Morgan Lewis | White Paper

THE LANDMARK DEFEND TRADE SECRETS ACT OF 2016

May 2016

Mark L. Krotoski
Silicon Valley | Washington, DC
Partner

Greta L. Burkholder | Washington, DC
Jenny Harrison | San Francisco
Corey R. Houmand | Silicon Valley
Associates

www.morganlewis.com

I. OVERVIEW OF THE DEFEND TRADE SECRETS ACT OF 2016

The Defend Trade Secrets Act of 2016 (DTSA), enacted on May 11, 2016,[1] represents the most significant trade secret reform legislation in several decades. Given the importance of this landmark statute, this White Paper provides an overview of the key provisions and identifies practical suggestions for trade secret owners to protect their trade secrets under the new federal law.

The DTSA amends the Economic Espionage Act of 1996 (EEA),[2] which provides for federal criminal penalties for foreign economic espionage and trade secret theft and adds new federal civil trade secret protections. The DTSA modernizes and strengthens trade secret law in a number of key respects.

Some of the primary features include the following:

- **New Federal Remedies**: A federal private right of action for trade secrets that provides for federal law remedies instead of only state law remedies for the theft of trade secrets (*See* Section VI(A), page 7, *infra*). The federal remedies may include injunctive relief, damages, and the possibility of double damages for willful and malicious misappropriation (*See* Section VI(D), page 10, *infra*).
- **Choice of Federal or State Remedies**: Because the legislation does not preempt state law, trade secret owners have the choice to pursue relief in federal or state court, depending on the circumstances (*See* Section VI(A), page 7, *infra*). A variety of factors may apply to any particular case in determining whether to pursue federal or state remedies (*See* Section VII(G), page 15, *infra*).
- **New Recovery Mechanism**: In appropriate cases, new tools to recover stolen trade secrets based on a short-term, *ex parte* court order to seize trade secrets by law enforcement officials and bring them within the custody of the court, with a full hearing held within seven days with all parties present (*See* Section VI(B), page 8, *infra*).
- **Stronger Protections for Trade Secrets During Litigation**: Several protections will better safeguard the use of trade secrets in litigation, including the use of protective orders, and the opportunity for a trade secret owner to inform the court of the interests to maintain confidentiality of the trade secret (*See* Section VI(C), page 9, *infra*).
- **Digital Issues**: New provisions addressing unique digital issues that arise in trade secret cases (*See* Section VI(F), page 12, *infra*).
- **Whistleblower Protections**: A new whistleblower provision concerning the disclosure of trade secrets to law enforcement to report or investigate possible violations of law (*See* Section VI(E), page 11, *infra*).
- **New Notification Requirement**: A new disclosure requirement about the immunity provisions is required in every employee contract "that governs the use of a trade secret or other confidential information" that is "entered into or updated after" May 11, 2016, when the DTSA was enacted. The failure to provide notice will bar exemplary damages or attorney fees against an employee who did not receive notice (*See* Section VI(E), page 12, *infra*).
- **Criminal Penalties**: Increasing the maximum criminal penalties for organizations convicted of foreign economic espionage or trade secret theft (*See* Section VI(H), page 12, *infra*).

These and other aspects of the new law are further explained below.

II. BACKGROUND: CHALLENGES IN PROTECTING TRADE SECRETS UNDER PRIOR LAW

A. Key Role of Trade Secrets to the Economy, Jobs, and Innovation

Trade secrets, as one form of intellectual property, provide tremendous value to the economy, companies, and the innovation process. By some estimates, "as much as 80 percent of companies' assets are intangible, the majority of them in the form of trade secrets" that include "everything from financial, technical, economic, and engineering information to formulas, designs, prototypes, processes, procedures and computer code."[3] Others have estimated that "trade secrets are worth $5 trillion to publicly listed American companies alone."[4]

Trade secrets take many forms. They touch nearly every sector of the economy, including the technology, financial institution, health, manufacturing, automobile, agriculture, and military industries, among many others. Trade secrets can include commercial information, such as "financial, business, scientific, technical, economic, or engineering information."[5] Illustratively, trade secrets may include prototypes, plans, processes, codes, designs, methods, and techniques. Some trade secret examples include chemical formulas for the manufacture of silicone and rubber products,[6] collections of confidential information regarding customers,[7] high-frequency trading strategy and infrastructure source code,[8] and designs of memory macros for computer chips,[9] among many others.[10]

Because of trade secrets' high value, they are often targeted for theft or misappropriation. As the DTSA House Report noted, "Trade secrets are an integral part of a company's competitive advantage in today's economy, and with the increased digitization of critical data and increased global trade, this information is highly susceptible to theft."[11]

B. Consequences of Trade Secret Theft

Trade secret theft can be devastating on many levels. It can destroy the value of a trade secret and competitive advantages for the trade secret owner. It can also result in lost jobs and harm to a company or industry. The cost of trade secret theft has been estimated to be "from one to three percent of the Gross Domestic Product (GDP) of the United States and other advanced industrial economies."[12] As noted during the DTSA congressional debate, "[t]oday the misappropriation of trade secrets is estimated to cost American companies between $160 and $480 billion annually."[13]

When trade secrets are stolen by insiders, hackers, or competitors, obtaining meaningful relief under prior law could be challenging, particularly when trade secrets are removed to other jurisdictions or outside the United States. Until the DTSA took effect, trade secrets were the only form of US intellectual property in which an owner did not have access to a federal civil action or remedy for misuse or misappropriation.[14] Instead, trade secret owners were limited to state law remedies for trade secret misappropriation. Currently, 47 states have enacted some form of the Uniform Trade Secret Act (UTSA).[15]

Although these state-based remedies may be effective for the local misappropriation of a trade secret, Congress recognized that they posed challenges for several reasons.[16]

First, despite the enactment of state laws based on the UTSA, over time, most states adopted their own versions of trade secrets laws such that state laws "today are perhaps even more variable in their treatment of trade secrets than they were at the time the Uniform Trade Secrets Act was proposed in 1979."[17] Compliance with different state standards can be costly.[18]

Second, under state law, efforts to obtain remedies for the stolen trade secrets taken to other jurisdictions can be cumbersome, costly, and ineffective. For example, the process to obtain a deposition

of a witness in another state can require multiple court orders and delay.[19] Instead, in federal court, parties have nationwide subpoena service power.[20]

Third, federal courts are typically "better situated" to provide the "swift action by courts across state lines" required "to preserve evidence" and prevent the transfer of the stolen trade secrets.[21]

Fourth, in today's digital world, "[p]rotecting trade secrets has become increasingly difficult given ever-evolving technological advancements."[22]

III. FEDERAL CRIMINAL OFFENSES UNDER THE EEA

The EEA established federal criminal penalties for the theft of trade secrets. It was enacted to protect and promote national and economic security by filling in gaps under the law that previously allowed this conduct to go unpunished.[23]

Because the DTSA amends the EEA to provide for new civil remedies and adopts portions of the EEA, it is important to understand the EEA's role. Additionally, for some cases, the EEA's criminal provisions along with the new civil remedies under the DTSA may come into play.

A. Two Distinct Criminal Offenses

The EEA provides for two distinct criminal trade secret offenses (often referred to by their statutory sections). The first concerns trade secret theft (under Section 1832), and the second concerns foreign economic espionage (under Section 1831).[24]

First, traditional trade secret theft or misappropriation, under Section 1832, requires proof of the "intent to convert a trade secret . . . to the economic benefit of anyone other than the owner" and "intending or knowing that the offense will, injure any owner of that trade secret." For example, a former Coca-Cola employee was convicted under Section 1832 for misappropriating Coca-Cola's marketing information and a product sample and attempting to sell this information for profit to a Coca-Cola competitor.[25]

The underlying trade secret theft can form the basis for both criminal and civil parallel actions. One recent example involved a South Korean company's attempt and conspiracy to steal E.I. du Pont de Nemours & Co.'s trade secrets regarding Kevlar technology. This conduct resulted in a criminal convicton and civil action.[26]

Second, foreign economic espionage, under Section 1831, involves the misappropriation of a trade secret with the intent to benefit a foreign government, foreign instrumentality, or foreign agent. Under US Department of Justice (DOJ) policy, a federal prosecutor may not charge a Section 1831 offense without prior review and approval by the assistant attorney general for the National Security Division.[27] Some of the factors considered in the review process include an assessment of foreign policy consequences and issues and strength of the evidence.[28] Since 1996, 11 foreign economic espionage cases have been authorized for prosecution, with six resulting in Section 1831 convictions, one resulting in complete acquittal and dismissal of all charges, and three remaining cases with the primary defendants at large. The foreign economic espionage cases that resulted in Section 1831 convictions involved trade secrets and confidential information regarding the design and manufacture of computer microprocessors,[29] visual simulation software,[30] space shuttle and Delta IV rocket designs,[31] insecticides,[32] customer information,[33] and pigment manufacturing processes.[34]

