



The Labouring Oar



Message from the Chair

By Corie Tarara

The Labor and Employment Law Section had a very busy winter! On March 9-10, we held our 7th Biennial Labor & Employment Law Conference at the Hilton Palacio Del Rio in San Antonio, Texas. It was great to meet all those who attended, and from the

feedback received, it was an excellent program! We owe a very big thank you to Phil Kitzer, Brian Rochel, Allison Moore and Caitlin Rider (FBA national), for their work in coordinating the event, as well as all of our speakers, many of whom flew in from across the nation (as far away as Puerto Rico—thank you, Jose!) to provide a great program.

In addition to providing live CLEs, the section has been busy writing as well. We have been given the dedicated issue for the next edition of *The Federal Lawyer*, so we are excited for that opportunity, and greatly appreciate the authors who have submitted articles. Of course, we continue to publish our monthly *Circuit Updates* and *The Labouring Oar*, and could not do so without our dedicated authors. If you are interested in writing, please contact our Publications & CLE co-chairs Whitney Meister or Caitlin Andersen—we are always looking for additional authors to share their knowledge with the rest of the Section.

Our board has seen another change this past quarter that brings us mixed emotions. Our former secretary and publications co-chair, Betsey Chestney, was nominated to serve as U.S. Magistrate Judge for the U.S. District Court for the Western District of Texas, San Antonio Division. While we are excited for her, she will be greatly missed! If you were fortunate enough to attend, Judge Chestney was one of the speakers last year on the traveling CLE program, Employment Law in a Nutshell. The excitement she brought to the program was infectious and I lost count of how many chapters she flew to along with Brett Strand (3M). Congratulations, Judge Chestney, we wish you the best in your new chapter!

To that extent, we have new members on the board to welcome. First, we welcome our newest board member, Kevin Green (Arizona Chapter Representative). With Judge Chestney's departure, Whitney Sedwick Meister (former Chapter Representative) has agreed to assume the secretary role, which includes co-chairing publications. Thank you, Kevin and Whitney, for stepping up! In addition, we are excited to partner with the Law Student Division and have two new representatives joining the board as non-voting members, Annie Calvert (University of Kansas School of Law) and Danny Treadaway (University of Cincinnati College of Law). If you are interested in speaking, authoring an article or otherwise getting involved in the L&E Section, please contact any one of us. ■

A LOOK AT WHAT'S INSIDE

Bank Whistleblower Litigation Highlights Limits of Employee Confidentiality Agreements to Curb Data Misappropriation.....	2
7th Biennial Labor and Employment Law Conference held in San Antonio.....	4
A Membership Perk: Monthly Circuit Updates	5
The Defend Trade Secrets Act of 2016: What Are Trade Secrets and Why Are They Important?.....	6
Labor and Employment Law Section Governing Board	11

Bank Whistleblower Litigation Highlights Limits of Employee Confidentiality Agreements to Curb Data Misappropriation

By Peter D. Hardy, Edward J. McAndrew, Brian D. Pedrow, and Priya Roy

Employers increasingly face the difficult scenario of employees who misappropriate company data in the pursuit of whistleblower claims alleging misconduct by the employer. Such cases can present a complex mix of regulatory, cybersecurity, and employment issues. These issues were front and center in a recent whistleblower case pitting a bank against its former internal auditor, who engaged in computer-facilitated misappropriation of the bank's confidential information allegedly to support whistleblower conduct.

The U.S. District Court for the Southern District of California recently declined to summarily adjudicate whether the employee's confidentiality agreement precluded any whistleblower affirmative defense based on the employee's alleged violation of computer fraud, contract, and tort laws. The whistleblower laws in question included Sarbanes-Oxley, Dodd-Frank, the Bank Secrecy Act, and the California Labor Code.

In *Erhart v. BofI Holding*, plaintiff Charles Matthew Erhart filed a whistleblower complaint against his employer, Bank of the Internet (BoFI), alleging BoFI retaliated against him for reporting unlawful conduct to the government. BoFI, in turn, filed a complaint, alleging that Erhart breached his employee confidentiality agreement by misappropriating confidential data relating to his employer and its clients and disseminating that data to the government, family members, and the national press.

Erhart illustrates the complex and practical problems faced by employers dealing with employees who engage in conduct that would otherwise constitute computer fraud, intellectual property theft, breaches of employment-related agreements and policies, and related tort claims under the mantle of "whistleblower." A key issue in the case was whether Erhart would be entitled to pursue his retaliation claims before a jury or would be precluded from doing so as a matter of law given his computer-facilitated theft of confidential information.

BoFI hired Erhart as an internal auditor in 2013 and required him to execute a confidentiality agreement to safeguard the information BoFI treated as proprietary and confidential (including banking information, communications with regulators, internal audit findings, and the personal information of BoFI employees and customers). When performing his audits, Erhart discovered what he believed was wrongdoing in relation to responding to a subpoena from the Securities and Exchange Commission (SEC) and dealing with a certain loan customer. Erhart shared these concerns, and others, with the SEC and BoFI's primary regulator, the Department of the Treasury's Office of the Comptroller of the Currency (OCC).

