwise, what was once considered a reasonable policy at work may get applied to private or protected activity and thereby become at a minimum, unreasonable; and in some cases illegal.

Inside Views: The Intersection Of Trade Secret Law And Social Media Privacy Legislation

By Eric Barton (August 25, 2015)

Eric Barton authored the following article on August 20, 2015 in *Intellectual Property Watch* summarizing several recent cases addressing trade secret claims involving social media issues, as well as providing some suggested takeaways for employers based on the limited information presently available.

There is no question that social media privacy issues now permeate the workplace. In an attempt to provide further guidance and regulation in this area, since April 2012, a growing number of state legislatures in the United States have passed various forms of social media privacy legislation. In fact, to date, nearly all state legislatures, as well as the United States Congress, have considered or are considering some kind of social media privacy legislation.

The precise impact that these new social media privacy laws have on existing trade secret law is still very much in its infancy. Compounding matters, the plain language of several recently enacted privacy laws directly conflicts with judicial decisions regarding "company vs. employee" ownership of social media content that may otherwise constitute protectable trade secrets, including contact lists and business relationships. Moreover, very few court decisions have yet to interpret any of the new social media privacy laws.

In light of this uncertainty, the following is a summary of several recent cases addressing trade secret claims involving social media issues, as well as some suggested takeaways for employers based on the limited information presently available.

A. Definition of a Trade Secret – Brief Summary

In the simplest terms, under the Uniform Trade Secrets Act, which is in effect in 48 states, information and data may qualify for statutory protection if the valuable information ***is*** a secret, and its owner ***keeps*** it a secret. Though there are no bright lines for whether information ***is*** a protectable trade secret, it is likely to be found protectable if it is the result of a substantial investment of time, effort, and expense, generates independent economic value for its owner, is not generally known in the relevant industry, cannot easily be accessed by legitimate means, and cannot be independently reverse engineered without significant development efforts and expense. Experience shows that in many cases, the more egregious a defendant's theft of an alleged secret, the more likely the court will find that the stolen data qualifies as a trade secret. Not merely to punish, but also because an employee's

theft and subsequent use of the stolen data or information itself tends to show (i) the independent economic value of the stolen information, and (ii) the information was not available publicly.

Information is ***kept*** secret if its owner takes affirmative measures to prevent its unauthorized disclosure, such as, but not limited to, non-disclosure, restricted-use, and mandatory-return agreements, confidentiality stamps, limited internal distribution and access permissions, and password protection of computers. Those efforts need only be "reasonable under the circumstances," and "absolute" secrecy is not required.

B. The New Laws' Potential Impact on Account-Content Ownership

The new privacy laws appear to be penetrating trade-secret-ownership lawsuits between companies and their former employees regarding who owns the latters' social media relationships (i.e. LinkedIn contacts). For example, in*PhoneDog v. Noah Kravitz*, No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D.Cal.) (Nov. 8, 2011) and *Eagle v. Morgan*, No. 11-4303, 2011 WL 6739448 (E.D.Pa.) (Dec. 22, 2011), held that the company's Twitter feeds (*PhoneDog*) and the employee's LinkedIn account *(Eagle)* may "belong to" the employer, due to the employer's prior investment of time and expense in developing and maintaining those accounts. Further, in *Ardis Health, LLC v. Nankivell,* 2011 WL 4965172 (S.D.N.Y. Oct. 19, 2011), the court held that the employer owned its employee's account content, due to the employment agreement's spelling that out.

With the onset of social media privacy laws, however, will employees have ammunition to argue that they own their social-media relationships, especially in states where *personal* and *non-personal* accounts are not clearly defined? Employees in trade secrets cases may argue that the new laws imply a degree of ownership of their social media accounts, even where they use them in part to advertise their employers' businesses.