B. EEA Amendments in 2012

Congress amended the EEA to strengthen prosecutions and deter violations. The Foreign and Economic Espionage Penalty Enhancement Act of 2012 increased penalties for foreign economic espionage[35] with the objective "to deter and punish criminals who target U.S. economic and security interests on behalf of foreign interests."[36] In the Theft of Trade Secrets Clarification Act of 2012,[37] Congress clarified federal jurisdiction

(which was based on "a product or service used in or intended for use in interstate or foreign commerce") to correct the limitations imposed by a decision from the US Court of Appeals for the Second Circuit.[38]

C. Limited Number of EEA Criminal Cases

Only a handful of federal criminal trade secret cases are prosecuted each year. As noted in the recent congressional debate, during nearly 20 years under the EEA, about 300 defendants have been charged, which "equates to an average of about 10 prosecutions annually" when considering that multiple defendants are often prosecuted in individual trade secret cases.[39] Although the number of cases varies each year, during 2013, as an example, approximately 25 Section 1832 cases were prosecuted.[40] As the Senate Report summarized, "while fighting economic espionage and the theft of trade secrets is a top priority for Federal law enforcement, criminal enforcement remains a limited solution to stopping trade secret theft as the Federal Bureau of Investigation and Department of Justice are limited in the resources they can bring to bear."[41]

Finally, there are limits to relying largely on criminal law. As noted in the House Report, criminal trade secret statutes are normally "not suited to making whole the victims of misappropriation."[42]

D. Civil Remedies Now Complementing Criminal Sanctions

During the congressional debate on the DTSA, members of Congress noted that federal law should allow trade secret owners to pursue federal civil remedies. Under the DTSA, the criminal provisions of the EEA are now augmented by new civil protections.

IV. SUMMARY OF CONGRESSIONAL ACTION

In April 2016, the DTSA sailed through the US Senate and US House of Representatives with nearly unanimous bipartisan support. Only two votes in Congress opposed the act, a rarely seen feat.

On July 29, 2015, bipartisan legislation was introduced in the Senate as S. 1890 by Senator Orrin Hatch (R-UT) and Senator Chris Coons (D-DE).[43] On the same day, identical bipartisan legislation, H.R. 3326, was introduced in the House by Representative Doug Collins (R-GA) and Representative Jerrold Nadler (D-NY).[44] The DTSA was first considered in the Senate.

A. Senate Action

On December 2, 2015, the US Senate Committee on the Judiciary held the hearing "Protecting Trade Secrets: the Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm."[45] On January 28, 2016, the Senate Judiciary Committee reported out an amended version of the DTSA (S. 1890), on a bipartisan, unanimous voice vote.[46] The DTSA Senate Report issued on March 7, 2016.[47] Sixty-five senators cosponsored the DTSA. On April 4, 2016, the Senate unanimously passed the DTSA by a vote of 87 to 0.[48]

B. House Action

On April 20, 2016, the US House Committee on the Judiciary approved the DTSA, as passed by the Senate, in a bipartisan voice vote.[49] One hundred and sixty-four representatives cosponsored the DTSA. On April 27, 2016, the House passed the DTSA by a vote of 410 to 2.[50]

C. Enactment

Following passage in the Senate and House, the DTSA became law on May 11, 2016.[51] The new protections under the DTSA took effect the same day.

D. Prior Congressional Consideration

The protections and rights under the DTSA have been developed over the last several years. In the prior Congress, an earlier version of the DTSA[52] was reported out of the House Judiciary Committee on September 17, 2014,[53] following hearings in the House and Senate.[54] Further action on the legislation was not taken because the congressional session ultimately ended.

V. SCOPE OF PROTECTED TRADE SECRETS FROM MISAPPROPRIATION

The definition of a "trade secret" under federal law (both under the EEA and now the DTSA) is based on the UTSA,[55] but the definition is broader under federal law in two significant respects.[56] First, the federal definition is more explicit in the forms of covered information. The federal definition includes "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."[57] Second, the federal definition expressly covers "intangible" information.

Under the DTSA, civil claims may be brought for the "misappropriation" of a trade secret that is based on the "established definition" of "misappropriation: under the UTSA.[58] Thus, misappropriation generally includes the "acquisition of a trade secret by improper means, disclosure or use of a trade secret by a person who had reason to know that the trade secret was acquired by improper means or under circumstances giving rise to a duty of secrecy, or disclosure or use of a trade secret by a person who had reason to know it was disclosed by accident or mistake."[59] "Improper means" may include "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[60] However, improper means does not include "reverse engineering, independent derivation, or any other lawful means of acquisition."[61]

VI. THE DTSA'S KEY ELEMENTS

In this section, we review the key elements under the new federal law.

A. Federal Private Right of Action

For the first time, the DTSA authorizes a federal private right of action to remedy trade secret misappropriation. Trade secret owners now have the option to pursue civil remedies under federal law. Federal district courts hold "original jurisdiction" over DTSA civil actions.[62]

Specifically, the DTSA provides that "[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is *related to a product or service used in, or intended for use in, interstate or foreign commerce*."[63] As both the Senate and House reports explain, the DTSA's jurisdictional nexus to interstate or foreign commerce "is identical to the existing language required for Federal jurisdiction over the criminal theft of a trade secret under § 1832(a)."[64] Because of this new private right of action, trade secret owners "will be able to rely on a national standard to efficiently protect their intellectual property."[65]

The DTSA also fills a prior gap in the law by ensuring a federal private cause of action is available for all four intellectual property forms.[66] Previously, federal courts could hear claims of infringement in copyright,[67] trademark,[68] and patent cases.[69] Civil trade secret misappropriation was limited to state law civil remedies.[70] The DTSA now allows federal courts to consider civil trade secret claims based on federal law.

Significantly, by allowing civil trade secret claims to be heard in federal court, the DTSA does not preempt state trade secret laws. Under the DTSA, trade secret owners now can choose whether to seek remedies in either federal or state court.[71]

B. New Tools for the Seizure and Recovery of Stolen Trade Secrets

In many trade secret theft cases, recovery of the stolen trade secrets remains elusive. In "extraordinary circumstances," the DTSA provides a new *ex parte* seizure provision to "prevent the propagation or dissemination of the trade secret" pending a full court hearing.[72]

Upon a proper showing in "extraordinary circumstances," a trade secret owner can request a short-term *ex parte* seizure order to seize "property necessary to prevent the propagation or dissemination of the trade secret."[73] Examples may include when "a defendant is seeking to flee the country or planning to disclose the trade secret to a third party immediately or is otherwise not amenable to the enforcement of the court's orders."[74]

A court order is served by a law enforcement officer, not a party to the case.[75] Any seized materials remain in the custody of the court pending further court determination.

Congress has adopted the use of a civil seizure remedy in other similar contexts. Specifically, this tool has been enacted for trademark counterfeiting cases,[76] and for the impoundment of records in copyright infringement cases.[77]

1. Focused and Balanced Requirements to Obtain Court Seizure Order

The *ex parte* seizure order is subject to several requirements and restrictions to ensure that it is limited to appropriate circumstances. The requirements include the showing by the applicant to justify the seizure, certain findings by the court, and the order's manner of the execution, pending a full hearing. In issuing a seizure order, the court will "balance the need to prevent or remedy misappropriation with the need to avoid interrupting the legitimate interests of the party against whom a seizure is issued, and the business of third parties."[78]

First, to seek relief, an applicant must make a proper showing based on an affidavit or verified complaint.[79] Specifically, the applicant must allege "specific facts" that demonstrate that

- a standard 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";
- an "immediate and irreparable injury will occur" in the absence of seizure;
- the harm in denying relief outweighs any harm to others;
- the applicant is likely to succeed in showing that the information is a trade secret and the person who is the subject of the order misappropriated or conspired to misappropriate the trade secret;
- the matter to be seized is described with "reasonable particularity" and the location is identified;
- the person subject to the order "would destroy, move, hide, or otherwise make such matter inaccessible to the court" if notice were provided; and
- the requested seizure has not been publicized by the applicant.[80]

Second, the court must make certain findings and conclusions before issuing a seizure order. The seizure order shall

- set forth findings of fact and conclusions of law required for the order;

- provide for the "narrowest seizure of property" in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate, unrelated business operations of the person accused of misappropriating the trade secret;
- be accompanied by an order protecting the seized property from disclosure by restricting the access of the applicant and prohibiting any copies of the seized property;
- provide guidance to law enforcement officials executing the court's order;
- set a prompt hearing within seven days, unless the parties otherwise consent; and
- require the applicant to provide the security determined adequate by the court for payment of such damages that a person may be entitled to recover as a result of a wrongful or excessive seizure.[81]

Third, a neutral law enforcement official serves the seizure order and the "submissions of the applicant to obtain the order."[82] This ensures that an experienced professional executes the court's order. Upon law enforcement request, a neutral technical expert, bound by a nondisclosure agreement, may assist in the seizure if the court concludes that "the expert will aid the efficient execution of and minimize the burden of the seizure." [83]

Fourth, any materials seized are retained into the custody of the court.[84] The court is required to secure the material from physical and electronic access.[85] Additionally, the court may take protective steps to verify that any electronic medium containing the trade secret is not "connected to an electronic network or the Internet without the consent of both parties, until the hearing" with all parties present. The seized material remains secure within federal court control.