Erhart sued BoFI, claiming that it violated federal and state law by retaliating against him for reporting unlawful

conduct to the government. The retaliatory conduct allegedly included a downgrade in his performance rating that adversely impacted his bonus. The next day, the national media published an article about the lawsuit, and BoFI's shares plummeted. BoFI quickly countersued under state and federal law, alleging that Erhart had published confidential company information and deleted hundreds of files from his company-issued laptop. The two suits were consolidated.

BoFI's countersuit alleged a set of facts that are becoming increasingly common, given the ease with which employees may use technology to appropriate employer information—Erhart used his personal Gmail account to email files containing confidential BoFI information, including customer Social Security numbers and bank account information, to himself and to his mother. According to BoFI, he printed copies of BoFI's documents containing customer bank account information and downloaded BoFI files including supervisory communications from the OCC to his personal computer and to a personal USB drive; he accessed electronic data on his girlfriend's computer; and he disclosed confidential information in his publicly filed whistleblower complaint and is alleged to have passed the complaint to the press.

Erhart responded by relying on various affirmative defenses based on the whistleblower provisions found in various state and federal statutes, regulations, and rules. BoFI filed a motion for summary adjudication of Erhart's affirmative defenses, arguing Erhart's defenses failed because his conduct was not protected whistleblower activity.

The court held that Erhart's reliance on the whistleblower provisions as an affirmative defense was tantamount to alleging that enforcement of his confidentiality agreement with BoFI would violate public policy. Relying on principles of contract interpretation, the court analyzed whether the public policy interests in the enforcement of the confidentiality agreement outweighed the interest against the enforcement of the contract (the public policy exception). Among the interests present in favor of enforcement, the court cited California's longstanding policy of respecting and promoting the freedom of private parties to contract, the significant government interests in promoting the legal protection of trade secrets (including business information that did not qualify for trade secret protection), and the data privacy protection of banking institutions' clients. On the other hand, the court also looked to federal and state statutes, regulations, and rules—including Sarbanes-Oxley and the Dodd-Frank Act—that reflect a "strong public policy in favor of protecting whistleblowers."

The court attempted to balance the interests in enforcement and against the specific conduct Erhart sought to shield by reliance on the whistleblower protection provisions. For instance, the court found that as to Erhart's communications with the OCC and the SEC, the public policy in favor of whistleblower protection clearly outweighed the enforcement of the agreement, thus rendering the confidentiality agreement unenforceable as to this conduct. On the other hand, as to Erhart's alleged disclosure to the media, the court held that "leaks to the media are not protected" conduct under the various whistleblower protection provisions cited by Erhart.

Thus, if the facts at trial demonstrated that Erhart passed information to the press (which Erhart denied), the whistleblower defenses would not preclude liability for a breach of the confidentiality agreement.

As for the misappropriation and dissemination of Boff's confidential information in the publicly filed whistleblower complaint, the court held that the public policy exception applied—thereby making the confidentiality agreement unenforceable—if:

- the removal of the documents and disclosure of such information contained in those documents in the complaint was reasonably necessary to support his allegations of wrongdoing; and
- he did not engage in the “wholesale stripping” of confidential company documents and his appropriation and disclosure was not “vast and indiscriminate.”

Finally, as for Erhart's emailing and downloading of Boff's confidential data to accounts and devices under his and his family members' control, the court held that the public policy exception would apply if a jury were to determine that Erhart's conduct was necessary to protect relevant information from what he reasonably perceived was a risk of destruction. Even though Erhart had sent an email to his mother containing a spreadsheet containing bank customers' Social Security numbers (conduct that may constitute a “data breach” under various state and federal laws), he alleged that doing so was necessary to prevent bank management from deleting or altering the information. He further alleged that he reasonably feared such misconduct, because bank management had accessed his work laptop remotely and senior managers had made hostile comments about his auditing activities. The court viewed this as sufficient to create a jury issue.

Employers can best protect themselves from liability and legitimate whistleblowers from retaliation by employing some basic technical and legal controls. First, employers should have well-documented and disseminated whistleblower notices and procedures. Because public policy considerations and whistleblower protections may render confidentiality provisions unenforceable, effective and secure methods for employees to air their grievances internally may reduce the chance that employees will become so dissatisfied that they begin to misappropriate data. A reference to such a grievance process in the confidentiality agreement also may address the public policy interests in enforcing confidentiality agreements while also respecting the public policy interests in protecting whistleblowers. In fact, certain statutes (like the Defend Trade Secrets Act of 2016) may only be used by employers to protect their confidential information if they adequately notify employees of whistleblower protections.

Second, employers should have clear policies relating to technology use (devices, communications, internet services, etc.), the protection of confidential information, and employee separation. Third, employers should utilize technical safeguards that make it more difficult for employees to engage in the most common forms of data misappropriation. Examples

include data loss prevention and digital rights management tools, mobile device management apps, security information and event management software, internet activity monitoring, and whitelisting/blacklisting of internet applications.

