BOSTON BAR ASSOCIATION
YEAR IN REVIEW (2015)
TRADE SECRETS

By

Russell Beck[1]
Beck Reed Riden LLP
155 Federal Street, Suite 1302
Boston, MA 02110
www.beckreedriden.com
rbeck@beckreed.com
Blog: faircompetitionlaw.com

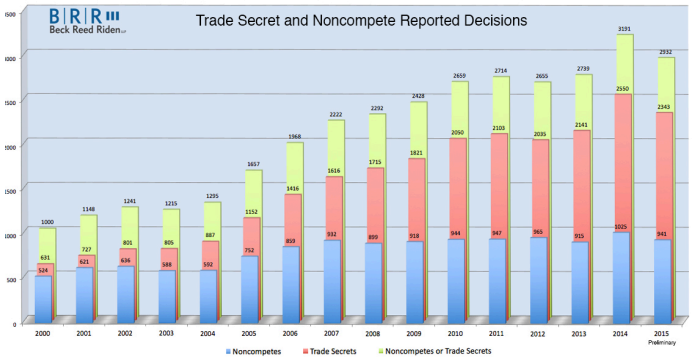
[1] Special thanks to Nicole Corvini Daly, Hannah Joseph, and Will Haddad for their tremendous assistance, updates, and additions on several of the topics.

Table of Contents

I. Introduction/Statistics

2015 was a year of continued stage setting, with no major changes, in the landscape of trade secrets law. There have been a handful of developments on both the civil side and criminal side, through case law as well as through legislation. The highlights are below.

Before turning to the specific noteworthy cases and legislation of the past year, there are some statistics that bear mention. Each year I have run a "back of the envelope" calculation of all decisions involving trade secrets and noncompetition agreements (also known as "noncompetes"[2]). This year's chart is to the right.[3] The blue bars (front row) reflect all reported noncompete decisions, the red bars (middle row) are all reported trade secrets decisions, and the yellow bars (back row) are all decisions involving noncompetes, trade secrets, or both. It bears noting that the closer the year analyzed to the date on which the analysis is run, the more underreported the number tends to be when compared to later review. Accordingly, I fully expect that the numbers for 2015 (and other recent years) will ultimately be hirer than reflected in the graph.



II. Economic Espionage Act: A Private Right of Action Looms Again… And This Time They Mean It – Really!

The federal government has remained focused on the protection of trade secrets, both from the criminal enforcement standpoint and in connection with a civil private right of action. The impetuous for this effort is reflected in part in then-Attorney General Eric Holder's comment two years ago that,

> [T]here are only 'two categories' of companies affected by trade secret theft – "[T]hose that know they've been compromised and those that don't know yet."

Attorney General Eric Holder Speaks at the Administration Trade Secret Strategy Rollout (Feb. 20, 2013).[4]

---

2 Noncompetes are included because they are frequently a key tool used by companies to protect their of trade secrets.

3 A larger image of the chart is available here: https://faircompetitionlaw.files.wordpress.com/2014/12/noncompete-and-trade-secret-cases-survey-graph-20141214.png.

4 The speech is available at http://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-administration-trade-secret-strategy-rollout.

Last year, FBI director James Comey echoed those comments, though highlighting the connection with China:

> There's only two types of corporations – big corporations – in America. Those who have been hacked by the Chinese, or those who don't yet know they've been hacked by the Chinese.
>
> It is sapping the lifeblood of a lot of these companies, and it's about our ability to compete and about the ability of our people to get and keep good jobs.

Interview with ABC News (May 19, 2014).[5]

This increasing threat to trade secrets has caused the federal government to the focus not just on government enforcement, but private sector efforts as well.[6] Consistent with that focus, Congress has been working on creating a potential federal private right of action under the Economic Espionage Act of 1996 (the "EEA"), 18 U.S.C. §§ 1831-1839.

The EEA was enacted in 1996 to criminalize the misappropriation of trade secrets. The statute has two operative parts: Section 1831(a) covering "economic espionage" (*i.e.*, theft of trade to benefit a foreign power) and section 1832(a), covering "theft of trade secrets" (*i.e.*, the theft of trade secrets to benefit someone other than the owner of the secrets).

Section 1831(a) provides as follows:

> In General.— Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly—
>
> > (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
> >
> > (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;

---

5 The interview is available at available at http://abcnews.go.com/US/fbi-director-tells-abc-news-us-goods-china/story?id=23787051.

6 *See* "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets" available at http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

(3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

(4) attempts to commit any offense described in any of paragraphs (1) through (3); or

(5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

Section 1832(a) provides as follows:

Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly[7]—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

---

[7] The Theft of Trade Secrets Clarification Act of 2012 (http://www.govtrack.us/congress/bills/112/s3642/text) was passed on December 28, 2012, to amend the EEA in response to *US v. Aleynikov*, 676 F.3d 71 (2nd Cir. 2012). As a result, the relevant provision of section 1832(a) was amended as follows (crossed-out language was deleted and bolded was inserted):

Whoever, with intent to convert a trade secret, that is related to ~~or included in a product that is produced for or placed in~~ **a product or service used in or intended for use in** interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly

> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

Prior to 2013, the criminal penalties under section 1831 included a fine of up to $500,000 (or up to $10,000,000 for an organization) and imprisonment of up to 15 years. 18 U.S.C. § 1831(b). The criminal penalties under section 1832 included a fine (up to $5,000,000 for an organization) and imprisonment of up to 10 years. 18 U.S.C. § 1832(b). However, on January 14, 2013, President Obama signed the Foreign and Economic Espionage Penalty Enhancement Act of 2012.[8] In addition to requiring a review of sentencing guidelines, the Act increased fines for foreign espionage under section 1831. Specifically, the fines for individuals went from $500,000 to $5,000,000, and the fines for organizations increased from $10,000,000 to "not more than the greater of $10,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided."

On the civil side, the U.S. Attorney General can bring an action under the EEA to obtain injunctive relief. 18 U.S.C. § 1836(a). There is, however, no private right of action under the EEA. As a result of the increase in the recognized need to protect trade secrets, there have been increasing Congressional efforts to create a private right of action. Given the momentum Congress has made in changing the EEA over the past two years, there is a belief that Congress is likely to pass some version of a bill to create a private right of action.

The effort started with the Protecting American Innovation and Trade Secrets Act of 2012 introduced by Senator Christopher Coons (D. Delaware) and retired Senator Herbert Kohl (D. Wisconsin). That bill would have created a private right of action if certain requirements were met (specifically, a "substantial need for nationwide service of process or misappropriation of trade secrets from the United States to another country"). It would have also established a mechanism for *ex parte* seizure orders for "the seizure of any property (including computers) used, in any manner or part, to commit or facilitate the

---

[8] http://www.gpo.gov/fdsys/pkg/BILLS-112hr6029enr/pdf/BILLS-112hr6029enr.pdf

commission of the violation alleged in the civil action" and for "the preservation of evidence in the civil action." That bill died in committee.[9]

In 2013, Representative Zoe Lufgren (D-CA) introduced an abbreviated bill known as the "Private Right of Action Against Theft of Trade Secrets Act of 2013." That bill provides for the addition of the following language to be added to section 1832 of the EEA:

> (c) Any person who suffers injury by reason of a violation of this section may maintain a civil action against the violator to obtain appropriate compensatory damages and injunctive relief or other equitable relief. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.
>
> (d) For purposes of this section, the term without authorization shall not mean independent derivation or working backwards from a lawfully obtained known product or service to divine the process which aided its development or manufacture.

In 2014, the effort has continued with a similar bills known as the Trade Secrets Protection Act of 2014 and the Defend Trade Secrets Act of 2014. Those bills ultimately died.

2015 was déjà vu all over again.

On July 29, 2015, a bipartisan group of Senators (Orrin Hatch (R-UT), Christopher Coons (D-DE), Jeff Flake (R-AZ), Richard Durbin, (D-IL), Thom Tillis (R-NC), and Tammy Baldwin (D-WI)) and Representative Doug Collins (R-GA) and 15 other Congressmen and Congresswomen) introduced a bill known as the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326)[10]. The bill essentially creates a federal private right of action for the misappropriation of trade secrets, largely adopting the definition of misappropriation from the Uniform Trade Secrets Act ("UTSA").

One key difference, however, is that in addition to expressly permitting reverse engineering (a concept widely accepted in trade secrets law), the bill permits "independent derivation." That term was carried over from prior bills and is was likely intended to mean "independent *development*." This is not a distinction without a difference. While independent development is a widely recognized and accepted concept under existing trade secrets laws (*i.e.*, the ability of some third party to come up with the same idea entirely on its own), independent derivation could be interpreted to suggest that it is permissible to create new trade secrets from the misappropriated information, so long as the new secrets are different from the misappropriated trade secret (*i.e.*, new trade secrets

---

9 https://www.govtrack.us/congress/bills/112/s3389

10 https://www.govtrack.us/congress/bills/114/s1890/text

developed through misuse of the misappropriated trade secrets). This is a significant mistake that needs to be addressed.

The DTSA would strike section 1836 of title 18(b) of the US Code (providing for exclusive original jurisdiction of the US district courts over civil actions brought by the US Attorney General under 18 USC 1836(a)). The new section 18(b) permits private rights of action as follows:

> An owner of a trade secret may bring a civil action under this subsection if the person is aggrieved by a misappropriation of a trade secret that is related to a product or service used in, or intended for use in, interstate or foreign commerce.

Perhaps most controversial about the bill are the provisions (similar to prior bills) that permit the issuance of an *ex parte* civil seizure order. Specifically, on motion supported by an affidavit or verified complaint containing satisfying the requirements set forth in the bill for the court to issue a seizure order, the court may order "the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."