Fifth, the court must hold a seizure hearing within seven days.[86] At the hearing, the court can consider the parties' arguments. If the applicant is unable to meet its burden to establish sufficient facts to support the order, "the seizure order shall be dissolved or modified appropriately."[87]

Sixth, the legislation includes various safeguards against an improper *ex parte* seizure order. The court may "take appropriate action to protect the person against" the subject of the order "from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order."[88]

A motion to dissolve or modify the seizure order may be filed "at any time" by "any person harmed by the order."[89] A person who suffers damage as a result of a wrongful or excessive seizure may bring a cause of action against the applicant to recover damages, including punitive damages and reasonable attorney fees.[90] These statutory sanctions are in addition to general sanctions that the court may issue under Federal Rule of Civil Procedure 11.[91] For any claim of misappropriation that is made in bad faith, the court may award reasonable attorney fees.[92]

The *ex parte* seizure provision is intended to apply to persons who have "actual possession" of the trade secret or "any property to be seized."[93] The seizure order is not intended to apply to third parties who do not possess the trade secret or relevant property. Instead, "the court may decide to issue a third-party injunction preventing disclosure of the trade secret using its existing authority to provide equitable relief."[94]

C. Stronger Protections for Trade Secrets During Civil and Criminal Litigation

In some key respects, the DTSA builds on protections under the EEA to safeguard trade secrets during litigation. First, a federal court may issue a protective order "and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets."[95]

Second, the DTSA also establishes new rights for trade secret owners to protect against the disclosure of a trade secret during litigation. A court may not authorize the disclosure of trade secret information "unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential."[96] The language makes clear that any

"provision" or "disclosure of information relating to a trade secret to the United States or the court in connection with a prosecution" under the EEA "shall not constitute a waiver of trade secret protection unless the trade secret owner expressly consents to such waiver."[97]

Third, in cases involving the government, the EEA already provides for an interlocutory appeal by the United States for review of an adverse disclosure ruling by a court.[98] This provision has helped protect against the disclosure of trade secrets in federal criminal cases.[99]

Finally, the legislative history makes clear that in criminal cases involving a conspiracy to steal a trade secret, "the actual trade secret itself is not subject to disclosure to the defense, because the actual secrecy of the information that is the object of the conspiracy is not relevant to the prosecution of a conspiracy charge."[100] Collectively, these provisions provide enhanced means to protect trade secrets from disclosure during civil and criminal litigation.

D. Remedies for Trade Secret Misappropriation

The DTSA provides for several types of potential remedies for the victims of trade secret misappropriation.[101] In general, the DTSA provides for (1) injunctive relief, (2) damages, and (3) the possibility of double damages for willful and malicious misappropriation.

1. Injunctive Remedies

Under the DTSA, in general, a court may grant an injunction "to prevent any actual or threatened misappropriation."[102] Injunctive relief can be among the most important steps taken in a case to mitigate damage from a misappropriation of trade secrets.

A court may also require affirmative actions be taken to protect the trade secret,[103] may bar disclosure of the trade secret,[104] or may condition future use of the trade secret upon payment of a reasonable royalty.[105] However, payment of a reasonably royalty is reserved only for exceptional circumstances that render an injunction inequitable.[106]

(i) Two Limitations on Injunctive Relief

The DTSA places two restrictions on the federal court's injunctive authority that "reinforces the importance of employee mobility."[107] The injunction may not (1) prevent anyone from entering into an employment relationship or (2) conflict with applicable state laws regarding restraints on trade.[108]

With regard to employee mobility,[109] one issue arises under the doctrine of inevitable disclosure, which is not accepted in every state because of its practical effect of restricting employee mobility. The inevitable disclosure doctrine allows a trade secret owner to "prove a claim of trade secret misappropriation by demonstrating that [the] defendant's new employment will inevitably lead him to rely on the plaintiff's trade secrets."[110] The doctrine of inevitable disclosure is explicitly rejected by certain jurisdictions because it conflicts with some states' expressed protection of an employee's ability to change employers.

Other states, including California, have adopted specific measures to protect employee mobility; in these states, trade secret owners cannot prevent an employee from moving to a new employer merely because the employee has knowledge of the former employer's trade secret. In other states, the doctrine of inevitable disclosure can enable a former employer to restrict an employee's future employment at other companies based on information and knowledge that the employee has gained from his or her position at the former employer. The legislative history notes the different positions taken "on the applicability of the inevitable disclosure doctrine."[111] Under the DTSA, "[a]ny conditions placed by a court on employment must be based on evidence of threatened misappropriation, and not merely on information a person knows."[112]

Therefore, the DTSA allows a court to issue an injunction with respect to an employment relationship only when there is evidence of threatened or actual misappropriation, "not merely on the information the

person knows."[113] This language ensures that jurisdictions that have already explicitly rejected the doctrine of inevitable disclosure will not be forced to abide by it.

Under the second limitation on injunctive relief, an injunction may not conflict with applicable state laws regarding restraints on trade.[114] This restriction ensures that a federal DTSA injunction will "coexist with, and not [] preempt, influence, or modify applicable State law governing when an injunction should issue in a trade secret misappropriation matter."[115] As noted in the Senate and House Reports, one example involves the application of the inevitable disclosure doctrine.[116] The DTSA will ensure that applicable state law is enforced on these issues.

(ii) Prior EEA Protections on the Ability to Transfer Special Skills and Knowledge

By amending the EEA, as summarized earlier, the DTSA adopts certain prior federal safeguards concerning employee mobility.[117] The EEA legislative history specified that general skills, knowledge, and experience are not sufficient to satisfy the definition of a trade secret and that the EEA was not intended to restrict employees with knowledge of trade secrets from seeking new employment.[118] In particular, the EEA Senate Report noted that the EEA "does not apply to innocent innovators or to individuals who seek to capitalize on their lawfully developed knowledge, skill or abilities," and that "[t]he Government cannot prosecute an individual for taking advantage of the general knowledge and skills or experience that he or she obtains or comes by during his [or her] tenure with a company."[119] These preexisting federal safeguards will continue to apply.

2. Damage Award

The DTSA authorizes damage awards for the actual loss and any unjust enrichment caused by the trade secret misappropriation.[120] This damage award is intended to serve as the primary means to compensate a trade secret owner.

However, in some instances, determining the actual loss may not be feasible. In these limited circumstances, in lieu of damages measured by any other method, a court may award a reasonable royalty "for no longer than the period of time for which such use could have been prohibited."[121] An award of a reasonable royalty under this provision requires an assessment of the trade secret's value, a determination of a reasonable royalty rate, and a determination of an appropriate time period based on the length of time the owner could have prohibited use of the trade secret. The legislative history does not encourage use of this reasonable royalty method to resolve trade secret misappropriation and specifically indicates a preference for other remedies that first halt the use and dissemination of the trade secret and then make available appropriate damages.[122]

3. Attorney Fees and Exemplary Damages for Willful and Malicious Misappropriation

The DTSA also authorizes the award of attorney fees and exemplary damages in certain situations. When there is a willful and malicious misappropriation of a trade secret, a court may award attorney fees as well as exemplary damages not exceeding twice the compensatory damages awarded.[123] Attorney fees may also be awarded if the claim of misappropriation was made in bad faith or if a motion to terminate an injunction was made or opposed in bad faith.[124]

E. New Whistleblower Protections: Immunity from Liability from Employee Disclosure of Trade Secrets

The DTSA provides for specific protections and immunity to employees who disclose trade secrets in two specific situations.[125] In this context, the definition of "employee" also includes both contractors and consultants doing work for an employer.[126]

First, the DTSA exempts individuals from liability when an individual disclosed the trade secret "in confidence" directly or indirectly to federal, state, and local government officials or to a lawyer and did so "*solely* for the purpose of reporting or investigating a suspected violation of law."[127] Second, an individual

may disclose a trade secret in the context of a document filed in court under seal.[128] Disclosure of trade secrets is also specifically authorized in antiretaliation lawsuits, as long as the information is disclosed only to an individual's lawyer, is filed under seal, and is not disclosed except by court order.[129] The Senate emphasized "that this provision immunizes the act of disclosure in [these] limited circumstances" and "does not immunize[] acts that are otherwise prohibited by law, such as the unlawful access of material by unauthorized means."[130]

The DTSA has a new notification requirement concerning the immunity protections. The new law requires an employer to "provide notice of the immunity . . . in any contract or agreement with an employee that governs the use of a trade secret or other confidential information."[131] This notification applies to all such contracts entered into or updated after the date of enactment, May 11, 2016.[132] The notice requirement can be satisfied "if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law."[133] An employer that fails to comply with this notice requirement "may not be awarded exemplary damages or attorney fees under" section 1836(b)(3)(C) or (D) "in an action against an employee to whom notice was not provided."[134]

The Senate and House Reports both clarify that the DTSA "preempt[s] state laws that govern matters of individual liability when trade secrets are disclosed to governmental officials during the course of an investigation or legal proceeding."[135] Thus, the immunity and protections added to Section 1833 would trump any conflicting state laws.