Ballard Spahr has launched Money Laundering Watch, a new blog focused exclusively on money laundering issues to keep readers informed of the latest developments in enforcement, compliance, and policy. Please visit the blog, and subscribe to receive updates, at www.moneylaundering-watchblog.com.

Ballard Spahr's Labor and Employment Group routinely assists employers with issues regarding whistleblowers and retaliation in the workplace. The firm's White Collar Defense/Internal Investigations and Privacy and Data Security Groups have experience conducting cybersecurity risk assessments, designing risk management and compliance plans, advising and representing companies in response to cyber incidents, data breaches, and related litigation, and conducting cyber investigations. ■



Peter D. Hardy is a partner in the Litigation Department at Ballard Spahr. Peter Hardy advises corporations and individuals in a range of industries against allegations of misconduct—including tax fraud, money laundering, Bank Secrecy Act, mortgage fraud and lending law violations, securities fraud, health care fraud, public corruption, Foreign Corrupt Practices Act violations, and identity theft and data breach. He spent more than a decade as a federal prosecutor before entering private practice, and is a frequent contributor to Money Laundering Watch, Ballard Spahr's blog focused exclusively on money laundering issues.



Edward J. McAndrew is a partner in the Litigation Department at Ballard Spahr and co-leader of the firm's Privacy and Data Security Group. Before entering private practice, he most recently served for nearly a decade as a federal cybercrime prosecutor in the U.S. Attorney's Offices for the Eastern District of Virginia and for the District of Delaware. Named a “Cybersecurity and Data Privacy Trailblazer” by The National Law Journal, Mr. McAndrew advises clients on cybersecurity, digital privacy, cyber-incident response, social media, online speech, defamation, commercial, employment, intellectual property, corporate governance, and regulatory compliance, and enforcement matters.



Brian D. Pedrow is a partner at Ballard Spahr and leads the firm's Labor and Employment Group. He represents employers and management in the full

Bank continued on page 5

7th Biennial Labor and Employment Law Conference held in San Antonio

The Labor and Employment Section held the 7th Biennial Labor and Employment Conference in San Antonio, Texas on March 9-10, 2017. Approximately 75 practitioners from across the country attended the conference and learned from well-respected judges, attorneys, and general counsel on a variety of advanced topics related to labor and employment law. The conference began with opening remarks from FBA President Judge Michael J. Newman. EEOC Commissioner Charlotte A. Burrows provided the keynote luncheon address, and discussed emerging trends in discrimination law. U.S. Magistrate Judge Betsy Chestney moderated a panel of federal judges, including Senior District Judge David Ezra (San Antonio, TX), U.S. Magistrate Judge Henry Bemporad (San Antonio, TX), and U.S. Magistrate Judge Mark Lane (Austin, TX). The panel discussed perspectives from the bench on litigating employment cases.

William “Kenan” Torrans, Deputy Director for Compliance Programs of the Veterans’ Employment and Training Service (“VETS”), and Paul Marones, Senior Investigator at VETS, provided an engaging presentation titled “USERRA: What Matters in Protecting Our Service Members’ Employment Rights.” The attendees also enjoyed presentations on several other topics, including emerging issues related to sex discrimination under Title VII, bankruptcy issues for employment lawyers, labor law primer for the employment law practitioner, immigration law issues, developing trends under the Federal Trade Secrets Act, practical tips for both plaintiff and defense lawyers on working with in-house counsel, and religious discrimination in the workplace.

The speakers received positive reviews and feedback from the attendees, and we received several excellent suggestions for topics at the next event. We hope you can join us in 2019 for the 8th Biennial Conference! ■



Join the Labor & Employment Law Section today! Visit www.fedbar.org.

Bank continued from page 3

scope of matters related to employment, labor, and employee benefit disputes. Mr. Pedrow's practice includes all facets of employment-related litigation, such as discrimination, harassment, retaliation, breach of contract, and employment-based torts. He also has a significant practice representing benefit plans, fiduciaries, and plan sponsors in Employee Retirement Income Security Act (ERISA) litigation arising from benefits eligibility disputes, breach of fiduciary litigation, and interference with benefits claims. His traditional labor practice includes both private and public sector labor negotiations, arbitrations, unfair labor practice charges, and related matters.



Priya Roy is an associate in the firm's Litigation Department. She focuses her practice on white collar defense, regulatory compliance and complex civil litigation. She conducts internal investigations and advises and defends companies and individuals facing criminal and civil investigation, and has participated in negotiations with the U.S. Department

of Justice and federal regulatory authorities. Ms. Roy's practice includes counseling clients in Anti-Money Laundering and Bank Secrecy Act matters, as well as matters involving allegations of tax fraud, violations of the False Claims Act and Anti-Kickback Statute, violations of the Food, Drug and Cosmetics Act, securities violations, and other fraud and regulatory offenses.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, including electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the author and publisher. This alert is a periodic publication of Ballard Spahr LLP and is intended to notify recipients of new developments in the law. It should not be construed as legal advice or legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult your own attorney concerning your situation and specific legal questions you have. Copyright © 2017 by Ballard Spahr LLP. www.ballardspahr.com (No claim to original U.S. government material.)