C. Whether the New Laws Will Affect the Protective-Measure Analyses in Trade Secrets Cases

Further, some might argue that unless employers investigate their employees' social-media activities and any related data theft, employers will lose trade secret protection for that data due to their alleged failure to use "reasonable" efforts to protect its secrecy. Recall that under the Uniform Trade Secrets Act section 1(4)(ii), trade secret owners must have employed "efforts that are reasonable under the circumstances to maintain its secrecy." The "reasonable under the circumstances" requirement is often the key disputed issue in trade secrets litigation – the owner claiming that it used reasonable efforts; the alleged thief claiming that plaintiff was too willy-nilly in handling its so-called secrets. Under the new laws, the question presented is whether an employer which could, but does not, investigate an employee's suspected data theft involving his social networking account, has failed to use "reasonable efforts" to protect the data's secrecy.

On the one hand, information that falls into the public domain, or becomes generally known to the relevant industry, usually loses its trade secret status. *See, e.g. Newark Morning Ledger Co. v. New Jersey Sports & Exposition Authority,*31 A.3d 623, 641 (N.J. App. 2011) (trade secrets' "only value consists in their being kept private…if they are disclosed or revealed, they are destroyed"). Similarly, information whose owner intentionally discloses it without imposing a confidentiality obligation on the

recipient is at high risk of losing any secrecy protection. *Seng-Tiong Ho v. Taflove,* 648 F.3d 489, 504 (7th Cir. 2011) (plaintiff's publishing its alleged secrets in trade journals destroyed any trade secret status that information had). An employee's posting confidential employer data on his or her social networking account would pose a significant risk that the data would lose its trade secret protection, especially if the employer was authorized by the applicable privacy law to demand access to the employee's account to investigate, but for whatever reason did not or had policies which did not prohibit such social media activities.

On the other hand, "absolute" secrecy is not required to maintain trade secrecy, but only reasonable efforts to maintain confidentiality. *See, e.g., Avidair Helicopter Supply, Inc. v. Rolls-Royce Corp.,* 663 F.3d 966, 974 (8th Cir. 2011) (efforts to maintain secrecy "need not be overly extravagant, and absolute secrecy is not required"). Indeed, two relevant features of many privacy laws are (i) employer immunity for not investigating suspected misconduct (*see* Michigan, Utah), and (ii) no duty to monitor employee account activity. (*Id.*). Employers faced with a waiver argument may cite these statutory provisions to counter the argument that they were required to investigate reports of employee-account-related data theft, lest they lose statutory protection for that data.

D. Takeaways

Issues related to social media privacy in the workplace are not going away, and we expect to see more litigation and legislation to define acceptable practices in this area. As detailed above, one's ability to differentiate between ***personal*** and ***business*** ownership of information is often extremely difficult. In light of this uncertainty, employers should at a minimum consider doing the following:

1. Determine whether your company has employees in any of the states that have adopted or are planning to adopt social media privacy laws.

2. Review existing policies and agreements regarding employees' use of social media and computer resources for business purposes to ensure that those policies and agreements clearly define ownership and access rights for such accounts.

3. Social media policies should be narrowly tailored and provide examples of protected confidential information.

4. Consider whether to block access to social networking sites not used for business purposes, as well as to other categories of potentially problematic Internet web sites that might be protected under some states' statutes, such as file-sharing and internet-mail sites.

5. Provide recurring training on the company's social media policy confidentiality policies and agreements as well as evaluate the company's computer network in order to reduce the opportunities for incidents of employee misconduct and network security breaches. Remind employees that the same confidentiality policies and agreements that apply in the workplace also apply in their social media activities.

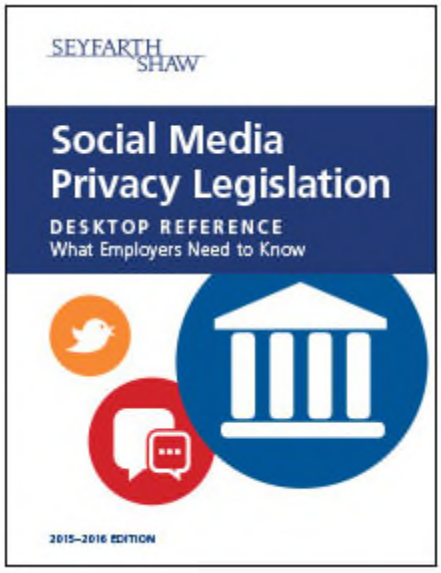
6. Evaluate whether the benefits of a bring your own device policy outweighs the risks to data security confidentiality, and employee privacy.