The whistleblower protections were added to the DTSA by a bipartisan amendment offered by Senate Judiciary Committee Chairman Chuck Grassley (R-IA) and Ranking Minority Member Patrick Leahy (D-VT). The amendment was unanimously approved on a voice vote on January 28, 2016.[136]

F. Digital Protections

The DTSA contains a number of new provisions to address trade secret issues and protections in the digital era. Compared to the protections offered under the UTSA and state laws, these provisions modernize the ways a court may protect materials that it has seized. Specifically, the DTSA instructs a court seizing materials to "secure the seized material from physical and electronic access during the seizure and while in the custody of the court."[137] The DTSA further instructs the court to prohibit any seized storage medium from "being connected to a network or the Internet without the consent of both parties" pending a full hearing.[138]

The DTSA further provides that "a party or a person who claims to have an interest in the subject matter seized may make a motion at any time, which may be heard *ex parte*, to encrypt any material seized or to be seized under this paragraph that is stored on a storage medium."[139]

G. Statute of Limitations

The statute of limitations for the DTSA's federal private right of action is three years "after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered."[140] During the Senate Judiciary Committee's markup, this three-year limitations period was reduced from five years to three.[141] The DTSA's statute of limitations is "identical to the limitations period of the UTSA" (subject to modifications that have been made on a state-by-state basis).[142] The DTSA further provides that for statute of limitations purposes, a continuing misappropriation constitutes a single claim of misappropriation.[143]

H. Enhanced Criminal Penalties for Organizations

The DTSA increases certain criminal penalties. Specifically, the statute amends the EEA to increase the maximum criminal penalty for an organization convicted of a criminal violation from $5 million to "the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."[144]

I. RICO Predicate Offenses

Under the Racketeer Influenced and Corrupt Organizations Act (RICO),[145] criminal or civil remedies may be obtained for certain conduct involving a "pattern of racketeering activity."[146] For example, a civil plaintiff bringing a successful private right of action may "recover threefold the damages he sustains and the cost of the suit, including a reasonable attorney's fee."[147]

The DTSA adds the foreign economic espionage (Section 1831) and criminal theft of trade secret (Section 1832) provisions as qualifying predicate offenses under RICO.[148] In establishing a "pattern of racketeering activity," a plaintiff must prove at least two predicate acts committed within 10 years of each other.[149] In appropriate cases, prosecutors and civil plaintiffs will be able to include criminal trade secret theft offenses to establish a pattern of racketeering activity in RICO cases.

J. Report on Theft of Trade Secrets Occurring Abroad

Given concerns about the theft of trade secrets outside the United States, the DTSA requires a biannual report from the attorney general that addresses multiple issues regarding the international scope of trade secret theft.[150] The attorney general must compile this report in consultation with the intellectual property enforcement coordinator, the director, and the heads of other appropriate agencies. The DTSA specifies eight areas of concern regarding the effect of foreign trade secret theft on United States companies, including the following:

- The scope and breadth of theft from abroad faced by United States companies
- The extent that such foreign trade secret theft is sponsored by foreign governments, agents, or instrumentalities
- The threat posed by foreign trade secret theft
- The limitations that trade secret owners face in preventing foreign trade secret theft or enforcing judgment against foreign entities for trade secret theft
- The protections and enforcement efforts provided to US companies by countries that are the United States' trading partners
- Instances of the federal government working with foreign countries to investigate, arrest, and prosecute those involved in the theft of trade secrets
- Progress made under trade agreements to protect US companies from foreign trade secret theft
- Recommendations for legislative and executive branch actions to reduce the threat and economic impact caused by foreign trade secret theft[151]

K. Judicial Best Practices Report

The DTSA requires the Federal Judicial Center (within two years of enactment) to develop recommended best practices for (1) the seizure of information and media storage of that information and (2) the securing of the information and media once seized.[152] The DTSA further requires the Federal Judicial Center to update its recommended best practices from time to time and to provide its recommendations, along with any updates, to the judiciary committees of both the House and Senate.[153]

VII. PRACTICAL CONSIDERATIONS UNDER THE DTSA

Given the new protections under the DTSA, there are a number of practical considerations that trade secret owners should review and take into account.

A. New Notice Requirement

The DTSA makes a significant change to employee agreements by requiring notice of the new whistleblower and immunity protections.[154] This requirement applies to all employee agreements that are newly drafted or updated after May 11, 2016. The meaning of "employee" under this section is defined broadly to include "any individual performing work as a contractor or consultant for an employer."[155] The effect of this new requirement is broad.

If an employer does not comply with this notice requirement and subsequently brings an action under the DTSA against an employee who did not receive proper notice, the employer may not be awarded exemplary damages or attorney fees.[156] Thus, for all newly drafted or updated employment agreements or nondisclosure agreements, companies should include a standard notification clause regarding the whistleblower protections. Companies could also consider creating and issuing a trade secret policy with the notification clause and then cross-referencing that policy in the employment agreements.[157]

B. The DTSA's Effective Date

The DTSA applies to any misappropriation of a trade secret "for which any act occurs on or after the date of the enactment."[158] Therefore, the DTSA should be considered a possible remedy for any misappropriation that occurred on or after May 11, 2016, but it cannot be used retroactively for misappropriations that occurred prior to this date.

C. *Ex Parte* Seizure Order in "Extraordinary Circumstances"

The DTSA provides a significant new tool to recover trade secrets in "extraordinary circumstances," such as to prevent imminent disclosure of the trade secret to a third party or risk of flight to another country. The court is required to balance various interests, including "the need to prevent or remedy misappropriation with the need to avoid interrupting the legitimate interests of the party against whom a seizure is issued, and the business of third parties."[159]

In using this new tool, an applicant's request for the seizure order will need to be carefully drafted to meet the specific requirements for the seizure order and be carefully particularized to accomplish the seizure without disrupting other interests that may be affected by the law enforcement seizure.

D. Statute of Limitations Issues

The DTSA maintains the three-year UTSA statute of limitations period.[160] The three years are measured after the misappropriation is discovered or should have been discovered with reasonable diligence. Trade secret owners must therefore be reasonably diligent in inspecting for any misappropriations and promptly bringing action under the DTSA once a misappropriation is discovered.

E. Reasonable Measures to Protect Trade Secrets

To obtain the protections and remedies offered under the DTSA, trade secret owners should take an inventory of their trade secrets and assess whether sufficient "reasonable measures" are in place to protect them.[161] The failure to have adequate reasonable measures may foreclose remedies under the DTSA.[162] Also, one common line of defense in many trade secret cases involves a challenge that the information does not qualify as a trade secret because reasonable measures were not used.

Because the commercial value of trade secrets depends on the trade secrets remaining confidential, trade secret owners are required to use reasonable measures to protect their trade secrets. One central aspect of establishing the existence of a trade secret is the requirement that reasonable measures are employed to safeguard the trade secret.[163] Establishing reasonable measures is an element for either civil or criminal trade secret claims. The EEA House Report explained this requirement as follows:

> The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it.[164]

The types of reasonable measures that apply will depend on the trade secrets in issue. Regrettably, in a number of trade secret cases, the trade secret owner loses legal protections by failing to periodically assess the sufficiency of the "reasonable measures" in place. Given the enactment of new federal remedies under the DTSA, trade secret owners are strongly advised to review the adequacy of the reasonable measures used to protect their trade secrets.

F. Safe-Guarding Trade Secrets During Litigation

In seeking a remedy for trade secret theft, one risk factor concerns the possible disclosure of the trade secret information during public civil or criminal proceedings. In recognizing this risk, the DTSA establishes stronger protective options to safeguard trade secrets during litigation. Trade secret owners will want to consider and fully avail themselves of these protections, and tailor them as necessary to their trade secrets during any trade secret litigation.

The options include an appropriately drafted protective order, which includes the nondisclosure of the trade secret during litigation and the return and disposition of the trade secret following the proceedings. The DTSA also provides the trade secret owner with a voice during the proceedings to advise the court of the interests to maintain the trade secret's confidentiality. In cases involving the government, in the event of any adverse ruling by the trial court ordering the disclosure of the trade secret to other parties, the DTSA provides for an interlocutory appeal by the United States for review and determination by an appellate court.