A Membership Perk: Monthly Circuit Updates

Don't forget that your membership in the Labor and Employment Section gives you access to the Monthly Circuit Updates! Each month, summaries of all the major labor and employment decisions in each Circuit are provided to all members in an eNewsletter that is also available on the Section's webpage at www.fedbar.org/sections/labor-employment-law-section.aspx. These Updates are an invaluable resource that keeps members up-to-date on important developments in each Circuit. Take a deep dive into all the new cases within your Circuit each month, and/or peruse all of the developments around the country to stay abreast of the law for your clients. If you would like to volunteer as a contributor for the Circuit Update, please contact Caitlin Andersen (candersen@seatonlaw.com) or Whitney Sedwick Meister (Whitney.Meister@bestwestern.com) for more information.

The Defend Trade Secrets Act of 2016 What Are Trade Secrets and Why Are They Important?

By John Balitis and Cameron Johnson

“There are only two categories of companies affected by trade-secret theft: those that know they’ve been compromised and those that don’t know yet.”¹ These are the words of then-Attorney General Eric Holder to Congress in describing the widespread impact of trade-secret theft on businesses in the United States.

So widespread is that damaging impact that Congress passed a sweeping trade-secret law this past year. The Defend Trade Secrets Act of 2016 must be understood by attorneys, especially in comparison to applicable state laws that remain in force and are not preempted by the DTSA. These laws provide a variety of tools for the lawyer defending her client’s trade secrets.

Businesses Impact of Trade-Secret Theft

Unlike a patent or a copyright, trade secrets are *non-public* intellectual property. Trade secrets are unique business assets because their economic value derives from their secrecy. Some of the most recognized trade secrets are KFC’s secret recipe and Coca-Cola’s formula, but trade secrets include many different types of proprietary business information that are crucial to economic success.

Along with the myriad benefits associated with the digital information age, a major downside for businesses is that trade-secret theft has become much easier to accomplish. Trade secret misappropriation may now be achieved, among other ways, through attaching documents to an email or downloading files onto a thumb drive. As a result, the pace of trade-secret theft continues to accelerate in the United States.²

Trade secrets are crucial to the success of both large and small businesses, and their theft can have crippling consequences. Imagine the economic impact, for example, if Google’s search algorithm fell into the hands of a competitor. By way of demonstration, a 2013 report from the Executive Office of the President provided examples to Congress of the magnitude of trade-secret theft to individual companies, including the theft of a Goldman Sachs trade secret valued at \$500 million and a Dupont trade secret valued at \$400 million.³

The devastating impact of trade-secret misappropriation on businesses also has been confirmed by recent civil cases involving trade-secret theft. In a recent case brought under Wisconsin’s version of the Uniform Trade Secrets Act, a jury returned a jaw-dropping verdict of \$940 million (comprised of \$240 million in compensatory damages and \$700 million in punitive damages).⁴ In that case, Epic Systems, a privately held medical software company, sued Tata Group, one of India’s largest companies, after Tata allegedly conspired with a third party to license Epic’s software and then download Epic’s confidential files containing trade-secret information relating to the development of a new product.

In another recent case, Miller UK Ltd., a family-owned company out of Great Britain, was awarded \$74 million in a trade-secret misappropriation suit brought against Caterpillar Inc. in the Northern District of Illinois.⁵ It was determined in that case

that Caterpillar misappropriated Miller’s trade secrets by using trade-secret information Miller shared with it pursuant to the parties’ confidentiality agreement to reverse-engineer and patent its own competing product.

These recent cases illustrate a common situation faced by businesses in today’s digital landscape: trade-secret misappropriation by those who have been granted access to company information. In fact, according to the 2016 Cyber Security Intelligence Index published by IBM, approximately 60 percent of all data breaches are carried out by company insiders.⁶ While testifying before Congress, a representative of the pharmaceutical company Eli Lilly & Co. discussed this dilemma faced by businesses:

We often run into situations where we find that an employee has left and is going to work for a competitor, and we find out something such that once they turn in their Lilly-issued computer, there has been a download of a number of documents which contain highly confidential Lilly trade secrets.⁷

This “company insider” scenario is much more prevalent than many are aware of, and virtually every business—regardless of size—is susceptible.

Reports shared with Congress offer a similarly grim outlook on trade-secret misappropriation. These reports—one from the Commission on the Theft of American Intellectual Property⁸ and the other from the Center for Responsible Enterprise and Trade and PricewaterhouseCoopers LLP⁹—claimed that the financial impact of trade-secret misappropriation has reached unprecedented levels and is costing the U.S. economy approximately \$300 billion to \$480 billion annually.

The Defend Trade Secrets Act of 2016

Against this backdrop of information regarding the magnitude of trade-secret theft on U.S. businesses, Congress passed—with a remarkable 87–0 approval in the Senate and 410–2 approval in the House—the Defend Trade Secrets Act of 2016 (the “DTSA”)¹⁰ on April 27, 2016. The DTSA, which President Obama signed into law on May 11, 2016, amends the Economic Espionage Act (a criminal statute empowering the Attorney General to bring criminal charges for trade-secret theft) and expands the body of trade-secret misappropriation law that has been traditionally reserved to the states. Most notably, the DTSA includes a new federal cause of action largely modeled after the Uniform Trade Secrets Act (“UTSA”) and an *ex parte* seizure remedy akin to that found in federal trademark law.