To issue the order, the court must find that the following "clearly appears from specific facts":

> (I) an order issued pursuant to Rule 65(b) of the Federal Rules of Civil Procedure would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;
>
> (II) an immediate and irreparable injury will occur if such seizure is not ordered;
>
> (III) the harm to the applicant of denying the application outweighs the harm to the legitimate interests of the person against whom seizure would be ordered of granting the application and substantially outweighs the harm to any third parties who may be harmed by such seizure;
>
> (IV) the applicant is likely to succeed in showing that—
>
> (aa) the information is a trade secret;
>
> (bb) the person against whom seizure would be ordered—
>
> (AA) misappropriated the trade secret of the applicant by improper means; or

(BB) conspired to use improper means to misappropriate the trade secret of the applicant; and

(cc) the person against whom seizure would be ordered has possession of the trade secret;

(V) the application describes with reasonable particularity the matter to be seized and, to the extent reasonable under the circumstances, identifies the location where the matter is to be seized;

(VI) the person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person; and

(VII) the applicant has not publicized the requested seizure.

Assuming these facts are established "clearly," the court is then to provide the narrowest seizure necessary and "direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret that are unrelated to the trade secret that has allegedly been misappropriated." The bill provides additional measures to protect the accused infringer, including the protection of the confidentiality of the information and integrity of the information, a hearing (on notice) within 7 days, the requirement of a posting of security by the person obtaining the order, protection from publicity, that the seized property be held by the court, expedited discovery, motions to encrypt electronic information, and the relief afforded by section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. 1116(d)(11)) where property was wrongfully seized (*i.e.*, damages including lost profits, cost of materials, loss of goodwill, punitive damages, interest, and where the seizure was sought in bad faith without extenuating circumstances, reasonable attorney's fees).

The bill also provides for injunctive relief and damages typical for traditional trade secrets claims, *i.e.*, damages for the actual loss (typically, lost profits) and unjust enrichment (typically, disgorgement of profits), or a reasonable royalty. In addition, for willful and malicious misappropriation, the act permits exemplary damages up to three times the amount of the damages. Accordingly, in contrast to Massachusetts' double damages (under the trade secrets statute (G.L. c. 93, § 42)) or more typical typical treble damages awards (such as under the Uniform Trade Secrets Act or G.L. c. 93A), the DTSA provides for the possibility of quadruple damages.

Other aspect of the bill creating some consternation is the fact that it vests original jurisdiction – but, in contrast to the current section 18(b), *not* exclusive – jurisdiction in the US District Courts. Accordingly, state courts could be called upon to consider claims under the DSTA and, more concerning for some, issue *ex parte* seizure orders. This issue is not

significant in Massachusetts where the state judiciary is well regarded, but there is significant concern in certain other states where that is not the case.

Also controversial is the bill's five-year statute of limitations. The UTSA provides for three years, as do the majority of states.

Separately, the bill also provides that by the end of the first year after its enactment, and then "biannually thereafter, the Attorney General, in consultation with the Intellectual Property Enforcement Coordinator, the Director, and the heads of other appropriate agencies, shall submit to the Committees on the Judiciary of the House of Representatives and the Senate, and make publicly available on the Web site of the Department of Justice and disseminate to the public through such other means as the Attorney General may identify, a report on" trade secrets misappropriation occurring outside the United States, progress in efforts to combat such misappropriation, and recommendations for additional actions.

On December 10, 2015, the Senate Committee on the Judiciary held a hearing to consider, among other things, the DTSA. The committee took testimony from DuPont, Corning, and a Mitchell Hamline School of Law Professor Sharon Sandeen. In addition, Senator Coons introduced several letters of support for the bill, including a letter from a group of private practitioners around the country (including me).[11] According to the report of audience members, Senator Sheldon Whitehouse (D-RI) asked for additional information concerning the degree of force that may be used when executing a seizure order and the nature of the privacy concerns implicated by such orders.[12]

Since its introduction, the bill has received the support of a total of 24 Senators and 108 Congressmen and Congresswomen and no opposition.

III. Computer Fraud and Abuse Act: The Fraud Awakens

> Computers have become an indispensable part of our daily lives. We use them for work; we use them for play. Sometimes we use them for play at work. Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

---

11 The letter is available at https://tradesecretstrends.crowellmoringblogs.com/wp-content/uploads/sites/11/2015/12/Trade-Secret-Practitioner-Letter-of-Support-Final.pdf.

12 *See* https://www.crowelltradesecretstrends.com/2015/12/dupont-corning-and-others-speak-out-in-support-of-defend-trade-secrets-act-at-senate-judiciary-committee-hearing/.

U.S. v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc).

Background

> In 1984, Congress initiated a campaign against computer crime by passing the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984. Pub.L. No. 98–473, 98 Stat. 2190. Shortly thereafter, in 1986, it expanded the Act with a revised version, the Computer Fraud and Abuse Act of 1986, Pub.L. No. 99–474, 100 Stat. 1213. Today, the CFAA remains primarily a criminal statute designed to combat hacking. *A.V. ex rel. Vanderhye v. iParadigms, LLC,* 562 F.3d 630, 645 (4th Cir.2009). Nevertheless, it permits a private party "who suffers damage or loss by reason of a violation of [the statute]" to bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). Notably, although proof of at least one of five additional factors is necessary to maintain a civil action, a violation of any of the statute's provisions exposes the offender to both civil and criminal liability.[13]
>
> Among other things, the CFAA renders liable a person who (1) "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer," in violation of § 1030(a)(2)(C); (2) "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value," in violation of § 1030(a)(4); or (3) "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[,] or ... causes damage and loss," in violation of § 1030(a)(5)(B)-(C).

WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 201 (2012) (footnote omitted).

Liability for violation of the act is both criminal and civil. 18 U.S.C. § 1030(c), (g). In a civil action, a successful plaintiff is entitled to "compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g). For most claims likely to arise in the civil context, the damage caused by the wrongful access must aggregate $5,000 in value during any one-year period. 18 U.S.C. § 1030(g); *see, e.g.*, Walsh v. Microsoft Corporation, 63 F.Supp. 3d 1312, 2014 WL 5365450, at *5 (W.D. Wash. Oct. 20, 2014). This requirement is frequently satisfied if forensic work is necessary to determine whether there was a violation. *See Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg. & Consulting, LLC*, 600 F. Supp. 2d 1045, 1052–53 (E.D. Mo. 2009). However, if the alleged violation is merely copying information from a computer, the dollar threshold may be moot, as copying (by itself

---

[13] David Nosal (the subject of the high-profile *Nosal* decision quoted above and discussed herein) was convicted in 2013 for violating the CFAA and later sentenced to jail time (stayed pending appeal). In October 2015, the Ninth Circuit heard oral argument in Nosal's pending appeal of his CFAA conviction.

without, for example, deleting the original) may not even constitute "damage" within the meaning of law. *See NetApp, Inc. v. Nimble Storage, Inc.*, 2015 WL 400251, at *11-15 (N.D. Cal. Jan. 29, 2015) (summarizing the divide).

Split in Scope

There is another deepening split in the circuits concerning the reach of the CFAA – commonly arising in connection with employees (or former employees) use of their employer's (or former employer's) computers to misappropriate confidential information (or for other illicit purposes). The issue turns on what it means to access a computer "without authorization" or by "exceed[ing] authorized access," the latter of which is defined to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6).

The issue has been framed by the Ninth Circuit (in an *en banc* opinion issued in 2012) as follows:

> The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). This language can be read either of two ways: First, . . . it could refer to someone who's authorized to access only certain data or files but accesses unauthorized data or files—what is colloquially known as "hacking." For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would "exceed[ ] authorized access" if he looks at the customer lists. Second, . . . the language could refer to someone who has unrestricted physical access to a computer, but is limited in the use to which he can put the information. For example, an employee may be authorized to access customer lists in order to do his job but not to send them to a competitor.

Nosal, 676 F.3d at 856-57.

Stated somewhat differently, the Fourth Circuit summarized the issue as follows:

> The crux of the issue presented here is the scope of "without authorization" and "exceeds authorized access." We particularly examine whether these terms extend to violations of policies regarding the use of a computer or information on a computer to which a defendant otherwise has access.

WEC Carolina Energy Solutions LLC, 687 F.3d at 203.

Prior to the Ninth and Fourth Circuit decisions quoted above and discussed in more detail below, the First, Fifth, Seventh, Ninth, and Eleventh Circuits had all spoken on the scope of "without authorization" and "exceeds authorized access" – and all but the Ninth Circuit had taken a broad interpretation to the CFAA.[14] *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001) (addressing the issue indirectly); *United States v. John,* 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin,* 440 F.3d 418 (7th Cir. 2006); *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127 (9th Cir. 2009); *United States v. Rodriguez,* 628 F.3d 1258 (11th Cir. 2010). Under the broad view (which was initially articulated by the Seventh Circuit), "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it." *See Int'l Airport Ctrs., LLC v. Citrin,* 440 F.3d 418, 420–21 (7th Cir. 2006).

The three most recent circuit court decisions that substantively address the scope split, *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012 (en banc), *WEC Carolina Energy Solutions LLC v. Miller,* 687 F.3d 199 (4th Cir. 2012), and *United States v. Valle*, 807 F.3d 508 (2nd Cir. 2015) have gone the other way and each adopts the narrow view.[15]

In reaching its conclusion in *Nosal*, the Ninth Circuit stated:

> We need not decide today whether Congress *could* base criminal liability on violations of a company or website's computer use restrictions. Instead, we hold that the phrase "exceeds authorized access" in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly. The rule of lenity requires "penal laws ... to be construed strictly."

---

[14] As discussed below, there is some question as to whether the First Circuit has in fact adopted this approach.

[15] In *United States v. Christenson*, the Ninth Circuit recently confirmed the importance and staying power of its decision in *Nosal*. *See* 801 F.3d 970, 990-92 (9th Cir. 2015). In the underlying case, the jury had received the following instruction, to which the defense did not object, concerning authorization under the CFAA:

> [A] defendant exceeds authorized access . . . when the defendant accesses a computer with authorization but uses such access to obtain information in the computer that the defendant is not entitled to obtain.