As another protective measure, the DTSA specifically provides for anyone with an interest in seized material to make a motion to encrypt any material seized under the *ex parte* provision that is stored on a storage medium.[165] Trade secret owners and others with interests in the information at issue will want to consider this new legal protection in appropriate cases to prevent disclosure of any digitized trade secrets.

G. Choosing Federal or State Trade Secret Remedies

One of the DTSA's benefits is that trade secret owners will have a choice to seek a remedy under federal or state trade secret law. Whether federal or state law is appropriate will depend on the circumstances of the particular case.

Given the potential differences between the DTSA and trade secret law enacted and individualized by a particular state, there may be advantages, disadvantages, and potential conflicts to including such a state law cause of action. There are a variety of factors that may be considered in this decision. Some are noted below:

- **Federal Jurisdiction**: Can the federal jurisdiction requirement be satisfied to pursue federal relief? The DTSA remedies are available so long as the misappropriation involves a "trade secret" that "is *related to a product or service used in, or intended for use in, interstate or foreign commerce*."[166]
- **Misappropriation Across Jurisdictional Lines**: Was the misappropriation local, or did it involve trade secrets removed to other jurisdictions? State trade secret law may provide an effective remedy for local misappropriation. Once a trade secret is removed to other jurisdictions, federal law typically will provide a more effective and efficient means to obtain evidence in other jurisdictions.
- **Need for Limited Court Order to Seize Trade Secrets**: Is there a need for a prompt seizure of trade secrets, such as to prevent the destruction or use of trade secrets or removal

to another jurisdiction? In "extraordinary circumstances," and upon a proper showing, the DTSA provides new tools that can be used to recover stolen trade secrets. This new court remedy is not available under any state trade secret law.

- **Statute of Limitations**: What time remains to file a civil claim under the applicable statute of limitations? Under the DTSA, a three-year statute of limitations applies, similar to the UTSA.[167] However, for those states that apply a longer or shorter period, the time to file a civil claim could make a difference in a particular case.
- **Scope of Information Qualifying as a Trade Secret**: Are questions raised whether the trade secrets fall within the broader federal definition of trade secrets compared with state law?[168] Generally, federal law applies a broader definition of "trade secrets" than the UTSA and under state law.
- **Proof of "Reasonable Measures"**: Would satisfying the reasonable measures requirement make a difference under applicable federal or state law?
- **Protecting Trade Secrets During Litigation**: Are the stronger protections to safeguard trade secrets during litigation under the DTSA needed for the case? If this is a significant factor, federal law may be selected.
- **Other Substantive and Procedural Differences**: An analysis of substantive and procedural differences between federal and state law may be case dispositive. Some examples may include:
    - **Party Burden**—Identifying which party has "the burden of establishing that a trade secret is not readily ascertainable."[169]
    - **Innocent Acquisition Rights**—Determining "whether the owner has any rights against a party that innocently acquires a trade secret"[170]
    - **Pleading Requirements**—Confirming the ability to satisfy certain pleading requirements, such as the California Uniform Trade Secrets Act statutory requirement that "before commencing discovery relating to the trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity."[171]

The facts and legal issues in each case must be independently assessed. The foregoing and other factors should be considered in the decision of whether federal or state remedies should be pursued for any trade secret misappropriation.

VIII. CONCLUSION

The DTSA modernizes and strengthens trade secret law in a number of significant respects. Trade secret owners now have a "complementary" federal remedy[172] with state law remedies. The new federal tools will help redress the theft and misappropriation of trade secrets in a number of factual settings that previously encountered legal and other obstacles. Federal remedies will allow trade secret owners "to move quickly to Federal court, with certainty of the rules, standards, and practices to stop trade secrets from winding up being disseminated and losing their value."[173]

CONTACTS

If you have any questions or would like more information on the issues discussed in this White Paper, please contact any of the following Morgan Lewis lawyers:

Silicon Valley

Mark L. Krotoski	+1.650.843.7212	mark.krotoski@morganlewis.com
Corey R. Houmand	+1.650.843.7524	corey.houmand@morganlewis.com

Washington, DC

Greta L. Burkholder	+1.202.739.5894	greta.burkholder@morganlewis.com

San Francisco

Jenny Harrison	+1.415.442.1426	jenny.harrison@morganlewis.com

About Morgan, Lewis & Bockius LLP

Founded in 1873, Morgan Lewis offers 2,000 lawyers—as well as patent agents, benefits advisers, regulatory scientists, and other specialists—in 28 offices across North America, Europe, Asia, and the Middle East. The firm provides comprehensive litigation, corporate, transactional, regulatory, intellectual property, and labor and employment legal services to clients of all sizes—from globally established industry leaders to just-conceived start-ups. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

Endnotes

[1] Pub. L. No. 114-153 (May 11, 2016).
[2] Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended 18 U.S.C. §§ 1831–1839), https://www.gpo.gov/fdsys/pkg/PLAW-104publ294/pdf/PLAW-104publ294.pdf.
[3] 162 CONG. REC. S1626 (daily ed. Apr. 4, 2016) (statement of Sen. Klobuchar).
[4] *Id.* at S1629 (statement of Sen. Coons).
[5] *See, e.g.,* Economic Espionage Act, 18 U.S.C. § 1839(3) (defining trade secrets); *see also* Uniform Trade Secret Act § 1(4) (same), http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf.
[6] Plea Agreement, *United States v. Agodoa,* No.13-CR-20525 (E.D.Mich. Sept. 25, 2013) (ECF No. 22); Judgment (E.D. Mich. Jan. 17, 2014) (ECF No.29).
[7] Amended Judgment, *United States v. Nosal,* No .08-CR-00237-EMC (N.D. Cal. May 30, 2014) (ECF No. 552); *see United States v. Nosal*, Nos. 14-10037, 14-10275 (9th Cir. 2015) (pending appeal).
[8] Plea Agreement, *United States v. Pu,* No. 11-CR-00699 (N.D. Ill. Aug 7, 2014) (ECF No. 175); Judgment, (N.D. Ill. Jan 15, 2015) (ECF No. 206).
[9] Entry of Judgment, *UniRAM Tech., Inc. v. Taiwan Semiconductor Mfg. Co.,* No. 04-CV-01268 (N.D. Cal. Apr. 17, 2008) (ECF No. 628).
[10] For recent examples, *see* Trade Secret Examples Based on Recent Criminal and Civil Cases, https://www.morganlewis.com/~/media/files/publication/practice%20resource/supplemental%20info/protecting%20trade%20secrets/lpg_tradesecrets_appendixb.ashx.
[11] H.R. Rep. 114-529, 114th Cong., 2d Sess. 3 (Apr. 26, 2016) [hereinafter DTSA House Report].
[12] Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, 3 (Feb. 2014), https://create.org/wp-content/uploads/2014/07/CREATe.org-PwC-Trade-Secret-Theft-FINAL-Feb-2014_01.pdf.
[13] 162 CONG. REC. S1630 (daily ed. Apr. 4, 2016) (statement of Sen. Coons); *see also* DTSA House Report, at 4 (citing Center for Responsible Enterprise and Trade & PwC, Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats, at 7–9 (February 2014), https://www.pwc.com/us/en/forensic-services/publications/assets/economic-impact.pdf); Sen. Rep. No. 114-220, 114th Cong., 2d Sess. 2 (Mar. 7, 2016) [hereinafter DTSA Senate Report] 2 (referring to study of Pricewaterhouse-Coopers LLP and the Center for Responsible Enterprise and Trade).
[14] 162 CONG. REC. S1627 (statement of Sen. Hatch).
[15] For the UTSA, *see* http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf. For UTSA jurisdictions, *see* http://www.uniformlaws.org/LegislativeFactSheet.aspx?title=Trade Secrets Act.
[16] Concerning the challenges under prior law in obtaining trade secret remedies, *see* M. Krotoski, Reviewing the Challenges in Bringing a Federal Trade Secret Case Under Current Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 475 (Dec. 19, 2014), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna_reviewingchallengesbringingfederaltradesecretcase_19dec14.ashx; M. Krotoski & D. Miller, What Legal Options Does Your Company Have After Your Trade Secrets Are Stolen by Cyber Espionage or Cyber Attack?, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 1719 (Apr. 17, 2015), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bbnainsight_legaloptionsaftertradesecretsstolen_17april15.ashx; M. Krotoski, The Time Is Ripe for a New Federal Civil Trade Secret Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 28 (Nov. 7, 2014), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bnapatent_krotoski-timefornewfederalciviltradesecretlaw_07nov14.ashx.
[17] 162 CONG. REC. S1627 (daily ed. Apr. 4, 2016) (statement of Sen. Hatch); *see also* the DTSA Senate Report, at 2 (noting that "[a]lthough the differences between State laws and the UTSA are generally relatively minor, they can prove case-dispositive" and listing examples).
[18] DTSA House Report, at 4 (noting state laws may "require companies to tailor costly compliance plans to meet each individual state's law").
[19] 162 CONG. REC. S1627 (daily ed. Apr. 4, 2016) (statement of Sen. Hatch); *see also* DTSA House Report, at 4 ("The theft increasingly involves the movement of secrets across state lines, making it difficult for state courts to efficiently order discovery and service of process."); *see generally* M. Krotoski, Reviewing the Challenges in Bringing a Federal Trade Secret Case Under Current Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 475 (Dec. 19, 2014), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna_reviewingchallengesbringingfederaltradesecretcase_19dec14.ashx.
[20] Fed. R. Civ. P. 45(b)(2) ("A subpoena may be served at any place within the United States").