Although the DTSA was largely modeled after the UTSA and therefore mirrors many aspects of state trade-secret statutes, the DTSA does *not* displace or preempt state law. Thus, in counseling a client on matters pertaining to trade secret misappropriation, it is critical for attorneys to understand the key differences and similarities between the DTSA and the trade-secret statute of the state in which the alleged misappropriation occurs. This article addresses the key similarities and differences of the DTSA and the Arizona Trade Secret Act (the “AUTSA”), supplying Arizona attorneys with information critical to providing thorough and up-to-date legal advice in the

area of trade-secret misappropriation law.

DTSA and AUTSA Origins

In 1979, the Uniform Law Commission—a non-profit organization consisting of commissioners appointed by each state, the District of Columbia, Puerto Rico and the U.S. Virgin Islands—published the Uniform Trade Secrets Act (“UTSA”).¹¹ The purpose of the UTSA was to provide a statutory framework for the states to adopt in developing uniform standards and remedies for trade-secret misappropriation.¹²

As of today, the UTSA—or some version thereof—has been adopted by 48 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. (Notably, the legislatures of the only two hold-out states—New York and Massachusetts—have introduced bills this year to enact it.) Nevertheless, there are still significant variations in trade-secret law across the country as many states differ in their statutory interpretations and others have enacted a modified version of the model statute—including Arizona.

In 1990, Arizona enacted its modified version of the UTSA—the Arizona Uniform Trade Secrets Act (“AUTSA”).¹³ Although the AUTSA tracks the majority of the language of the UTSA, the Arizona Legislature did not adopt the directive in the UTSA that would have required Arizona courts to apply and construe the statute “to effectuate its general purpose to make uniform the law with respect to the subject of this Act among states enacting it.”¹⁴ Arizona courts are under no obligation, therefore, to apply or construe the AUTSA in conformance with other states that have enacted the UTSA.

Like the AUTSA, many of the key provisions of the DTSA have origins in the UTSA.¹⁵ The DTSA and the AUTSA are therefore similar in many ways. However, the DTSA also includes several features and provisions that were not derived from the UTSA. These distinct features and provisions differentiate the DTSA from its Arizona counterpart and should be understood and carefully considered before providing counsel in this area of the law. (For detail on similarities and differences, **see the table on page 9.**)

DTSA Unique Features

***Ex Parte* Seizure**

As a powerful remedy unavailable under the AUTSA (and other state versions of the UTSA), the DTSA allows courts to order the seizure of trade-secret materials by law enforcement upon an *ex parte* application.¹⁶ This unique remedy is available in “extraordinary” circumstances in which it is “necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.”¹⁷ The court must find, among other things, that “it clearly appears from specific facts that” a preliminary injunction or temporary restraining order would be inadequate “because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order.”¹⁸ The court also must find that the material to be seized is indeed a trade secret that was misappropriated by the person against whom seizure would be ordered and that such person “would destroy, move, hide, or otherwise make such matter inaccessible to the court.”¹⁹

Although an *ex parte* seizure is a powerful new means

to combat trade-secret misappropriation, caution should be exercised in seeking such relief as courts may award compensatory damages, punitive damages, and attorneys’ fees against the party seeking the seizure if the court subsequently determines the seizure was wrongful or excessive.²⁰

Whistleblower Protections

Unlike the AUTSA, the DTSA provides immunity for whistleblowers from civil and criminal liability for making limited disclosures of trade secrets to government officials or the court under certain enumerated circumstances.²¹ These circumstances include: (1) a disclosure made “in confidence” to a government official or attorney for the purpose of “reporting or investigating” a violation of law, or in a sealed court filing; or (2) a disclosure by a plaintiff employee to his or her attorney or in a sealed filing in a lawsuit for retaliation for reporting a violation of law (*i.e.*, a whistleblower retaliation action).²²

Critically, the DTSA requires employers to provide notice of the DTSA’s whistleblower immunity protections in contracts with employees and independent contractors that govern the use of trade-secret or other confidential information entered into or updated after the enactment of the DTSA.²³ If an employer fails to provide notice of the DTSA’s whistleblower immunity protections, the employer may not be awarded exemplary damages or attorneys’ fees in a claim brought under the DTSA.²⁴

Protection of Trade-Secret Information in Court Proceedings

The DTSA reflects a policy of protecting the confidentiality of trade secrets. To this end, the DTSA expressly requires courts to protect “information the owner asserts to be a trade secret” until the owner has the opportunity to file a submission under seal detailing the owner’s interest in keeping the information confidential.²⁵

DTSA Implications for Arizona Practitioners

Although many of the DTSA’s provisions are similar to those of the AUTSA, the DTSA contains key distinctions that may have a substantial impact on the legal counsel provided by Arizona attorneys. Whether advising an employer on the language of employment contracts or confidentiality policies, helping a trade-secret owner assess potential misappropriation claims under the AUTSA or the DTSA, or defending an employee in a misappropriation action brought in federal court, knowledge of the key features and provisions of the DTSA and how they compare to the AUTSA will facilitate the most thorough and up-to-date legal advice to clients. ■



John Balitis is a director and attorney with Fennemore Craig in Phoenix, where he chairs the firm’s Labor Relations and Employment Practice Group. He represents businesses in all aspects of employment

law. Cameron Johnson is an associate attorney with Fennemore

Craig in Phoenix, where he practices in both the Commercial Litigation Group and the Labor Relations and Employment Practice Group.