Id. at 991. The Court, exercising plain error review, held that the jury instruction violated the requirements of *Nosal*: "Although it was not obvious to the district court at the time, this definition of exceeding authorized access was flawed in that it allowed the jury to convict for unauthorized use of information rather than only for unauthorized access. Such an instruction is contrary to *Nosal*, and therefore the instruction constituted plain error." *Id*. at 992.

United States v. Wiltberger, 18 U.S. (5 Wheat.) 76, 95, 5 L.Ed. 37 (1820). "[W]hen choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *Jones,* 529 U.S. at 858, 120 S.Ct. at 1912 (internal quotation marks and citation omitted).

Similarly, the Fourth Circuit summed up its holding as follows: "[W]e conclude that an employee 'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access. Notably, neither of these definitions extends to the improper *use* of information validly accessed." *WEC Carolina Energy Solutions LLC v. Miller,* 687 F.3d at 204 (citation omitted).[16]

Recently, on December 3, 2015, the Second Circuit weighed in for the first time on this issue and joined the Ninth and Fourth Circuits in adopting the narrow view. In *United States v. Valle*, the Second Circuit considered, among other things, Valle's appeal of his conviction for having violated the CFAA.[17] On that issue, the Court stated that

The dispositive question is whether Valle "exceeded authorized access'

---

[16] While the Sixth Circuit has not explicitly adopted either the narrow or broad approach, the Court in *United States v. Shahulhameed,* ___ Fed. Appx. ___, 2015WL 6219237, recently affirmed a defendant's CFAA conviction, finding that he was not "authorized" when he accessed his former employer's systems to launch a cyber attack in the overnight hours between learning of his termination and the employer's disabling of his user account. Although the timing of the defendant's termination and bad acts create a factual wrinkle that makes it difficult to draw any definitive conclusion as to whether the Sixth Circuit will adopt the narrow or broad approach, it is worth noting that the Court cited *WEC Carolina Energy Solutions LLC*, discussed above, as follows: "The evidence also shows that Shahulhameed acted without authorization. Authorization requires approval or sanction. *See WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 204 (4th Cir.2012)." This reference to the Fourth Circuit's decision may signal the Sixth Circuit's inclination toward the narrow approach adopted in the *WEC Carolina Energy Solutions LLC* case.

[17] In the underlying action, Valle had been charged with various crimes, including violation of the CFAA. The evidence established, among other things, that Valle, then a New York Police Department Officer, engaged in disturbing, violent, sexual fetish fantasy discussions via emails and web chats which "consisted of gruesome and graphic descriptions of kidnapping, torturing, cooking, raping, murdering, and cannibalizing various women." *Valle*, 807 F.3d at 512. As an NYPD Officer, Valle had access to a computer program, called the Omnixx Force Mobile ("OFM"), which permits officers to search various restricted databases, which include personal information such as home addresses and dates of birth. Per NYPD policy, an officer was permitted to access these databases solely for official use. In May 2012, Valle accessed the OFM to research a specific woman, Maureen Hartigan, whom he had discussed kidnapping in his online communications. Valle's accessing of the OFM to research Hartigan with no official purpose served as the basis for the CFAA charge against him. *Id*. at 513.

> when he used his access to OFM to conduct a search for Maureen Hartigan with no law enforcement purpose. Valle concedes that he violated the terms of his employment by putting his authorized computer access to personal use, but claims that he did not violate the statute because he never "used his access to obtain any information he was not entitled to obtain. In other words, Valle argues that he did not "exceed authorized access" because he was otherwise authorized to obtain the database information about Hartigan; his non-law enforcement purpose in running the search is irrelevant. The Government contends that Valle "exceeded authorized access" because his authorization to access OFM was limited to law enforcement purposes and he conducted a search for Hartigan with no such purpose.

807 F.3d at 523-24 (internal citations omitted). In other words, the prosecution argued for the broad view while Valle argued for the narrow view (previously adopted only by the Ninth and Fourth Circuits).

In reaching its decision to reverse Valle's CFAA conviction, the Second Circuit conducted a detailed analysis of the development of the rift in the circuits and the CFAA's legislative history. *Id.* at 524-26. The Court found support in the CFAA's legislative history for both the narrow and broad views but determined that "we are required by the rule of lenity to adopt the interpretation that favors the defendant." The Court "decline[d] to adopt the prosecution's construction, which would criminalize the conduct of millions of ordinary computer users and place [the Court] in the position of a legislature." *Id.* at 527. Instead, the Court, while recognizing the egregious factual circumstances at hand, ultimately reasoned that:

> Whatever the apparent merits of imposing criminal liability may seem to be *in this case*, we must construe the statute knowing that our interpretation of "exceeds authorized access" will govern many other situations. It is precisely for this reason that the rule of lenity requires that Congress, not the courts or the prosecutors, must decide whether conduct is criminal. We, on the other hand, are obligated to "construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals." While the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters. A court should not uphold a highly problematic interpretation of a statute merely because the Government promises to use it responsibly.

The Second Circuit's decision in *Valle* further emphasizes the divide in the circuits. The issue is ripe for the Supreme Court to weigh in and resolve.[18]

---

[18] Although the plaintiff in *WEC Carolina Energy Solutions* initially petitioned the Supreme Court for certiorari, the petition was withdrawn.

The Gap Continues to Widen, Including with a Legislative Twist

The battle over the scope issue has continued in the lower courts as well. For example, in *Facebook, Inc. v. Power Ventures, Inc.*, 2013 WL 5372341 (C.D. Calif., Sept. 25, 2013) (denying a motion to reconsider), a website that aggregated data from social media sites like Facebook was found to have violated the CFAA. Of particular note, in the summary judgment decision that was being reconsidered, the court had observed that while using a website such a Facebook.com in violation of its terms of use is not a violation of the CFAA, "access[ing] the network in a manner that circumvents technical or code-based barriers in place to restrict or bar a user's access" can be a violation. 844 F.Supp.2d 1025, 1036, 1040 (N.D. Calif. Feb. 16, 2012) (noting that California's penal code's requirement of "permission" is the equivalent of the CFAA's requirement of "authorization"). In a similar vein, the Northern District of California denied a motion to dismiss the CFAA claim where the defendant (a competitor of Craigslist) "scraped" the plaintiff's website after its authorization to do so had been revoked. *Craigslist, Inc. v. 3Taps, Inc.*, 2013 WL 1819999, at *3 (N.D. Cal. April 30, 2013).

In Massachusetts, several cases have wrestled with the First Circuit decision in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001), and struggled to discern the proper interpretation of the CFAA. In *Advanced Micro Devices, Inc. v. Feldstein*, 2013 WL 2666746, at *3 (D. Mass. June 10, 2013), United States District Court Judge Hillman, adopted the narrow interpretation, noting that the "narrow interpretation reflects a technological model of authorization, whereby the scope of authorized access is defined by the technologically implemented barriers that circumscribe that access," and the "broader interpretation defines access in terms of agency or use." In so doing, Judge Hillman disagreed with Judge Gorton's interpretation of *EF Cultural Travel*, as favoring a broad interpretation. Later in the year, in *Enargy Power Co. Ltd v. Xiaolong Wang*, 2013 WL 6234625 (D. Mass. Dec. 3, 2013), Judge Casper took a more nuanced approach, finding that Wang was not specifically provided access, and therefore defendants' access exceeded what was authorized. *See also Moca Systems, Inc. v. Bernier*, 2013 WL 6017295, at *3 (D. Mass. Nov. 12, 2013) (in which Chief Magistrate Judge Sorokin described the different interpretations, but noted that he did not need to reach a decision as to which was the proper interpretation) and *Pine Environmental Services, LLC v. Carson*, 43 F. Supp.3d 71 (Aug. 20, 2014) (in which Judge Talwani took a unique approach to narrowing the CFAA by finding that it did not apply because the computer was not a "protected computer" insofar as it was not being used in interstate commerce at the time of the unauthorized use – even though it had been used in interstate commerce prior to that point). It bears mention, however, that The *Pine Environmental Services* decision may be at odds with the Ninth Circuit's interpretation "that a computer falls within the definition of a 'protected computer' if it has internet access." *Roadlink Workforce Solutions, L.L.C. v. Malpass*, 2013 WL 5274812, at *5 (W.D. Wash. Sept. 18, 2013) (citing *U.S. v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012)).

With all of the cases in the background and recent events raising concerns, the legislature and even the Obama Administration has entered the fray. Congress has

amended the CFAA several times over the years, each time broadening it. *See Guest-Tek Interactive Entm't Inc. v. Pullen*, 665 F. Supp. 2d 42 (D. Mass. Oct. 19, 2009). However, in 2011, computer programmer/Internet "hacktivist" Aaron Swartz was arrested for hacking into and "downloading academic journal articles by the hundreds of thousands" from the electronic academic journal JSTOR. *The inside story of MIT and Aaron Swartz*, Boston Globe, Metro (March 30, 2014).[19] "The cascade of events that followed would culminate in tragedy: a Secret Service investigation, a federal prosecution, and ultimately Swartz's suicide." *Id.* Swartz's suicide prompted United States Representatives Zoe Lufgren (D-CA), James Sensenbrenner (R-WI), Mike Doyle (D-PA), Yvette Clarke (D-NY), and Jared Polis (D-CO) to file a bill called "Aaron's Law"[20] to narrow the reach of the CFAA. That bill died in 2013.[21]

In early 2015, in response to the news about rampant data breaches, the Obama Administration has proposed "modernizing the Computer Fraud and Abuse Act."[22] Such "modernization" would both broaden and strengthen the CFAA. For example, if adopted, it would be a violation for someone "to intentionally accesses a protected computer without authorization or exceed[] authorized access, and thereby obtain[] information from such protected computer; or . . . intentionally exceed[] authorized access to a protected computer, and thereby obtain[] information from such computer" if "the value of the information obtained exceeds $5,000," "the offence was committed in furtherance of any felony" or "the protected computer is owned or operated by or on behalf of a governmental entity . . . ." Further, the criminal penalties for such conduct would be significantly increased.