Trading Secrets

2015-2016 Edition of the Social Media Privacy Legislation Desktop Reference Now Available

By Robert B. Milligan and Daniel P. Hart (September 9, 2015)

Social Media Privacy Legislation Desktop Reference
What Employers Need to Know



There is no denying that social media has transformed the way that companies conduct business. In light of the rapid evolution of social media, companies today face significant legal challenges on a variety of issues ranging from employee privacy and protected activity to data practices, identity theft, cybersecurity, and protection of intellectual property.

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 summarizing existing social media privacy laws by state.
- 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 (BYOD) issues and concerns, social media discovery, and federal law implications.
- Concludes with some best practices to assist companies in navigating this challenging area.

We hope that you find its content useful.

How to get your Desktop Reference:

This publication may be requested from your Seyfarth contact 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 2015-2016 Edition of the Social Media Privacy Legislation Desktop Reference in eBook or hard copy, please click the button below:

Request eBook now

Information Security Policies and Data Breach Response Plans Webinar Now Available!

By Seyfarth Shaw LLP on (October 5, 2015)

We are pleased to announce the webinar "Information Security Policies and Data Breach Response Plans" is now available as a podcast and webinar recording.

With the recent uptick of high-profile data breaches and lawsuits being filed as a result by both employees and consumers as a result, every business should take a fresh look at its information security policies and data breach response plans with two thoughts in mind: compliance with applicable laws, and limiting liability in the event of litigation. Cybersecurity is a critical and timely issue for all businesses. If your company has employees and pays them or gives them benefits, then your company is maintaining their personally identifiable information and faces liability in the event of a data breach.

Currently, there is no comprehensive federal law that sets forth a uniform compliance standard for information security best practices or data breach response plans. Companies operating in the U.S. must comply with a patchwork of 47 different states' laws that set forth a company's obligations in the event of a data breach. In the wake of several high-profile data breaches, state legislators in the U.S. have been updating these state laws in the past few months, adding new requirements.

In addition to dictating how and when a company must respond in the event of a data breach in which personal information has been compromised, a number of these laws also contain substantive requirements about cybersecurity measures a company must take generally. Add into this mix that a U.S. Court of Appeals agreed with the Federal Trade Commission (FTC) that it has the right to file lawsuits against businesses that it deems have lax information security protocols – without informing companies in advance of the standard to which they will be held.

Against this backdrop, Seyfarth attorneys Karla Grossenbacher and John T. Tomaszewski provided a high-level discussion on how businesses can structure an information security program to comply with applicable law and minimize liability – since waiting for a breach is not an option. They discussed, from a legal perspective:

- Essential components of a comprehensive information security policy;

Trading Secrets

- Key elements of a data breach response plan including strategies for state law compliance; and
- Best practices for dealing with third party vendors that store personally identifiable information for your company.

Eric Barton on What Employers Should Know About Where Social Media Password Laws and Trade Secrets Intersect

By Eric Barton (November 2, 2015)

Social media is everywhere nowadays. The line between professional and personal with these accounts is growing more and more blurred. As such, lines designed to protect employee privacy are intersecting with trade secret protection in conflicting ways.

Joining LXBN TV to explain is Seyfarth Shaw attorney Eric Barton—author on the firm's blog, Trading Secrets.

https://www.youtube.com/watch?v=832ksrSRtSY

Trading Secrets

Webinar Recap! Social Media Privacy Legislation Update

By Robert B. Milligan, Daniel P. Hart, and Daniel Joshua Salinas (November 4, 2015)

We are pleased to announce the webinar "Social Media Privacy Legislation Update" is now available as a podcast and webinar recording.