Originally published in *Arizona Attorney Magazine*, State Bar of Arizona.

Endnotes

¹S. Rep. No. 114-220, at 2 (2016).

²Executive Office of the President of the United States, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets I (2013).

³*Id.* at 4-5, 12.

⁴*Epic Systems v. Tata Group*, No. 14-CV-748 (U.S. Dist. Court, W.D. Wis., April 14, 2016).

⁵*Miller UK Ltd. v. Caterpillar Inc.*, No. 10-03770 (U.S. Dist. Court, N.D. Ill.).

⁶Marc van Zadelhoff, *The Biggest Cybersecurity Threats Are Inside Your Company*, HARV. BUS. REV., available at hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company.

⁷*Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats? Before S. Comm. On the Judiciary*, 113th Cong. (2014) at 15 (statement of Douglas K. Norman, Eli Lilly & Co.).

⁸THE IP COMMISSION, THE REPORT OF THE COMMISSION ON THE THEFT OF

AMERICAN INTERNATIONAL PROPERTY 11 (May 2013), available at www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

⁹CREATE.ORG AND PWC, ECONOMIC IMPACT OF TRADE SECRET THEFT 3 (Feb. 2014).

¹⁰18 U.S.C. § 1836 *et seq.*

¹¹*Uniform Trade Secrets Act with 1985 Amendments*, www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf (last visited Nov. 18, 2016).

¹²*Id.* For more on the UTSA and its Arizona analogue, see Damian R. Meyer & Meaghan Kramer, *Trade Secret Protections Clarified*, ARIZ. ATT'Y (April 2015) at 12.

¹³A.R.S. § 44-301 *et seq.*

¹⁴UTSA § 8.

¹⁵S. Rep. No. 114-220, at 10 (2016); H. Rep. No. 114-529, at 14 (2016).

¹⁶18 U.S.C. § 1836(b)(2).

¹⁷*Id.* § 1836(b)(2)(A)(i).

¹⁸*Id.* § 1836(b)(2)(A)(ii).

¹⁹*Id.*

²⁰*Id.* § 1836(b)(2)(G).

²¹*Id.* § 1833(b).

²²*Id.*

²³*Id.*

²⁴*Id.*

²⁵*Id.* § 1835(b).

TABLE: Contrasting the DTSA and AUTSA

Despite the many similarities in the DTSA and the AUTSA, there may be reasons for a plaintiff to bring a claim under just one statute or the other—or both. In order to better understand such scenarios, the differences and similarities in the key features and provisions of the DTSA and the AUTSA are reflected in the table below.