[21] DTSA House Report, at 4.
[22] DTSA Senate Report, at 2.
[23] *See, e.g.*, H. Rep. No. 788, 104th Cong., Sess. 4 (1996) [hereinafter "1996 EEA House Report"] (noting "the nation's economic interests are part of its national security interests" and "threats to the nation's economic interest are threats to the nation's vital security interests"); *id*. at 6–7 (noting gaps under federal law).
[24] *See* 18 U.S.C. §§ 1831 (foreign economic espionage), 1832 (theft of trade secrets).
[25] *United States v. Williams,* 526 F.3d 1312 (11th Cir. 2008) (affirming conviction and sentence); *see also* Judgment, *United States v. Williams,* No. 06-CR-00313-03-JOF (N.D. Ga May 23, 2007) (ECF No.137).
[26] Plea Agreement, *United States v. Kolon Industries, Inc.,* No. 12-CR-00137 (E.D. Va. April 30, 2015) (ECF No. 191); Judgment (E.D. Va. May 1,2015) (ECF No.196); Complaint, *E. I. du Pont de Nemours and Company v. Kolon Industries Inc.,* No. 09-CV-00058 (E.D. Va. Feb. 3, 2009) (ECF No. 1); Dismissal (E.D. Va. May 27, 2015) (ECF No. 3056).
[27] *See* US Attorney's Manual § 9-59.100 (Economic Espionage Act of 1996 (18 U.S.C. §§ 1831-1837) — Prosecutive Policy), http://www.justice.gov/usam/usam-9-59000-economic-espionage, § 9-90.020 (National Security Matters Prior Approval, Consultation, and Notification.
[28] For more information on foreign economic espionage cases under Section 1831 cases, *see* M. Krotoski & J. Harrison, Reviewing the First Foreign Economic Espionage Cases, BNA's Patent, Trademark & Copyright Journal, 90 PTCJ 1951 (May 8, 2015), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bbnainsight_foreigneconomicespionage.ashx.
[29] Judgment, *United States v. Fei Ye, et al.,* No. 02-CR-20 145 (N.D. Cal. Nov. 25, 2008) (ECF No. 268); Judgment, *United States v. Fei Ye, et al.,* No. 02-CR-20145 (N.D. Cal. Nov. 25, 2008) (ECF No. 270); *see also* Press Release, US Dep't of Justice, Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China (Dec. 14, 2006).
[30] Redacted Plea Agreement, *United States v. Meng,* No. 04-CR-20216-JF (N.D. Cal. Aug. 1, 2007) (ECF No. 76); Judgment (N.D. Cal. June 24, 2008) (ECF No. 103); *see also* Press Release, US Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html.
[31] *United States v. Chung,* 633 F. Supp. 2d 1134 (C.D. Cal. 2009) (Memorandum of Decision), *aff'd*, 659 F.3d 815 (9th Cir. 2011) (affirming conviction and sentence); Judgment, *United States v. Chung,* No. 8:08-CR-00024 (C.D. Cal. Feb. 11, 2010) (ECF No. 172); *see also* Press Release, US Dep't of Justice, Former Boeing Engineer Sentenced To Nearly 16 Years In Prison For Stealing Aerospace Secrets For China (Feb. 8, 2010), http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2012/03/15/chungSent.pdf.
[32] Judgment, *United States v. Kexue Huang,* No. 10-CR-00102 (S.D. Ind. Mar. 6, 2012) (ECF No. 107); *see also* Press Release, US Dep't of Justice, Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec. 21, 2011), http://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets.
[33] Plea Agreement, *United States v. Elliot Doxer,* No. 11-CR-10268 (D. Mass. July 20, 2011) (ECF No. 19); *see also* Press Release, US Dep't of Justice, Employee of High Technology Company Charged with Seeking to Provide Confidential Business Information to a Foreign Government (Oct. 6, 2010), http://www.justice.gov/archive/usao/ma/news/2010/October/DoxerElliotPR.html.
[34] Judgment, *United States v. Liew,* No. 11-CR-0057 3 (N.D. Cal. Aug. 28, 2014) (ECF No. 921); Judgment, *United States v. Liew,* No. 11-CR-0057 3 (N.D. Cal. Sep. 2, 2014) (ECF No. 924); *see also* Press Release, US Dep't of Justice, Walter Liew Sentenced to 15 Years in Prison for Economic Espionage (July 11, 2014), http://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage.
[35] Pub. L. No. 112-269, 126 Stat. 2442 (Jan. 14, 2013), https://www.congress.gov/112/plaws/publ269/PLAW-112publ269.pdf; *see also* H. Rep. 112-610, 112th Cong., 2d Sess. (July 19, 2012), https://www.gpo.gov/fdsys/pkg/CRPT-112hrpt610/pdf/CRPT-112hrpt610.pdf.
[36] 158 CONG. REC. H5506 (daily ed. July 31, 2012) (remarks of Cong. Smith).
[37] Pub. L. No. 112-236, § 2, 126 Stat. 1627 (Dec. 28, 2012), https://www.congress.gov/112/plaws/publ236/PLAW-112publ236.pdf.
[38] *United States. v. Aleynikov*, 676 F.3d. 71 (2d Cir. 2012).
[39] *See* 162 CONG. REC. S1627 (daily ed. Apr. 4, 2016) (remarks of Sen. Hatch).
[40] Press Release, Senator Coons, Hatch Introduce Bill to Combat Theft of Trade Secrets and Protect Jobs, (Apr. 29, 2014), https://www.coons.senate.gov/newsroom/press-releases/senators-coons-hatch-introduce-bill-to-combat-theft-of-trade-secrets-and-protect-jobs (noting "the Department of Justice brought only 25 trade secret theft cases last year").