As of January 2016, the proposed modernization has not been put into effect. Whether and how Congress and the President ultimately balance the tension between the perceived need to narrow the scope of the CFAA as highlighted by the Aaron Swartz suicide with the need to increase its scope to address the increasing risk of potentially devastating computer intrusions remains to be seen.

---

19 *Available at* http://www.bostonglobe.com/metro/2014/03/29/the-inside-story-mit-and-aaron-swartz/YvJZ5P6VHaPJusReuaN7SI/story.html.

20 The full name of the bill was "Aaron's Law Act of 2013 and is available at: https://www.govtrack.us/congress/bills/113/hr2454.

21 On April 21, 2015, a new version of the 2013 bill, now called "Aaron's Law Act of 2015," was introduced in the United States House and Senate by United States Representatives Lofgren and Sensenbrenner along with United States Senator Ron Wyden (D-OR). The bill was immediately referred to committee; there have been no further developments. The bill is available at https://www.govtrack.us/congress/bills/114/hr1918.

22 A copy of the proposal is available at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

IV. E.U. Trade Secrets Development

In 2015, the European Union (EU) made significant progress in its efforts to unify trade secrets law across the 28 Member States. On December 15, 2015, the European Council, represented by the Luxembourg presidency,[23] reached a provisional agreement with the European Parliament on final language for the *Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure* (the "Directive").[24] The Directive seeks to "bring legal clarity and a level playing field to all European companies . . . [and] help increase their interest in the development of research and innovation activities."[25]

Origins of the Directive

First introduced by the European Commission in November 28, 2013, the Directive was published alongside an Impact Assessment that recognized the need for the adoption of a cohesive trade secrets law in the EU:

> 86% of companies and research institutes participating in a recent survey considered trade secrets as an important tool for business and research bodies in the EU to protect their valuable information. If not protected by formal intellectual property rights (IPR; e.g. patents), such information is only relatively weakly protected by national law against misappropriation by third parties in almost all Member States; in most cases this protection is not even clearly defined.
>
> In view of trends such as globalisation, increased outsourcing and use of ICT, the threat of misappropriation of trade secrets is expected to continue to increase in the future. Particularly vulnerable to this threat are SMEs and small research institutions which often can neither afford and effectively defend formal IPR nor inform themselves about trade secrets protection nor risk defending their trade secrets in court in view of the risks and uncertainties involved under current conditions.
>
> As a result of the poor legal protection and the increased risk of misappropriation of trade secrets, businesses' competitive advantages

---

23 The European Counsel's president rotates every six months. The Luxembourg presidency ended on December 31, 2015. The current president is from Netherlands.

24 *Available at* http://data.consilium.europa.eu/doc/document/ST-15382-2015-REV-1/en/pdf.

25 "Trade secrets protection: Luxembourg presidency seals deal with Parliament", European Council (Dec. 22, 2015), http://www.consilium.europa.eu/en/press/press-releases/2015/12/15-trade-secrets-protection/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Trade+secrets+protection%3a+Luxembourg+presidency+seals+deal+with+Parliament (quoting Etienne Schneider, Deputy Prime Minister and Minister for Economic Affairs of Luxembourg).

which are based on trade secrets are at risk and incentives for cross-border innovative activities within the EU are sub-optimal (e.g. owners of trade secrets are reluctant to share trade secrets with business partners or in research projects, and even less so in a cross-border context as knowledge about the level and form of protection in other Member States is scarce and expensive to buy from, e.g., law firms).[26]

By imposing minimum rules for the protection of trade secrets through the Directive, the Commission hoped to encourage innovation and information sharing across the Member States, thereby strengthening the internal market and increasing the EU's competitiveness in the global economy.

Legislative History of the Directive

Since its introduction, the Directive has been the subject of ongoing negotiations.

In December 2013, Parliament and Council consulted with the European Economic and Social Committee (EESC) on the proposed Directive. On March 25, 2014, the EESC issued the *Opinion of the European Economic and Social Committee on the Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure*.[27] Noting that the proposal did not go far enough to reach the full scope of what should be protected as a trade secret under the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS),[28] the EESC urged the Commission to amend the

---

26 Impact Assessment at 6, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013SC0471&qid=1419251177102&from=EN.

27 *Available at* http://eescopinions.eesc.europa.eu/eescopiniondocument.aspx?language=en&docnr=8066&year=2013.

28 TRIPS, in Part II, Section 7, Article 39 (entitled "protection of undisclosed information," *available at* http://www.wto.org/english/docs_e/legal_e/27-trips_04d_e.htm), covers trade secrets. It provides as follows:

1. In the course of ensuring effective protection against unfair competition as provided in Article 10*bis* of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.

2. Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices so long as such information:

   (a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of

proposed Directive (for example, by expanding the scope of protectable information and otherwise strengthening protections) "without any further delay."

On May 26, 2014, the Council agreed on a "general approach for establishing a new legal framework for the protection of trade secrets."[29] The general approach, which set the Council common position, supported the proposed Directive with some amendments. Among other things, the Council's version allowed individual Member States to apply stricter protective measures than set forth in the Directive, extended the statute of limitations period to six years, and incorporated additional language to preserve the confidentiality of the alleged trade secret(s) during the course of litigation.

On June 16, 2015, Parliament's Committee on Legal Affairs adopted its own report.[30] Notably, the Committee's proposed text limited the statute of limitations to three years, carved out exceptions for specific activities (including "the use of information, knowledge, experience and skills honestly acquired by employees in the normal course of their previous employment"), and eliminated the possibility of designating documents containing alleged trade secrets as "Attorneys' Eyes Only" ("AEO") during the course of litigation.[31]

Negotiations with Parliament started on September 15, 2015 and continued over four meetings through December 15, 2015, culminating in the provisional agreement on the Directive. The final language "presents a compromise that goes to the limits of the flexibility of the co-legislators" and is "therefore to be considered as a package-deal that

---

information in question;

(b) has commercial value because it is secret; and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use. In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

29 *Available at* http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/142780.pdf.

30 *Available at* http://ec.europa.eu/DocsRoom/documents/14622/attachments/1/translations/en/renditions/native.

31 *Id.* at 29 ("The measures referred to . . . shall at least include the possibility: (a) to restrict access to any document containing trade secrets ***or alleged trade secrets*** submitted by the parties or third parties ***to a limited number of persons***, in whole or in part ***provided that at least one person from each of the parties*** . . . ***are given access to the document in full***") (the Committee's edits, bolded and italicized, in original).

cannot be reopened at any part without jeopardizing the whole agreement."[32] The Council's Committee of Permanent Representatives confirmed the agreement on December 18, 2015.

The Directive will now undergo a legal-linguistic review and then be submitted for confirmation through vote by Parliament.

Noteworthy Features of the Directive

The Directive sets out to cure some of the disparities in trade secrets laws among the Member States, especially as they pertain to (i) defining trade secrets and unlawful acquisition, use, and disclosure; (ii) available remedies and the calculation of damages; (iii) the treatment of good-faith third parties; (iv) the treatment of goods, documents, files or materials that incorporate unlawfully acquired or used trade secrets; and (v) the protection of trade secrets during and after the course of litigation.[33]

Accordingly, the Directive imposes standard definitions[34]:

(1) "trade secret" means information which meets all of the following requirements:

(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

(b) has commercial value because it is secret;

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

(2) "trade secret holder" means any natural or legal person lawfully controlling a trade secret;

(3) "infringer" means any natural or legal person who has unlawfully acquired, used or disclosed trade secrets;

(4) "infringing goods" means goods whose design [*in fr "conception"*], characteristics, functioning, manufacturing process or marketing

---

32 Directive at p. 3.

33 *Id.* at 8-9.

34 *Id.* at Ch. I, Art. 2.

significantly benefits from trade secrets unlawfully acquired, used or disclosed.

The Directive also defines lawful acquisition, use and disclosure,[35] unlawful acquisition, use and disclosure,[36] and carves out specific exceptions.[37]

The Directive limits the statute of limitations to not more than six years[38] and provides for the possibility of both injunctive relief (including preliminary injunctive relief) and damages.[39] Although the Directive imposes some protections for preserving the confidentiality of trade secrets during and after litigation, it adopts the position proposed by Parliament's Committee on Legal Affairs in that it does away with the AEO designation.[40]

If enacted, Member States will have two years to pass national laws in accordance with the Directive.

V. Trans-Pacific Partnership

On October 4, 2015, representatives of 12 Trans-Pacific Partnership countries (Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, United States, and Vietnam) announced the conclusion of negotiations over the largest regional trade agreement in history: the Trans-Pacific Partnership Agreement ("TPP").[41]

---

35 *Id.* at Ch. II, Art. 2a (including independent discovery or creation, reverse engineering, and other practices that conform with "honest commercial practices").

36 *Id.* at Ch. II, Art. 3 (including "[t]he production, offering or placing on the market of infringing goods, or import, export or storage of infringing goods for those purposes . . . when the person carrying out such activities knew, or should . . . have known that the trade secret was used unlawfully").

37 Directive at Ch. II, Art. 4 (providing for dismissal where the alleged acquisition, use or disclosure was carried out in the exercise of freedom of expression, including in the media, through whistleblowing activities, through collective bargaining activities, and for the purpose of protecting the public interest).

38 *Id.* at Ch. III, Sec. 1, Art. 7.

39 *Id.* at Ch. III, Sec. 2, Arts. 9 through 13. Notably, Member States must allow judiciaries to provide for preliminary injunctive relief or, alternatively, "make the continuation of the alleged unlawful use of a trade secret subject to the lodging of guarantees . . . ." *Id.* at Ch. III, Sec. 2, Art. 9.

40 *Id.* at Ch. III, Sec. 2, Art. 8 (The persons who have access to trade secrets or alleged trade secrets in litigation "shall be no greater than what is necessary in order to ensure compliance with the right to an effective remedy and to a fair trial of the parties to the proceedings and shall include,[] at least, one natural person from each party . . . .").