Key Provisions & Features	Defend Trade Secrets Act	Arizona Uniform Trade Secrets Act	Similarities & Differences
Private Cause of Action & Statute of Limitations	18 U.S.C. § 1836(b) (1) (private cause of action for trade-secret misappropriation) 18 U.S.C. § 1836(d) (three-year statute of limitations)	A.R.S. § 44-403(A) (private cause of action for trade-secret misappropriation) A.R.S. § 44-406 (three-year statute of limitations)	Both the DTSA and the AUTSA provide a private right of action for misappropriation of trade secrets. An action brought under either statute is subject to a three-year statute of limitations. To bring an action under the DTSA, the plaintiff must be an “owner” of the trade secret that “is related to a product or service used in, or intended for use in, interstate or foreign commerce.” The AUTSA does not expressly require the plaintiff be an “owner” of the trade secret. Nor does the AUTSA require that the trade secret be related to a product used, or intended for use, in interstate commerce.
Definition of “Trade Secret”	18 U.S.C.A. § 1839(3) (definition of “trade secret”)	A.R.S. § 44-401(4) (definition of “trade secret”)	Both the DTSA and the AUTSA provide expansive definitions of a “trade secret.” The DTSA definition is more expansive than the AUTSA definition in that it enumerates more “forms and types” of information that may qualify as a trade secret. Although the AUTSA definition may be interpreted to cover such examples of trade secrets, the DTSA definition may bolster claims based on the types of information expressly described. The AUTSA definition is broader in that it extends to all information that derives economic value from not being generally known and is the subject of reasonable efforts to maintain its secrecy. The DTSA, on the other hand, limits trade secrets to financial, business, scientific, technical, economic or engineering information that derives independent economic value from not being generally known and the owner has taken reasonable measures to keep such information secret.
Definition of “Misappropriation” and “Improper Means”	18 U.S.C.A. § 1839(5) (definition of “misappropriation”) 18 U.S.C. § 1839(6) (definition of “improper means”)	A.R.S. § 44-401(2) (definition of “misappropriation”) A.R.S. § 44-401(1) (definition of “improper means”)	The DTSA’s and the AUTSA’s definitions of “misappropriation” are virtually identical. The crux of the definitions in both statutes is the “acquisition, use or disclosure of a trade secret that was acquired by improper means.” The definition of “improper means” under both statutes includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy or espionage through electronic or other means. The DTSA’s definition of “improper means” differs from the AUTSA’s definition in its express exclusion of “reverse engineering, independent derivation, or any other lawful means of acquisition.”
Preemption of Claims Based on Similar Facts	18 U.S.C. § 1838 (effect on other laws)	A.R.S. § 44-406 (effect on other laws)	The DTSA does not preempt other state causes of action that may arise under the same nucleus of facts. The AUTSA, on the other hand, preempts other common law claims based on a misappropriation of “trade secrets,” while leaving available claims based on misappropriation of confidential information (that does not constitute trade secrets). ¹ The AUTSA also does not preempt contractual or criminal remedies, whether or not based on misappropriation of a trade secret.
Damages	18 U.S.C. § 1836(b) (3)(B) (damages provision) 18 U.S.C. § 1836(b) (3)(C) (exemplary damages provision) 18 U.S.C. § 1836(b) (3)(D) (attorney fee provision)	A.R.S. § 44-403(A) (damages provision) A.R.S. § 44-403(B) (exemplary damages provision) A.R.S. § 44-404 (attorney fee provision)	Both the DTSA and the AUTSA authorize an award of damages for “actual loss” and for unjust enrichment caused by trade secret misappropriation. The DTSA and the AUTSA also authorize, in lieu of damages for “actual loss” or for unjust enrichment, damages measured by the amount of a reasonable royalty for a misappropriator’s unauthorized disclosure or use of a trade secret. The DTSA and the AUTSA both authorize an award of “exemplary damages” up to double the total awarded damages if the trade secret misappropriation is determined to be “willful and malicious.” The DTSA and the AUTSA authorize an award of reasonable attorneys’ fees to the prevailing party for any of the following: (1) a claim of misappropriation made in bad faith; (2) a motion to terminate an injunction made or resisted in bad faith; or (3) willful and malicious trade-secret misappropriation.
Injunctive Relief	18 U.S.C. § 1836(b) (3)(A) (injunctive relief provision)	A.R.S. § 44-402 (injunctive relief provision)	Both the DTSA and the AUTSA authorize courts to grant injunctive relief to prevent actual or threatened misappropriation. An injunction under both the DTSA and the AUTSA also may require that a party found liable for misappropriation take affirmative steps to protect a trade secret. Both statutes also permit courts to order payment of a reasonable royalty for the use of a trade secret when “exceptional circumstances” would make an injunction inequitable. The main difference between the injunctive relief provisions of the DTSA and the AUTSA is that an injunction under the DTSA must not prevent a person from entering into an employment relationship. This language in the DTSA rejects the “inevitable disclosure” doctrine recognized by some states, under which a court can enjoin an employee from accepting employment that would inevitably result in the use or disclosure of trade-secret information known to the employee. Because the DTSA does not preempt state law, the “inevitable disclosure” doctrine remains available to the extent it is recognized under Arizona law. Arizona courts, however, have apparently not yet ruled as to whether the theory of “inevitable disclosure” is recognized in Arizona. ²

¹See *Orca Communications Unlimited LLC v. Noder*, 236 Ariz. 180, 184-85 (2014) (discussing scope of A.R.S. § 44-406).

²See, e.g., *Liss v. Exel Transp. Servs., Inc.*, No. CIV 04-2001 PHXSM, 2007 WL 891167, at *9 (D. Ariz. Mar. 20, 2007) (“It is unclear whether Arizona recognizes the theory of inevitable disclosure as the Court did not locate a single case in Arizona applying this theory.”).



ATLANTA

Federal Bar Association Annual Meeting and Convention

September 14–16, 2017 • Westin Peachtree Plaza

SPONSORSHIP OPPORTUNITIES AVAILABLE!

Contact Heather Gaskins at (571) 481-9106 or hgaskins@fedbar.org.

Follow the FBA |



Labor and Employment Law Section Governing Board

CHAIR

Corie Tarara
Seaton, Peters & Revnew, P.A.
7300 Metro Blvd. Suite 500
Minneapolis, MN 55439
(952) 921-4615
ctarara@seatonlaw.com

VICE CHAIR

Kathryn M. Knight
Stone, Pigman, Walther,
Wittmann LLC
546 Carondelet St.
New Orleans, LA 70130
(504) 593-0915
kknight@stonepigman.com

DEPUTY CHAIR

Craig A. Cowart
Jackson Lewis P.C.
999 Shady Grove Road
Suite 110
Memphis, TN 38120
(901) 462-2618
craig.cowart@jacksonlewis.com