[41] DTSA Senate Report, at 3; *see also* DTSA House Report, at 4 ("[T]he FBI does not have the resources to investigate every case of trade secret theft. And the EEA, as a criminal statute, is not suited to making whole the victims of misappropriation.").
[42] DTSA House Report, at 4.
[43] S. 1890, 114th Cong., 1st Sess. (2015), https://www.congress.gov/114/bills/s1890/BILLS-114s1890is.pdf.
[44] H.R. 3326, 114th Cong., 1st Sess. (2015), https://www.congress.gov/114/bills/hr3326/BILLS-114hr3326ih.pdf.
[45] For further analysis of the trade secret reform legislation, *see* Statement of Mark Krotoski Submitted to the US Senate Judiciary Committee for the hearing "Protecting Trade Secrets: The Impact of Trade Secret Theft on American Competitiveness and Potential Solutions to Remedy This Harm" (Dec. 2, 2015) [hereinafter Krotoski SJC Statement], https://www.morganlewis.com/pubs/protecting-trade-secrets.
[46] During the Senate Judiciary Committee mark-up hearing on January 28, 2016, the authors offered an amendment in the nature of a substitute, which was unanimously accepted. S. 1890, 114th Cong., 2d Sess. (2016), https://www.congress.gov/114/bills/s1890/BILLS-114s1890rs.xml.
[47] DTSA Senate Report.
[48] *See* 162 CONG. REC. S1635 (daily ed. Apr. 4, 2016); *see also* US Senate, Defend Trade Secrets Act of 2016, Senate Roll Call Vote (Apr. 4, 2016), http://www.senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=114&session=2&vote=00039.
[49] Press Release, Judiciary Committee Approves Bipartisan Trade Secrets Legislation (Apr. 20, 2016), https://judiciary.house.gov/press-release/judiciary-committee-approves-bipartisan-trade-secrets-legislation.
[50] *See* 162 CONG. REC. H2046-47 (daily ed. Apr. 27, 2016); *see also* US House of Representatives, Defend Trade Secrets Act of 2016, Final Vote (Apr. 27, 2016), http://clerk.house.gov/evs/2016/roll172.xml.
[51] *See* Remarks by the president at Signing of S. 1890—Defend Trade Secrets Act of 2016 (May 11, 2016), https://www.whitehouse.gov/the-press-office/2016/05/11/remarks-president-signing-s-1890-defend-trade-secrets-act-2016. During congressional consideration of the legislation, the White House indicated support for the DTSA before final passage. *See* Statement of Administration Policy, S. 1890—Defend Trade Secrets Act of 2016 (Apr. 4, 2016), https://www.whitehouse.gov/sites/default/files/omb/legislative/sap/114/saps1890s_20160404.pdf.
[52] *See* H.R. 5233, 113th Cong., 2d Sess. (July 29, 2014), http://www.gpo.gov/fdsys/pkg/BILLS-113hr5233ih/pdf/BILLS-113hr5233ih.pdf.
[53] *See* Committee Markup Transcript of: H.R. 5233, the Trade Secrets Protection Act of 2014 (Sept. 17, 2014); *see also* H. Rep. No. 657, 113th Cong., 2d Sess. (2014); Press Release: Judiciary Committee Approves Trade Secrets Legislation (Sept. 17, 2014), http://judiciary.house.gov/index.cfm/press-releases?ContentRecord_id=316CB38D-2FE7-462A-8FCC-71205AEE2152.
[54] Hearings were also held during the prior Congress. *See* Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Senate Judiciary Comm., Subcomm. on Crime and Terrorism, 113th Cong. (2014), http://www.judiciary.senate.gov/meetings/economic-espionage-and-trade-secret-theft-are-our-laws-adequate-for-todays-threats; Trade Secrets: Promoting and Protecting American Innovation, Competitiveness, and Market Access in Foreign Markets: Hearing Before the House Judiciary Comm., Subcomm. on Courts, Intellectual Property, and the Internet, 113th Cong. (2014), https://www.gpo.gov/fdsys/pkg/CHRG-113hhrg88436/pdf/CHRG-113hhrg88436.pdf.
[55] 1996 EEA House Report, at 12 ("The definition of the term 'trade secret' is based largely on the definition of that term in the Uniform Trade Secrets Act.").
[56] 1996 EEA House Report, at 12 ("These general categories of information are included in the definition of trade secret for illustrative purposes and should not be read to limit the definition of trade secret. It is the Committee's intent that this definition be read broadly."); *see generally* Krotoski SJC Statement, at 17–18 (describing broader trade secret definition under the EEA and summarizing the legislative history).
[57] 18 U.S.C. § 1839(3).
[58] DTSA House Report, at 2, 14.
[59] *Id.* at 5.
[60] 18 U.S.C. § 1839(6)(A). The definition of "improper means" is "identical" to the UTSA definition. *Id.* at 10.
[61] 18 U.S.C. § 1839(6)(B); *see also* DTSA House Report, at 2–3, 14; DTSA Senate Report, at 10.
[62] 18 U.S.C. § 1836(c); *see also* DTSA Senate Report, at 9; DTSA House Report, at 13.
[63] 18 U.S.C. § 1836(b)(1) (emphasis added). As the Senate Report explains, the DTSA amends 18 U.S.C. § 1836 by striking the prior language of subsection (b), which provided that federal district courts have exclusive jurisdiction over civil actions brought by the attorney general for trade secret misappropriation. DTSA Senate Report, at 5; *see also* DTSA House Report, at 9.
[64] DTSA Senate Report, at 5; DTSA House Report, at 9.

[65] 162 CONG. REC. S1635 (daily ed. Apr. 4, 2016) (statement of Sen. Amy Jean Klobuchar); see also DTSA House Report, at 6 (noting the DTSA "will provide a single, national standard for trade secret misappropriation with clear rules and predictability for everyone involved"); DTSA Senate Report, at 14 (same).
[66] DTSA Senate Report, at 3 ("A Federal cause of action will allow trade secret owners to protect their innovations by seeking redress in Federal court, bringing their rights into alignment with those long enjoyed by owners of other forms of intellectual property, including copyrights, patents, and trademarks."); DTSA House Report, at 2 (noting DTSA provides for a federal trade secret claims "just as owners of other forms of intellectual property, including copyrights, patents, and trademarks, can seek remedies in Federal court for violations of their rights").
[67] *See* 17 U.S.C. §§ 501 *et seq*.
[68] *See* Lanham Act, 15 U.S.C. §§ 1051–1127.
[69] *See* US Patent Act, 35 U.S.C. §§ 1 *et seq*.
[70] Federal criminal statutes already apply to copyright and trademark infringement and trade secret misappropriation. Criminal copyright cases are authorized under 17 U.S.C. § 506(a) and 18 U.S.C. § 2319; criminal trademark cases are provided for under 18 U.S.C. § 2320. Trade secret misappropriation is subject to criminal penalties under the EEA, 18 U.S.C. §§ 1831–1839.
[71] 18 U.S.C. § 1838; *see also* DTSA House Report, at 5 (noting the DTSA "does not pre-empt these state [trade secret] laws and offers a complementary Federal remedy if the jurisdictional threshold for Federal jurisdiction is satisfied").
[72] 18 U.S.C. § 1836(b)(2)(A)(i); *see also* CONG. REC. S1635 (daily ed. Apr. 4, 2016) (colloquy between Sen. Judiciary Chairman Grassley and Sen. Hatch discussing the vital role of the seizure provision and balanced protections to protect against abuse); *see generally* M. Krotoski & M. Carr, Defend Trade Secrets Act *Ex Parte* Seizure Provision: Striking a Reasonable Balance in Addressing the Need for Prompt Recovery of Stolen Trade Secrets, BNA's Patent, Trademark & Copyright Journal, 90 PTCJ 3134 (Sept. 11, 2015), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bna-defend-trade-secrets-act-ex-parte-seizure-provision-11sept15.ashx.
[73] 18 U.S.C. § 1836(b)(2)(A)(i).
[74] DTSA House Report, at 10; DTSA Senate Report, at 6.
[75] 18 U.S.C. § 1836(b)(2)(A)(i).
[76] Pub. L. No. 98-473, § 1502, 98 Stat. 1837, 2178–79 (codified as amended at 15 U.S.C. § 1116(d) (2006)); *see also* See Joint Statement on Trademark Counterfeiting Legislation, 130 Cong. Rec. H12076, H12080 (Oct. 10, 1984) (discussing role for seizure provision).
[77] 17 U.S.C. §503(a)(3).
[78] DTSA Senate Report, at 12 (referring to Section 5 Sense of Congress language, noting "it is important when seizing information to balance the need to prevent or remedy misappropriation with the need to avoid interrupting the legitimate interests of the party against whom a seizure is issued, and the business of third parties"); DTSA House Report, at 16 (same).
[79] 18 U.S.C. § 1836(b)(2)(A)(i).
[80] *Id.*; *see also* DTSA Senate Report, at 6; DTSA House Report, at 10.
[81] 18 U.S.C. § 1836(b)(2)(B).
[82] *Id.* § 1836(b)(2)(E).
[83] *Id.*
[84] *Id.* § 1836(b)(2)(D).
[85] *Id.* § 1836(b)(2)(D).
[86] *Id.* §§ 1836(b)(2)(B)(v), (F)(i).
[87] *Id.* § 1836(b)(2)(F)(ii).
[88] *Id.* § 1836(b)(2)(C).
[89] *Id.* § 1836(b)(2)(F)(iii).
[90] *Id.* § 1836(b)(2)(G).
[91] *See, e.g.*, *Homecare CRM, LLC v. Adam Group, Inc.*, 952 F. Supp. 2d 1373, 1380 (N.D. Ga. 2013) (Rule 11 sanctions ordered when "the factual allegations in support of Homecare's trade-secrets claim do not, and did not at the time this action was filed, have evidentiary support . . . "); *see also Qad., inc. v. ALN Assoc., Inc.*, 18 U.S.P.Q. 2d 1122 (N.D. Ill. 1990) (dismissing Qad's trade secret count and awarding Rule 11 sanctions to defendant based on Qad's persistent failure to identify a claim); *Robertshaw Controls Co. v. Weerstra*, 1990 US Dist. LEXIS 17380 at *16 (W.D. Mich. 1990) (ordering Rule 11 sanctions when "[a]lthough the Court has concluded that it was at least reasonable to file the complaint, further investigation of the facts would have revealed that defendant never stole any confidential information or trade secrets").
[92] 18 U.S.C. § 1836(b)(3)(D).