41 *See* https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership. The full text of TPP is available here: https://ustr.gov/trade-agreements/free-trade-agreements/trans-pacific-partnership/tpp-full-text and (for now at least) here: https://medium.com/the-trans-pacific-partnership.

Although focused on enhancing trade among Pacific Rim countries, TPP contains some potential implications for trade secrets in the United States.[42] Specifically, Article 18.78 (the only place in the entire 30-chapter, 2,000-page agreement that even touches on trade secrets[43]) addresses the protections for trade secrets that each country must have in place and provides, in full, as follows[44]:

> Article 18.78: Trade Secrets
>
> 1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention, each Party shall ensure that persons have the legal means to prevent trade secrets lawfully in their control from being disclosed to, acquired by, or used by others (including state-owned enterprises) without their consent in a manner contrary to honest commercial practices. As used in this Chapter, trade secrets encompass, at a minimum, undisclosed information as provided for in Article 39.2 of the TRIPS Agreement.
>
> 2. Subject to paragraph 3, each Party shall provide for criminal procedures and penalties for one or more of the following:
>
> (a) the unauthorised and wilful access to a trade secret held in a computer system;
>
> (b) the unauthorised and wilful misappropriation of a trade secret, including by means of a computer system; or
>
> (c) the fraudulent disclosure, or alternatively, the unauthorised and wilful disclosure, of a trade secret, including by means of a computer system.
>
> 3. With respect to the relevant acts referred to in paragraph 2, a Party may, as appropriate, limit the availability of its criminal procedures, or limit the level of penalties available, to one or more of the following cases in which:
>
> (a) the acts are for the purposes of commercial advantage or financial gain;

---

42 TPP also provides for the protection for trademarks (Articles 18.18-18.36), copyrights (Articles 18.57-18.70), and patents (Articles 18.37-56). Those protections are of far greater detail than the trade secrets section.

43 Section 18.83.4(f)(xvii) permits Vietnam to have three years to implement the required protections.

44 Words are spelled as they are in the actual section; they are not corrected to American English.

(b) the acts are related to a product or service in national or international commerce;

(c) the acts are intended to injure the owner of such trade secret;

(d) the acts are directed by or for the benefit of or in association with a foreign economic entity; or

(e) the acts are detrimental to a Party's economic interests, international relations, or national defence or national security.

Two terms from above are explained in associated footnotes. Specifically, the phrase, "'a manner contrary to honest commercial practices,' means at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties that knew, or were grossly negligent in failing to know, that those practices were involved in the acquisition." Misappropriation is defined "to be synonymous with 'unlawful acquisition'."

In addition, TPP provides general enforcement obligations related to all areas of IP (not just trade secrets). *See* Article 18.71. "TPP is the first free trade agreement to require criminal penalties for trade secret theft, including by means of a computer system."[45] Further, it "is the first trade agreement to make clear that Parties cannot exclude State-owned enterprises from IP enforcement rules, including trade secret enforcement procedures, subject to certain TRIPS Agreement disciplines."

TPP must still pass Congress.

VII. New Electronic Discovery Rules

In response to skyrocketing costs and all-consuming discovery battles, particularly in the e-discovery realm, the Federal Rules of Civil Procedure were amended, effective December 1, 2015, to promote greater efficiency in civil litigation through more "proportional" discovery.

Most significantly, the Rules have been revised as follows (underlined text has been added by the amendments, struck-through text has been eliminated):

Rule 26:

Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the

[45] https://ustr.gov/sites/default/files/TPP-Chapter-Summary-Intellectual-Property.pdf.

needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable. ~~— including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).~~

Rule 37(e):

Failure to ~~Provide~~ Preserve Electronically Stored Information. ~~Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system~~. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:

(1) upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or

(2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:

(A) presume that the lost information was unfavorable to the party;

(B) instruct the jury that it may or must presume the information was unfavorable to the party; or

(C) dismiss the action or enter a default judgment.

The amended rules reflect the ever-expanding role of discovery, and e-discovery, in particular, in driving up the costs civil of litigation and the consequent need to shepherd voluminous amounts of information through the discovery process in a manner that is proportional to the value of the case and the sophistication of the parties, among other things. Watch for the federal courts to begin construing the meaning of these amendments, particularly in the context of trade secrets litigation, where documents exchanged in discovery often run into hundreds of thousands and discovery costs can often dwarf the value of the actual controversy.

VII. Forum Selection

Trade secrets litigation often involves interstate disputes. Sometimes there is a related contract between or among the parties that includes a forum selection clause and sometimes there is not. And, oftentimes, even when there is a contract with such a provision, there is a question about its enforceability.

In 2013, the Supreme Court issued the decision, *Atlantic Marine Construction Company, Inc. v. United States District Court for the Western District of Texas*, 134 S.Ct. 568 (2013), which, although not involving trade secrets, set the stage for greater enforcement of forum selection clauses. Since the *Atlantic Marine* decision, a substantial number of cases have applied its tenets to noncompetition agreements (contracts used to protect, among other things, trade secrets).

Atlantic Marine Construction Company, Inc.
***v. United States District Court for the Western District of Texas*,**
134 S.Ct. 568 (2013)

Although a case involving a contractor's alleged failure to pay its subcontractor may appear at first blush to be irrelevant to trade secrets litigation, *Atlantic Marine Construction Company, Inc. v. United States District Court for the Western District of Texas*, 134 S.Ct. 568 (2013), is in fact quite significant.

The case came to the Supreme Court as follows:

> Petitioner Atlantic Marine Construction Co., a Virginia corporation, entered into a subcontract with respondent J–Crew Management, Inc., a Texas corporation, for work on a construction project. The subcontract included a forum-selection clause, which stated that all disputes between the parties would be litigated in Virginia. When a dispute arose, however, J–Crew filed suit in the Western District of Texas. Atlantic Marine moved to dismiss, arguing that the forum-selection clause rendered venue "wrong" under 28 U.S.C. § 1406(a) and "improper" under Federal Rule of Civil Procedure 12(b)(3). In the alternative, Atlantic Marine moved to transfer the case to the Eastern District of Virginia under 28 U.S.C. § 1404(a). The District Court denied both motions.

Id. at 573 (internal citations omitted). The Fifth Circuit agreed. *Id.*

The Supreme Court identified and answered the issue as follows:

> The question in this case concerns the procedure that is available for a defendant in a civil case who seeks to enforce a forum-selection clause. We reject petitioner's argument that such a clause may be enforced by a motion to dismiss under 28 U.S.C. § 1406(a) or Rule

> 12(b)(3) of the Federal Rules of Civil Procedure. Instead, a forum-selection clause may be enforced by a motion to transfer under § 1404(a) (2006 ed., Supp. V), which provides that "[f]or the convenience of parties and witnesses, in the interest of justice, a district court may transfer any civil action to any other district or division where it might have been brought or to any district or division to which all parties have consented." When a defendant files such a motion, we conclude, a district court should transfer the case unless extraordinary circumstances unrelated to the convenience of the parties clearly disfavor a transfer. In the present case, both the District Court and the Court of Appeals misunderstood the standards to be applied in adjudicating a § 1404(a) motion in a case involving a forum-selection clause, and we therefore reverse the decision below.

Id. at 575.

First, the Supreme Court explained, "Section 1406(a) and Rule 12(b)(3) allow dismissal only when venue is 'wrong' or 'improper.' Whether venue is 'wrong' or 'improper' depends exclusively on whether the court in which the case was brought satisfies the requirements of federal venue laws, and those provisions say nothing about a forum-selection clause." *Id.* at 577.

Citing to 28 U.S.C. § 1391(b), the Court then explained that venue is "proper" if venue is brought in any of the following three districts:

> (1) a judicial district in which any defendant resides, if all defendants are residents of the State in which the district is located; (2) a judicial district in which a substantial part of the events or omissions giving rise to the claim occurred, or a substantial part of property that is the subject of the action is situated; or (3) if there is no district in which an action may otherwise be brought as provided in this section, any judicial district in which any defendant is subject to the court's personal jurisdiction with respect to such action."

Id. at 577.

The Court then went on to explain the proper method for addressing a forum selection clause, fundamentally altering the way in which many federal district courts had been used to analyzing the issue. Specifically, the Court stated,

> Although a forum-selection clause does not render venue in a court "wrong" or "improper" within the meaning of § 1406(a) or Rule 12(b)(3), the clause may be enforced through a motion to transfer under § 1404(a). That provision states that "[f]or the convenience of parties and witnesses, in the interest of justice, a district court may transfer any civil action to any other district or division where it might

have been brought or to any district or division to which all parties have consented." Unlike § 1406(a), § 1404(a) does not condition transfer on the initial forum's being "wrong." And it permits transfer to any district where venue is also proper (*i.e.*, "where [the case] might have been brought") or to any other district to which the parties have agreed by contract or stipulation.

Section 1404(a) therefore provides a mechanism for enforcement of forum-selection clauses that point to a particular federal district. And . . . a proper application of § 1404(a) requires that a forum-selection clause be "given controlling weight in all but the most exceptional cases."

Id. at 579. The Court also noted that "the appropriate way to enforce a forum-selection clause pointing to a state or foreign forum is through the doctrine of *forum non conveniens*." *Id*. at 580. As the Court explained, "Section 1404(a) is merely a codification of the doctrine of *forum non conveniens* for the subset of cases in which the transferee forum is within the federal court system; in such cases, Congress has replaced the traditional remedy of outright dismissal with transfer." *Id*.

The Court then explained the application of § 1404(a) as follows:

When the parties have agreed to a valid forum-selection clause, a district court should ordinarily transfer the case to the forum specified in that clause. Only under extraordinary circumstances unrelated to the convenience of the parties should a § 1404(a) motion be denied. . . .

In the typical case not involving a forum-selection clause, a district court considering a § 1404(a) motion (or a *forum non conveniens motion*) must evaluate both the convenience of the parties and various public-interest considerations. Ordinarily, the district court would weigh the relevant factors and decide whether, on balance, a transfer would serve "the convenience of parties and witnesses" and otherwise promote "the interest of justice." § 1404(a).