SECRETARY

Whitney Sedwick Meister
Best Western International, Inc
6201 N. 24th Parkway
Phoenix, AZ 85016
(602) 957-5758
whitney.meister@bestwestern.com

TREASURER

M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

IMMEDIATE PAST CHAIR

Donna P. Currault
Gordon, Arata, McCollam,
Duplantis & Eagan, LLC
201 St. Charles Ave. 40th Floor
New Orleans, Louisiana 70170
(504) 582-1111
DCurrault@gordonarata.com

EDITOR, THE LABOURING OAR

Whitney Sedwick Meister
Best Western International, Inc
6201 N. 24th Parkway
Phoenix, AZ 85016
(602) 957-5758
whitney.meister@bestwestern.com

STANDING COMMITTEES:

(All Chairs/Co-Chairs are mem-
bers of the Governing Board)

Standing Committee on Membership and Chapter Relations:

Co-Chairs:
Craig A. Cowart
Jackson Lewis P.C.
999 Shady Grove Road
Suite 110
Memphis, TN 38120
Phone: (901) 462-2618
craig.cowart@jacksonlewis.com

Whitney Sedwick Meister
Best Western International, Inc
6201 N. 24th Parkway
Phoenix, AZ 85016
(602) 957-5758
whitney.meister@bestwestern.com

Standing Committee on Publications and Public Relations:

Co-Chairs:
EDITOR, THE LABOURING OAR
Whitney Sedwick Meister
Best Western International, Inc
6201 N. 24th Parkway
Phoenix, AZ 85016
(602) 957-5758
whitney.meister@bestwestern.com

Caitlin Andersen
Seaton Peters & Revnew PA
7300 Metro Blvd Ste 500
Minneapolis, MN 55439
(952) 896-1700
candersen@seatonlaw.com

Standing Committee on Programming and Continuing Legal Education:

Co-Chairs:
Brian Rochel
Teske Micko Katz Kitzer & Rochel
222 S 9th St Ste 4050
Minneapolis, MN 55402
(612) 746-1558
rochel@teskemicko.com

Phillip Kitzer
Teske Micko Katz Kitzer & Rochel
222 S 9th St Ste 4050
Minneapolis, MN 55402
(612) 746-1558
kitzer@teskemicko.com

Standing Committee on Finance and Expenditures:

Co-Chairs:
M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

Karleen Green
Karleen.Green@phelps.com

Standing Committee on Executive Agency Outreach:

Co-Chairs:
M. Kathleen McKinney
National Labor Relations Board
600 South Maestri Place
7th Floor
New Orleans, LA 70130
(504) 589-6374
Kathleen.mckinney@nlrb.gov

Danielle Brewer Jones
The Brewer Law Office, PLLC
1891 Pass Rd.
Biloxi, MS 39531
(228) 388-0053
dbrewer@brewerlegalservices.com

Standing Committee on Legislation and Congressional Relations:

Co-Chairs:
Kevin M. Green
Fennemore Craig
2394 E. Camelback Road, Suite
600
Phoenix, Arizona 85016
(602) 916-5466
kgreen@fclaw.com

Joel P. Schroeder
Best & Flanagan LLP
60 South Sixth Street, Suite 2700
Minneapolis, MN 55402
(612) 339-7121
jschroeder@bestflaw.com

Special Committee on Awards/ Marketing:

Donna P. Currault
Gordon, Arata, McCollam,
Duplantis & Eagan, LLC
201 St. Charles Ave. 40th Floor
New Orleans, Louisiana 70170
(504) 582-1111
DCurrault@gordonarata.com

Special Committee on Community Outreach & Civics Education:

Joyce Kitchens
Kitchens New Cleghorn LLC
2973 Hardman Ct.
Atlanta, GA 30305
(678) 244-2880
joyce.kitchens@knclawfirm.com

CHAPTER REPRESENTATIVES:

(All are members of the Governing
Board and of Standing Committee
on Membership and Chapter
Relations)

Timothy Bliss
CenterPlace
50 Park Row West, Suite 109
Providence, RI 02903
(401) 274-2100
TBLISSLAW@gmail.com

José Gonzalez-Nogueras
Pizarro & Gonzalez
P.O. Box 194302
San Juan, P.R. 00919-4302
650 Plaza, Suite 502
650 Muñoz Rivera Ave.
San Juan, Puerto Rico 00918
(787) 667-7397
jgonzalez@pg.legal

Jim Hammerschmidt
The Law Firm of Paley Rothman,
Attorneys at Law
4800 Hampden Ln 4th Floor
Bethesda, MD 20814
(301) 951-9338
jrh@paleyrothman.com

Kevin M. Green
Fennemore Craig
2394 E. Camelback Road, Suite
600
Phoenix, Arizona 85016
(602) 916-5466
kgreen@fclaw.com

Joyce Kitchens
Kitchens New Cleghorn LLC
2973 Hardman Ct.
Atlanta, GA 30305
(678) 244-2880
joyce.kitchens@knclawfirm.com



The **Labouring Oar**

Labor and Employment Section
Federal Bar Association
1220 North Fillmore Street
Suite 444
Arlington, VA 22201