[93] *Id*. § 1836(b)(2)(A)(ii)(V).
[94] DTSA Senate Report, at 6; DTSA House Report, at 10.
[95] 18 U.S.C. § 1835.
[96] 18 U.S.C. § 1835(b); *see also* DTSA Senate Report, at 11; DTSA House Report, at 14–15.
[97] 18 U.S.C. § 1835(b).
[98] *Id*. § 1835(a).
[99] Krotoski SJC Statement, at 17 (explaining role of Section 1835 to protect trade secrets in criminal cases).
[100] DTSA Senate Report, at 11; DTSA House Report, at 15. This disclosure limitation is consistent with case law. *See, e.g.*, *United States v. Lange*, 312 F.3d 263, 268-69 (7th Cir. 2002); *United States v. Yang*, 281 F.3d 534, 541–45 (6th Cir. 2002); *United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000); *United States v. Hsu*, 155 F.3d 189, 203 (3rd Cir. 1998).
[101] 18 U.S.C. § 1836(b)(3) (providing for civil remedies).
[102] *Id*. § 1836(b)(3)(A)(i). This language is based on the UTSA. DTSA Senate Report, at 8; DTSA House Report, at 12. As noted in the text, a couple of limitations have been adopted on the injunctive authority of a federal court under the DTSA.
[103] 18 U.S.C. § 1836(b)(3)(A)(ii).
[104] DTSA House Report, at 10 (noting "the court may decide to issue a third-party injunction preventing disclosure of the trade secret using its existing authority to provide equitable relief"); DTSA Senate Report, at 6 (same).
[105] [105] 18 U.S.C. § 1836(b)(3)(A)(iii).
[106] *Id*.
[107] DTSA Senate Report, at 9; DTSA House Report, at 12.
[108] 18 U.S.C. § 1836(b)(3)(A)(i).
[109] This amendment was offered by Sen. Dianne Feinstein (D-CA) during the January 28, 2016, Senate Judiciary Committee markup of S. 1890. *See also* DTSA Senate Report, at 8, 9 (noting concerns of Sen. Feinstein).
[110] *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995).
[111] DTSA Senate Report, at 8 n.16; *see also* DTSA House Report, at 12 n.12 (same).
[112] DTSA Senate Report, at 8; *see also* DTSA House Report, at 12 (same).
[113] 18 U.S.C. § 1836(b)(3)(A)(I) –(II).
[114] *Id*. § 1836(b)(3)(A)(i)(II).
[115] DTSA Senate Report, at 9; *see also* DTSA House Report, at 12–13.
[116] DTSA Senate Report, at 9 ("Some courts have found, based on the information possessed by the employee alone, that an injunction may issue to enjoin a former employee from working in a job that would inevitably result in the improper use of trade secrets.") ; *see also* DTSA House Report, at 12–13 (same).
[117] 18 U.S.C. § 1836(b)(3)(A)(I).
[118] 1996 EEA House Report, at 7 ("The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed."); S. Rep. No. 359, 104th Cong., 2d Sess. 12-13 (1996) [hereinafter 1996 EEA Senate Report] (noting safeguards to protect against applying the statute to general skills and knowledge); *see also* 142 CONG. REC. S12212-13 (daily ed. Oct. 2, 1996) (manager's statement).
[119] 1996 EEA Senate Report, at 12.
[120] 18 U.S.C. § 1836(b)(3)(B)(i). This provision is "drawn directly" from the UTSA. *See* DTSA Sentate Report, at 9; DTSA House Report, at 13.
[121] 18 U.S.C. § 1836(b)(3)(B)(ii).
[122] DTSA Senate Report, at 9.
[123] 18 U.S.C. §§ 1836(b)(3)(C), (D). These provisions are based on the UTSA. *See* DTSA Sentate Report, at 9; DTSA House Report, at 13.
[124] 18 U.S.C. § 1836(b)(3)(D).
[125] *Id*. § 1833(a)(2)(b).
[126] *Id*. § 1833(a)(2)(b)(4); *see also* DTSA House Report, at 16; DTSA Senate Report, at 12.
[127] 18 U.S.C. § 1833(b)(1)(A)(i)–(ii); *see also* DTSA House Report, at 16; DTSA Senate Report, at 12.
[128] 18 U.S.C. § 1833 (b)(2); *see also* DTSA House Report, at 16; DTSA Senate Report, at 12.
[129] 18 U.S.C. § 1833 (b)(2); *see also* DTSA House Report, at 16; DTSA Senate Report, at 12.
[130] DTSA Senate Report, at 12.
[131] 18 U.S.C. § 1833 (b)(3)(A); *see also* DTSA House Report, at 16; DTSA Senate Report, at 13.
[132] 18 U.S.C. § 1833 (b)(3)(D); *see also* DTSA House Report, at 16; DTSA Senate Report, at 13.
[133] 18 U.S.C. § 1833 (b)(3)(B); *see also* DTSA House Report, at 16; DTSA Senate Report, at 13.
[134] 18 U.S.C. § 1833 (b)(3)(C); *see also* DTSA House Report, at 16; DTSA Senate Report, at 13.

[135] DTSA House Report, at 8; DTSA Senate Report, at 14.
[136] The amendment offered in the nature of a substitute during the Senate Judiciary Committee mark-up was unanimously accepted. S. 1890, 114th Cong., 2d Sess. (2016), https://www.congress.gov/114/bills/s1890/BILLS-114s1890rs.xml.
[137] 18 U.S.C. § 1836(b)(2)(D)(i).
[138] *Id.* § 1836(b)(2)(D)(ii).
[139] *Id.* § 1836(b)(2)(H).
[140] *Id.* § 1836(d).
[141] DTSA Senate Report, at 9–10; DTSA House Report, at 13.
[142] *Id.*
[143] 18 U.S.C. § 1836(d).
[144] *Id.* § 1832(b); *see also* DTSA Senate Report, at 11; DTSA House Report, at 14.
[145] 18 U.S.C. §§ 1961–1968. The RICO statute was enacted as part of the Organized Crime Control Act of 1970. *See* Pub. L. No. 91–452, title IX, § 901(a), Oct. 15, 1970, 84 Stat. 942.
[146] 18 U.S.C. § 1962 (Prohibited activities). Under RICO, criminal penalties are set forth in 18 U.S.C. § 1963, and civil remedies are provided in 18 U.S.C. § 1964.
[147] 18 U.S.C. § 1964(c).
[148] DTSA, § 3(b) (amending 18 U.S.C. § 1961(1) by adding 18 U.S.C. §§ 1831, 1832); *see also* DTSA Senate Report, at 11.
[149] 18 U.S.C. § 1961(5).
[150] S. 1890, § 4; *see also* DTSA Senate Report, at 11; DTSA House Report, at 15–16.
[151] *Id.*
[152] S. 1890 § 6(a); *see also* DTSA Senate Report, at 12; DTSA House Report, at 16.
[153] S. 1890 § 6(b)–(c).
[154] 18 U.S.C. § 1833(b)(3)(A).
[155] *Id.* § 1833(b)(4).
[156] *Id.* § 1833(b)(3)(C).
[157] For more guidance on the notice requirement, *see* our LawFlash, New Federal Law to Require Immediate Change to Agreements Governing Trade Secrets (May 10, 2016), https://www.morganlewis.com/pubs/new-federal-law-to-require-immediate-change-to-agreements-governing-trade-secrets#sthash.G8TuNZmO.dpuf.
[158] *Id.* § 1836(e).
[159] DTSA Senate Report, at 12 (referring to Section 5 Sense of Congress language, noting "it is important when seizing information to balance the need to prevent or remedy misappropriation with the need to avoid interrupting the legitimate interests of the party against whom a seizure is issued, and the business of third parties"); DTSA House Report, at 16 (same).
[160] *See* UTSA, § 6.
[161] For more information on the role of reasonable measures to protect trade secrets, *see* M. Krotoski, Do You Know Whether Your Trade Secrets Are Adequately Protected?, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 181 (Nov. 21, 2014), https://www.morganlewis.com/~/media/files/publication/outside%20publication/article/bloombergbna_patenttrademarkcopyrightjournal_21nov14.ashx.
[162] *See also* DTSA Senate Report, at 2 (noting "what measures are necessary to satisfy the requirement that the owner employ 'reasonable measures' to maintain secrecy of the information" as a potentially "case-dispositive" factor).
[163] 18 U.S.C. § 1838(3) (defining trade secret and noting the "reasonable measures" requirement); *see also* 1996 EEA House Report, at 12–13 (discussing "reasonable measures" requirement).
[164] 1996 EEA House Report, at 7.
[165] *Id.* § 1836(b)(3)(A)(I) – (II).
[166] 18 U.S.C. § 1836(b)(1) (emphasis added). As the Senate Report explains, the DTSA amends 18 U.S.C. § 1836 by striking the prior language of subsection (b), which provided that federal district courts have exclusive jurisdiction over civil actions brought by the attorney general for trade secret misappropriation. DTSA Senate Report, at 5; *see also* DTSA House Report, at 9.
[167] *See* UTSA, § 6 (statute of limitations).
[168] *See also* DTSA Senate Report, at 2 (noting "the scope of information protectable as trade secret" as a potentially "case-dispositive" factor).
[169] *See also* DTSA Senate Report, at 2 (noting as a potentially "case-dispositive" factor).
[170] *See also* DTSA Senate Report, at 2 (noting as a potentially "case-dispositive" factor).

[171] Cal. Civ. Proc. Code. § 2019.210.
[172] DTSA House Report, at 5 (noting the availability of "a complementary Federal remedy if the jurisdictional threshold for Federal jurisdiction is satisfied").
[173] DTSA Senate Report, at 15.