The calculus changes, however, when the parties' contract contains a valid forum-selection clause, which "represents the parties' agreement as to the most proper forum." The "enforcement of valid forum-selection clauses, bargained for by the parties, protects their legitimate expectations and furthers vital interests of the justice system." For that reason, and because the overarching consideration under § 1404(a) is whether a transfer would promote "the interest of justice," "a valid forum-selection clause [should be] given controlling weight in all but the most exceptional cases." The presence of a valid

forum-selection clause requires district courts to adjust their usual § 1404(a) analysis in three ways.

First, the plaintiff's choice of forum merits no weight. Rather, as the party defying the forum-selection clause, the plaintiff bears the burden of establishing that transfer to the forum for which the parties bargained is unwarranted. Because plaintiffs are ordinarily allowed to select whatever forum they consider most advantageous (consistent with jurisdictional and venue limitations), we have termed their selection the "plaintiff's venue privilege." But when a plaintiff agrees by contract to bring suit only in a specified forum—presumably in exchange for other binding promises by the defendant—the plaintiff has effectively exercised its "venue privilege" before a dispute arises. Only that initial choice deserves deference, and the plaintiff must bear the burden of showing why the court should not transfer the case to the forum to which the parties agreed.

Second, a court evaluating a defendant's § 1404(a) motion to transfer based on a forum-selection clause should not consider arguments about the parties' private interests. When parties agree to a forum-selection clause, they waive the right to challenge the preselected forum as inconvenient or less convenient for themselves or their witnesses, or for their pursuit of the litigation. A court accordingly must deem the private-interest factors to weigh entirely in favor of the preselected forum. As we have explained in a different but "instructive" context, "[w]hatever 'inconvenience' [the parties] would suffer by being forced to litigate in the contractual forum as [they] agreed to do was clearly foreseeable at the time of contracting."

As a consequence, a district court may consider arguments about public-interest factors only. *See* n. 6, supra [reproduced infra, n.14]. Because those factors will rarely defeat a transfer motion, the practical result is that forum-selection clauses should control except in unusual cases. Although it is "conceivable in a particular case" that the district court "would refuse to transfer a case notwithstanding the counterweight of a forum-selection clause," such cases will not be common.

Third, when a party bound by a forum-selection clause flouts its contractual obligation and files suit in a different forum, a § 1404(a) transfer of venue will not carry with it the original venue's choice-of-law rules—a factor that in some circumstances may affect public-interest considerations. A federal court sitting in diversity ordinarily must follow the choice-of-law rules of the State in which it sits. However, we previously identified an exception to that principle for § 1404(a) transfers, requiring that the state law applicable in the

> original court also apply in the transferee court. We deemed that exception necessary to prevent "defendants, properly subjected to suit in the transferor State," from "invok[ing] § 1404(a) to gain the benefits of the laws of another jurisdiction...."
>
> When parties have contracted in advance to litigate disputes in a particular forum, courts should not unnecessarily disrupt the parties' settled expectations. A forum-selection clause, after all, may have figured centrally in the parties' negotiations and may have affected how they set monetary and other contractual terms; it may, in fact, have been a critical factor in their agreement to do business together in the first place. In all but the most unusual cases, therefore, "the interest of justice" is served by holding parties to their bargain.

Id. at 581-83 (citations and footnotes omitted).[46]

Application of Atlantic Marine to the Protection of Trade Secrets

Since 2013, we have begun to see the impact of *Atlantic Marine* on cases involving the attempted enforcement of forum selection clauses in noncompetition agreements arising from an employer-employee relationship.

For example, in *Marcotte v. Micros Systems, Inc.*, 2014 WL 4477349 (N.D. Cal. Sept. 11, 2014), the Northern District of California (San Francisco division) enforced a forum selection clause in an employment agreement containing a noncompetition agreement. *Id*. at *8. There, the plaintiff, Dianne Marcotte, filed the action in the California state courts in violation of the agreement's forum selection clause providing for the exclusive jurisdiction in courts in Maryland. *Id.* at *1. The defendant Micros Systems, Inc. removed to federal court and moved to dismiss or to transfer to the District of Maryland, the contractually-selected forum. *Id*.

Before commencing its analysis, the court observed, "While the case might have been brought in the District of Maryland, the remaining factors all favor litigating the case

---

[46] Factors relating to the parties' private interests include "relative ease of access to sources of proof; availability of compulsory process for attendance of unwilling, and the cost of obtaining attendance of willing, witnesses; possibility of view of premises, if view would be appropriate to the action; and all other practical problems that make trial of a case easy, expeditious and inexpensive." *Piper Aircraft Co. v. Reyno*, 454 U.S. 235, 241, n. 6, 102 S.Ct. 252, 70 L.Ed.2d 419 (1981) (internal quotation marks omitted). Public-interest factors may include "the administrative difficulties flowing from court congestion; the local interest in having localized controversies decided at home; [and] the interest in having the trial of a diversity case in a forum that is at home with the law." *Ibid*. (internal quotation marks omitted). The Court must also give some weight to the plaintiffs' choice of forum. *See Norwood v. Kirkpatrick*, 349 U.S. 29, 32, 75 S.Ct. 544, 99 L.Ed. 789 (1955).

Id. at 581 n.6.

here: Ms. Marcotte's employment here, the execution of the contracts here, the parties' respective contacts with the forum, access to witnesses and evidence, the convenience of the parties and witnesses, administrative efficiencies, and Ms. Marcotte's choice of forum." *Id*. at *6.

Next, the court summarized the applicable standard as follows:

> A valid forum selection clause trumps this outcome. Courts ordinarily transfer venue to the contractually-designated forum unless the plaintiff shows "extraordinary circumstances unrelated to the convenience of the parties" to overcome the "controlling weight" given to the forum selection clause. *See Atlantic Marine,* 134 S.Ct. at 580. Put another way, "[a] proper application of § 1404(a) requires that a forum selection clause be given controlling weight in all but the most exceptional cases." *Id.* at 579 (quotation and citation omitted).

Id. The court then explained that, when there is a valid forum selection clause, "a plaintiff's choice of forum is no longer given any weight," "the parties' private interests . . . no longer factor into the court's inquiry," and "the court can still consider 'public interest' factors . . . ." *Id*. As to the consideration of the public interest factors, however, the court quoted *Atlantic Marine*: "But those interests will 'rarely defeat' the transfer motion because 'in all but the most unusual cases, 'the interest of justice' will be served by holding parties to their bargain." *Id*.

Not surprisingly, Marcotte contended, among other things, that the forum selection clause was unenforceable in that it was "an attempt to evade a strong policy of the forum here: California law that holds that covenants not to compete are unenforceable as contrary to public policy. This, of course, is likely one reason for the choice of law provision: in contrast to California, 'the federal or state courts in Maryland would permit and enforce the non- compete agreements in the Sales Plan.'" *Id*. at *8 (citations omitted).

The court rejected the plaintiff's conflation of choice of law and choice of forum as follows:

> The problem with this argument is that the choice of law issues are the same for a district court in Maryland or California: both courts, sitting in diversity, consider which law (California or Maryland) to apply to the claims. *See Google, Inc. v. Microsoft Corp.,* 415 F.Supp.2d 1018, 1022 (N.D.Cal.2005). "A forum selection clause determines where the case will be heard; it is separate and distinct from choice of law provisions that are not before the court." *Besag v. Custom Decorators, Inc.,* No. C 08–05463 JSW, 2009 WL 330934, at *3–4 (N.D.Cal. Feb. 10, 2009) (called into question on other grounds by *Narayan v. EGL, Inc.,* 616 F.3d 895, 899, 904 (9th Cir. 2010)). "Thus, a party challenging enforcement of a forum selection clause may not base its challenge on choice of law analysis." *Id.* at *4 (enforcing a forum

> selection clause in an employment agreement and characterizing as speculative the employee's argument that Oregon court would apply Oregon substantive law in a manner that would foreclose certain remedies). In sum, enforcing the forum selection clause is different than choice-of-law issues.

Id.

The court concluded, "Ms. Marcotte does not establish that having her case heard in Maryland contravenes a strong public policy of California." *Id.* The court's reasoning bares particular note:

> Enforcing the venue clause, and locating the forum in Maryland, do not require the application of Maryland law to the claims.
>
> While a federal court sitting in diversity ordinarily applies the choice-of-law rules of the forum, the Plan Agreement's choice of law provision excepts Maryland's conflict of law rules. The briefs did not address the import of this. The court asked Micros's counsel exactly what this meant. For example, did it mean that the Maryland court would apply no choice of law provision and had to apply Maryland law, period end of story? This matters because (as the parties agree) California public policy disfavors non-compete agreements. California also "has a strong interest in protecting its employees from noncompetition under section 16600." *Advanced Bionics v. Medtronic, Inc.,* 29 Cal.4th 697, 706– 07 (2002). By contrast, Maryland law and courts apparently allow and enforce covenants not to compete.
>
> At the hearing, Micros's counsel said that—regardless of the exception in paragraph 8—the Maryland forum court would apply its own conflicts laws, which counsel characterized as similar to California's laws [in that it] applie[s] the Restatement (Second) of Conflicts of Laws in evaluating whether it should apply [the relevant state's] law despite the parties' contractual agreement to apply Maryland law to their disputes. California also applies the Restatement (Second) of Conflicts of Law to determine whether choice-of-law provisions are valid.
>
> Given this context, . . . the court concludes that Ms. Marcotte has not carried the "heavy burden" of establishing that the forum selection clause is unenforceable.

Id. at *8-9[47] (some citations omitted).

---

[47] The court ultimately denied the motion without prejudice, as additional briefing was necessary to address a waiver argument. *Id*. 12.