In Seyfarth's eighth installment in its series of Trade Secrets Webinars, Seyfarth social media attorneys discussed their recently released Social Media Privacy Legislation Desktop Reference and addressed the relationship between trade secrets, social media, and privacy legislation.

As a conclusion to this well-received webinar, we compiled a list of brief summaries of the more significant cases that were discussed during the webinar:

- In *KNF&T Staffing Inc. v. Muller*, Case No. 13-3676 (Mass. Super. Oct. 24, 2013) a Massachusetts court held that updating a LinkedIn account to identify one's new employer and listing generic skills does not constitute solicitation. The court did not address whether a LinkedIn post could ever violate a restrictive covenant.

- Outside of the employment context, the Indiana Court of Appeals in *Enhanced Network Solutions Group Inc. v. Hypersonic Technologies Corp*., 951 N.E.2d 265 (Ind. Ct. App. 2011) held that a nonsolicitation agreement between a company and its vendor was not violated when the vendor posted a job on LinkedIn and an employee of the company applied and was hired for the position, because the employee initiated all major steps that led to the employment.

- In the context of Facebook, a Massachusetts court ruled in *Invidia LLC v. DiFonzo*, 2012 WL 5576406 (Mass. Super. Oct. 22, 2012) 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."

- Similarly, in *Pre-Paid Legal Services, Inc. v. Cahill*, Case No. CIV-12-346-JHP, 2013 U.S. Dist. LEXIS 19323 (E.D. Okla., Jan. 22, 2013) 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

- The Virginia Supreme Court in *Allied Concrete Co. v. Lester,* 285 Va. 295 (2013) upheld a decision sanctioning a plaintiff and his attorney a combined $722,000 for deleting a Facebook account and associated photographs that undermined the plaintiff's claim for damages stemming from the wrongful death of his wife in an car accident. The deleted photographs showed plaintiff holding a beer while wearing a T-shirt with the message, "I Love hot moms." Subsequent testimony revealed that the plaintiff's attorney had instructed his paralegal to tell the plaintiff to "clean up" his Facebook entries because "we do not want blowups of this stuff at trial."

- *PhoneDog v. Noah Kravitz,* No. C11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal., 2012) involved a dispute over whether a Twitter account's followers constitute trade secrets even when they are publically visible. The court denied the defendant's motion to dismiss and ruled that PhoneDog, an interactive mobile news and reviews web resource, could proceed with its lawsuit against Noah Kravitz, a former employee, who PhoneDog claimed unlawfully continued using the company's Twitter account after he quit. The court held that PhoneDog had described the subject matter of the trade secret with "sufficient particularity" and satisfied its pleading burden as to Kravitz's alleged misappropriation by alleging that it had demanded that Kravitz relinquish use of the password and Twitter account, but that he has refused to do so. With respect to Kravitz's challenge to PhoneDog's assertion that the password and the Account followers do, in fact, constitute trade secrets — and whether Kravitz's conduct constitutes misappropriation, the court ruled that the such determinations require the consideration of evidence outside the scope of the pleading and should, therefore, be raised at summary judgment, rather than on a motion to dismiss. The parties ultimately resolved the dispute.

- The Second Circuit Court of Appeals in *Triple Play v. National Labor Relations Board*, No. 14-3284 (2d. Cir. Oct. 21, 2015) affirmed an NLRB decision 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. The Facebook activity at issued involved a former employee posting to Facebook, "[m]aybe 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!!!!" A current employee "liked" the post and another current employee posted, "I owe too. Such an asshole." The employer terminated the two employees for their Facebook activity. The 2nd Circuit affirmed the NLRB's decision that the employer's termination of the two employees for their aforementioned Facebook activity was unlawful.

The following is a collection of social media policies that have been implemented by various companies: http://socialmediagovernance.com/policies/. While these policies can serve as a helpful guide, companies should tailor their own social media policies and consult with counsel.

Trading Secrets

Acknowledgments:

Special thanks to Leila Bijan, 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