Similar results have been reached in other cases. *See Meyer v. Howmedica Osteonics Corp.*, 2015 WL 728631, at **10-11 (S.D. Cal. Feb. 19, 2015) (rejecting plaintiffs' argument that enforcing the forum selection (New Jersey) and choice-of-law clause (New Jersey) would contravene California public policy); *Edwards v. Depuy Synthes Sales, Inc.*, 2014 WL 2194798, at **2-3 (N.D. Cal. May 22, 2014) (enforcing forum selection clause and transferring the case to Pennsylvania); *United American Healthcare Corp. v. Backs*, 997 F. Supp.2d 741, 749-51 (E.D. Mich. 2014) (differentiating between motions to transfer *to* the agreed-upon forum and *from* the agreed-upon forum, the court nevertheless applied *Atlantic Marine*, looked only at public interest factors, and enforced the forum selection clause).

Edwards v. Depuy Synthes Sales is particularly interesting. In that case, Edwards filed a declaratory judgment action in California (in violation of a forum selection clause mandating Pennsylvania as the forum) to declare that the parties' agreement, in particular the incorporated noncompete, was invalid and unenforceable. *Id.* at *1. A week later Depuy commenced an action in Pennsylvania seeking a preliminary injunction. *Id.* Edwards moved to dismiss or transfer the Pennsylvania action, after which Depuy moved to dismiss or transfer the California action. *Id.* The Pennsylvania court ruled first, and refused to dismiss or transfer the case. *Id.* Recognizing the judicial inefficiencies of dual proceedings, the California court then (somewhat surprisingly) analyzed the other "private" interests typically examined prior to the *Atlantic Marine* decision. *Id*. at *2. Given (1) that no facts were in dispute in the California action (according to Edwards) and therefore no need to consider the location of evidence or witnesses (indeed, none were even identified by Edwards) and (2) that Edwards' new lawyer was paying the costs of the litigation, the court concluded that "the interests of justice and convenience factors both weigh in favor of transferring th[e] case to . . . Pennsylvania." *Id.* at *3.

In contrast, in *Sirius Computer Solutions, Inc. v. Sparks*, Cv., 2015 WL5821840 (W.D. Tex. Oct. 5, 2015), defendant, a former employee of plaintiff subject to a non-solicitation agreement, sought to change venue from the contractually-specified venue, Texas, to Oregon, where Defendant and his new employer had filed a declaratory judgment action against Plaintiff. The court, applying *Atlantic Marine*, engaged in a detailed analysis of the public interest factors. *Id.* at **7-10. In particular, the court rejected defendant's argument that the "localized interest" factor weighed in favor of Oregon because a number of customers and employees that Defendant is alleged to have solicited live in the Pacific Northwest. *Id.* at *8. The court likened that argument to a private interests argument, which was expressly barred under *Atlantic Marine*. *Id.* The court also found that the familiarity of the forum with the local law to be applied weighed in favor of staying in Texas. *Id.* at **8-9. Even after acknowledging that this factor only comes into play if the governing law is "exceptionally arcane," (quoting *Atlantic Marine*), the court went ahead and did a choice-of-law analysis and concluded that Texas law applies under Texas choice-of-law rules. *Id.* at **8-9. Based upon its analysis, the court denied Defendant's motion for change of venue.

One recent case brought an international dimension to trade secret cases involving forum selection clauses. In *EMC Corporation v. Petter*, 104 F. Supp. 3d 127 (D. Mass. 2015), EMC sued its former employee, a resident of the United Kingdom, in Massachusetts federal court alleging that the former employee colluded with his new employer to misappropriate confidential EMC information and trade secrets. *Id.* at 130. On the basis of such "detrimental" activities, EMC sought rescission of certain vested stock units under a stock plan, which contained a forum selection and choice-of-law clause specifying Massachusetts federal and state courts and Massachusetts law. *Id.* Defendant sought dismissal, or, in the alternative, a stay of proceedings in favor of the case he filed in the U.K. two weeks after EMC sued him. *Id.* at 131. Citing *Atlantic Marine*, the court noted that because of the stock plan's forum selection clause, the court would give no weight to the defendant's private interests arguments. *Id.* at 134-135. The court then stated that the public interests factors favored keeping the case in Massachusetts because the dispute concerned stock in a Massachusetts corporation granted by a contract that invokes the protections of Massachusetts courts. Id. at 134-135. The court denied the defendant's motion.

One issue that has repeatedly come up in recent cases is whether the claims asserted tied back to the contract that contains the forum selection provision. For example, in *Auld v. Daugherty Systems, Inc.,* 2015 WL 5970731 (D. Minn. Oct. 13, 2015), the court granted defendant's motion to transfer venue based upon a forum selection clause contained in the employee agreement signed by plaintiff. Plaintiff alleged that defendant, his former employer, breached a severance agreement and retaliated against him for whistleblowing activity. *Id.* at *1. Defendant countersued claiming breach of the confidentiality provision of the employee agreement and misappropriation of trade secrets. *Id.* Plaintiff tried to get out of the forum selection clause and the dictates of *Atlantic Marine* by arguing that his tort and contract claims related to the alleged severance agreement and not the employee agreement. *Id.* at *2. The court disagreed finding that his claims directly related to the employee agreement and its status. *Id.* With respect to the whistleblower claim, that was "inextricably intertwined" with the core issue of whether the alleged promises relating to severance were enforceable. *Id.* Finally, the court found that the plaintiff had met his burden of showing that the public interest factors militated against transfer, noting, *inter alia*, that the transferee court could apply Minnesota's whistleblower act. *Id.* at **2-3. *See also, Medalogix, LLC v. Alacare Health Services Inc.,* 2015 WL 6158026, **3-5 (M.D. Tenn. Oct. 20, 2015) (rejecting defendant's contention that plaintiff's claims – seeking a declaration that the information at issue did not constitute trade secrets and that plaintiff had not misappropriated any such information – did not relate back to the business associate agreement containing the forum selection clause).[48]

---

[48] In contrast, in *Telesocial, Inc. v. Orange S.A.*, 2015 WL 1927697 (N.D. Cal. Apr. 28, 2015), the court found that the applicable forum selection clause, specifying the courts of Paris, France, did not apply to plaintiff's CFAA , trade secret, and breach of contract claims against defendant. *Id.* at **2-3. The parties had entered into a non-disclosure agreement (NDA) to protect confidential information during business negotiations. *Id.* at *1. The NDA contained a forum selection clause covering any dispute "arising out of or relating to" the NDA and provide that such disputes were to be heard in the "Court of Paris." *Id.* The court rejected defendant's contention that plaintiff's claims tied back to the NDA, noting that the thrust of the complaint is that

As these cases demonstrate, courts are facing increased motion practice, and ever more creative oppositions thereto, based upon *Atlantic Marine*. That trend is likely to continue as parties seeking transfer continue to rely upon *Atlantic Marine*.

VIII. Other Noteworthy State and Federal Developments

In the absence of a federal private right of action, the protection of trade secrets is largely left to state law.[49] The two most important areas are specific trade secrets laws and laws concerning the enforceability of noncompetition agreements (and nondisclosure agreements). While the laws tend to be similar in most states, there are nevertheless significant differences among the states.[50] Developments in a number states are noteworthy. In addition, several related federal developments not addressed above are nevertheless worth of mention. They are all discussed in turn below.

Massachusetts

Massachusetts continued to be active in 2015 in its efforts to pursue adoption of its own version of the Uniform Trade Secrets Act ("UTSA") and noncompete reform. The bills relating to trade secrets propose adoption of the UTSA with varying degrees of modifications, while the bills relating to noncompetition agreements would ban the use of employee non-compete agreements within Massachusetts. The bills are discussed in turn below.

House Bill H.1408, tracking language from bills submitted in prior sessions based on a bill filed by the Uniform Law Commissioners, proposes adopting the Uniform Trade Secret Act with certain changes. In particular, if passed, H.1408 would require, inter alia, that a party alleging a breach must describe the trade secret in question "with sufficient particularity" as to allow the respondent to prepare a defense. If passed, the bill would substantially weaken Massachusetts trade secrets law in three respects: (1) it would protect only trade secret owners (not others with rights in the secrets); (2) it would require the trade secret owner protect the secrecy of information, even if the information had been made public by the misappropriator; and (3) it would potentially raise the

---

defendant hacked into plaintiff's servers after negotiations had ended. *Id.* at *3. Further, the breach of contract claim arose out of alleged breaches of plaintiff's "Terms of Use" document that governed use of plaintiff's web application. *Id.*

49 While the Computer Fraud and Abuse Act is frequently a tool for the protection of trade secrets, that statute is not specifically directed to the protection of trade secrets (but rather the protection of electronically-stored information – regardless of its status as a trade secret – obtained or impaired through computer hacking or other computer-related conduct) and, as demonstrated above, is, in any event, the subject of substantial confusion and conflicting judicial interpretations.

50 For a summary of noncompete laws around the country, see "Employee Noncompetes, A State by State Survey," available at http://www.beckreedriden.com/50-state-noncompete-survey/.

pleading standards to require greater specificity of the trade secrets in order to commence the action.

As a result of criticism of those aspects of the bill, Steven Chow, on behalf of the Massachusetts Board of Commissioners on Uniform State Laws, revised their prior-years' bill and submitted H.32 addressing those concerns.[51] H.32 is otherwise substantially the same as H.1408. Accordingly, if adopted, H.32 will fill in the gaps in H.1408 and bring Massachusetts in as the 49th state to adopt some version of the UTSA.[52]

H.1195 would also incorporate the Uniform Trade Secrets Act, but would add a provision banning the use of non-compete agreements. Similar to H.1195, S.169 would incorporate the Uniform Trade Secrets Act and ban the use of non-compete agreements, but would contain exemptions for certain types of non-compete agreements (when the sale of the business is involved, for example). S169 (S334) would specifically note that it has no effect on non-disclosure agreements.

H.1701, H.1719, H.1761, and S.957 would implement a ban on employee non-compete agreements. Although H.1701 and S.957 differ in language from H.1719 and H.1761 (which are similar in structure and language to proposed legislation in the other states proposing bans), all of the bills permit non-compete agreements where the sale of the business is involved. However, H.1719 and H.1761 expressly exclude nondisclosure agreements from their reach, but do not mention nonsolicitation agreements. H.1701 and S.957, in contrast, specifically note that they do not affect nondisclosure covenants or non-solicitation covenants. H.1701 also expressly permits a court to impose what has been called a "springing noncompete," *i.e.*, a noncompete as a remedy for a violation or breach of another contractual obligation or violation of a statutory or common law.

Alabama

The Alabama legislature recently passed House Bill 352, which updated its law concerning noncompetes effective as of January 1, 2016. The new law retains the existing general ban on contracts in restraint of trade, but enumerates six exceptions for the protection of recognized protectable interests (*i.e.*, trade secrets, confidential information, customer, patient, vendor, or client lists, and specialized or unique training); most relevant among the exceptions are covenants not to compete within a geographic area. The new law also establishes a presumption that a two-year noncompete is reasonable. Finally, the law

---

51 More information about these concerns is available at "Massachusetts Noncompete Ban and Modified Version of the Uniform Trade Secrets Act Reported Out of Committee," http://faircompetitionlaw.com/2014/04/30/massachusetts-noncompete-ban-and-modified-version-of-the-uniform-trade-secrets-act-reported-out-of-committee/.

52 There is an ongoing debate about whether South Carolina has adopted the UTSA. While South Carolina did not purport to adopt it, the language of its trade secrets statute is, in many respects, substantially the same as the UTSA. Accordingly, for all practical purposes, South Carolina's statute is effectively another version of the UTSA.

also continues to allow for (mandatory) judicial reformation of unenforceably broad noncompete agreements.[53]

Arkansas

Arkansas noncompete law was statutorily modified by the addition of Ark. Code 4-70-207.[54] Under the new law, noncompetes in Arkansas must be limited with respect to time and scope in a manner that is not greater than necessary to defend the protectable business interest of the employer (see below). The lack of a geographic limit does not render the agreement unenforceable, provided that the time and scope limits appropriately limit the restriction. Factors to consider include the nature of the employer's business interest; the geographic scope, including whether a geographic limit is feasible; whether the restriction is limited to specific group of customers or others; and the nature of the employer's business. In addition, a two-year restriction is presumptively reasonable unless clearly demonstrated otherwise.

Legitimate business interests that may be protected include trade secrets; intellectual property; customer lists; goodwill with customers; knowledge of business practices; methods; profit margins; costs; other confidential information (that is confidential, proprietary, and increases in value from not being known by a competitor); training and education; other valuable employer data (if provided to employee and an employer would reasonably seek to protect or safeguard from a competitor in the interest of fairness).

Hawaii

In July of 2015, a new law (H.B. No. 1090) banning noncompete agreements in Hawaii took effect. The law is targeted specifically to prevent technology workers being driven out of Hawaii and to prevent employers within Hawaii from having to recruit workers from other states. The law notes that because "the geographic nature of Hawaii is unique and limited, noncompete agreements unduly restrict future employment opportunities for technology workers and have a chilling effect on the creation of new technology businesses within the State."

H.B. 1090 applies only to workers in technology businesses. The language of the bill provides that "it shall be prohibited to include a noncompete clause or a nonsolicit clause in any employment contract relating to an employee of a technology business." The bill further defines "technology business" as a business deriving the majority of its sales from software or information technology development.

---

53 *See* www.al.com/business/index.ssf/2015/06/alabamas_new_and_improved_non-.html.

54 http://www.arkleg.state.ar.us/assembly/2015/2015R/Acts/Act921.pdf.

Other States

As of July 1, 2015, New Mexico banned noncompetition agreements for dentists, physicians, podiatrists, osteopathic physicians, and certified registered nurses. However, the ban does not apply to any covered medical professional if they are a shareholder, owner, partner, or director of a health care practice.

Effective January 1, 2016, Oregon amended its noncompete law to limit the duration of noncompetes from two years to eighteen months.

In addition, Michigan, Pennsylvania, and Washington have bills pending to ban the use of noncompetes altogether. (Washington has two other bills as well, one that, among other things, would ban the use of noncompetes for low-income employees and persons involuntarily terminated without cause and one that would ban the use of noncompetes for physicians).

New York, in contrast, has a bill designed to "clarify" its existing law and Wisconsin has a bill that would make it easier to enforce noncompetes, including by adding presumptions of what is and is not a reasonable duration and by permitting the courts to modify overly broad restrictions (as opposed to having to invalidate them in their entirety).

Federal Developments: Confidentiality Agreements

On April 1, 2015 (and, no, it was not an April Fool's Day joke), the SEC issued the first cease and desist order against a company finding that the company's confidentiality statement (a confidentiality requirement imposed in connection with internal investigations) interfered with Rule 21F-17 ("Staff communications with individuals reporting possible securities law violations") promulgated by the SEC as of August 12, 2011, in accordance with the Dodd-Frank Wall Street Reform and Consumer Protection Act. *See In the Matter of KBR, Inc.*, Administrative Proceeding File No. 3-16466.[55]

Rule 21F-17 provides in relevant part as follows:

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

The confidentiality statement at issue provided as follows:

> I understand that in order to protect the integrity of this review, I am prohibited from discussing any particulars regarding this interview and the subject matter discussed during the interview,

[55] http://www.sec.gov/litigation/admin/2015/34-74619.pdf.

> without the prior authorization of the Law Department. I understand that the unauthorized disclosure of information may be grounds for disciplinary action up to and including termination of employment.

Although there were no known instances in which the confidentiality statement had any impact with respect to whistleblower activities, the SEC concluded that "This language undermines the purpose of Section 21F and Rule 21F-17(a), which is to 'encourage[e] individuals to report to the Commission.'" As a consequence, the SEC imposed a $130,000 fine against KBR and required KBR to provide a copy of the Order and certain additional information to all US employees who signed the agreement since the adoption of the rule. In addition, KBR amended its confidentiality statement to state as follows:

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

The SEC has made focusing on confidentiality agreements a priority. Accordingly, expect in 2016 to see see additional enforcement actions, as well as preemptive modifications of public company (and potentially private company) confidentiality agreements.

Federal Developments: Noncompetition Agreements

Noncompete law is generally a creature of state regulation. As such, it should come as no surprise that we have 50 variations (really 51, when you factor in DC – albeit 3 states (California, Oklahoma, and North Dakota) prohibit employee noncompetes altogether, so it's more like 48 variations).[56] Nevertheless, we may be on the verge of a 51st variation (or 49th, if you're keeping accurate count).

Specifically, on June 4, 2015, several U.S. senators – Al Franken (D-MN) and Chris Murphy (D-CT), with cosponsors Elizabeth Warren (D-MA) and Richard Blumenthal (D-CT) – filed proposed legislation to limit the use of noncompetes for low-wage employees. Entitled the "Mobility and Opportunity for Vulnerable Employees Act" (or the "MOVE Act"), the bill would prohibit the use of covenants not to compete (defined in the bill) for "low-wage employees," *i.e.*, employees earning the greater of (subject to inflation) $15 per hour or the applicable state or local minimum wage rate or $31,200 per year, but excluding any

---

[56] *See* http://www.beckreedriden.com/50-state-noncompete-survey/.

salaried employee earning (subject to inflation) more than $5,000/month for 2 consecutive months.[57] (It also requires notice of the Act in a conspicuous place in the workplace and is clear that it applies only to agreements entered after the enactment of the Act.)

Thresholds, notice, and timing requirements aside, the bill is somewhat unclear on its scope. Specifically, it is unclear whether it applies only to true noncompetes (*i.e.*, agreements that restrict someone from working for a particular category of employer, in a particular role, in a particular area, for a particular period) or to all restrictive covenants (including nonsolicitation agreements, no-poach/no-raid agreements, nondisclosure agreements, etc.)

In this regard, the language (in section 2(2) of the Bill) defining a covenant not to compete states as follows:

> [A]n agreement (A) between an employee and employer that restricts such employee from performing
>
> (i) any work for another employer for a specified period of time;
>
> (ii) any work in a specified geographical area; or
>
> (iii) work for another employer that is similar to such employee's work for the employer included as a party to the agreement . . . ."

So, for example, is a restriction on the employee soliciting (or providing services to) certain customers a restriction on the employee "from performing . . . any work for another employer" or (perhaps less likely) "from performing . . . work . . . that is similar to such employee's work for the [prior] employer"? The answer is, at this time, unclear.

Under the bill, the Secretary of Labor is charged with enforcement of the Act and may impose civil fines up to $5,000 for each noncompete violation for each affected employee and $5,000 for failure to post the appropriate notice.

The bill was referred to the Committee on Health, Education, Labor, and Pensions on December 15, 2015.

Not to be outdone, on June 24, 2015, United States Representatives Joe Crowley (D-NY), Linda Sánchez (D-CA), Keith Ellson (D-MN), and Mark Pocan (D-WI), filed their own version of the MOVE Act, entitled the "Limiting the Ability to Demand Detrimental Employment Restrictions Act" (the "LADDER Act"). The LADDER Act is virtually identical to the MOVE Act, just broadening somewhat the definition of the employees that are considered low-wage employees and tweaking the inflation adjustment language. The

---

[57] A full copy of the text of the bill is available here: http://www.franken.senate.gov/files/documents/150604MOVEsummary.pdf.

LADDER Act was referred to the House Education and the Workforce Committee on December 15, 2015.

That same day (December 15, 2015), Congressman Derek Kilmer introduced the Freedom for Workers to Seek Opportunity Act ("FWSOA").[58] Although not having quite as catchy an acronym as the MOVE Act or the LADDER Act, FWSOA does win on creativity in that it seeks to ban the use of noncompetes for grocery store workers (only). Specifically, the bill provides:

> No employer shall enter into a covenant not to compete with any grocery store employee of such employer, who in any workweek is engaged in commerce or in the production of goods for commerce (or is employed in an enterprise engaged in commerce or in the production of goods for commerce).
>
> The bill, if passed, would be enforced by the Secretary of Labor.

[58] https://www.govtrack.us/congress/bills/114/hr4254/text.