NYSBA FALL 2016 | VOL. 21 | NO. 2

NYLitigator

A Journal of the Commercial & Federal Litigation Section
of the New York State Bar Association

Inside

NYSBA

A New York Litigator's Guide to the New Federal Trade Secret Law

By Heath J. Szymczak and Bradley A. Hoppe

I. Introduction

On May 11, 2016, President Barack Obama signed into law the Defend Trade Secrets Act of 2016 ("DTSA"), creating the first federal civil claim for theft of trade secrets. This is one of the most significant developments in trade secret law in decades. Prior to DTSA, trade secrets did not receive the same protections afforded to other forms of intellectual property such as trademarks, copyrights, and patents. DTSA elevates the status of trade secrets to the point where its remedies, in many instances, now exceed those which may have been previously available under state law, including aggressive ex parte seizure mechanisms (similar to those used to seize counterfeit goods under trademark law), exemplary damages, and attorney's fees.

Trade secret misappropriation was previously governed by state law, with almost all other states adopting various versions of the Uniform Trade Secrets Act ("UTSA").[1] New York is one of the last states that have refused to adopt UTSA. The passage of DTSA thus has significant implications for a commercial litigator in New York, as he/she, for the first time, will have available to him/her a statutory framework for enforcement of trade secrets.[2]

DTSA is a civil amendment to the Economic Espionage Act of 1996 ("EEA"), a criminal statute.[3] The EEA makes it a federal criminal offense to misappropriate a trade secret that is linked to interstate or foreign commerce. The EEA, however, did not provide for a private right of action in federal court. Instead, trade secret owners seeking protection under the EEA had to stand in line and hope for investigation and prosecution by an already overextended Federal Bureau of Investigation and Department of Justice. Consequently, prosecutions under the EEA have been limited and have not provided an effective deterrent to trade secret theft.[4] By providing trade secret owners with direct access to federal courts through a mechanism to vindicate private rights, together with robust remedial provisions, DTSA is designed to create a greater deterrent to trade secret theft than previously existed at the federal level.

The purpose of this article is to provide New York commercial litigators, who may be unfamiliar with UTSA and the EEA, with an understanding of the background and context from which DTSA evolved, as well as a clearer picture of the scope of DTSA generally and how federal courts are likely to construe its provisions specifically. The reader will gain an understating of why DTSA was enacted and how it is different from and broader than both New York law and UTSA. Specifically, this article will provide: (1) a comparison of New York law and UTSA; (2) a description of the EEA and New York's *Aleynikov* case and how that led to DTSA's enactment; (3) a description of the procedural background and evolution of DTSA; and (4) a summary of DTSA's key provisions and how they are likely to be interpreted.

II. Comparison of New York Law and UTSA

DTSA draws significantly from UTSA and was designed, in part, to provide a mechanism for greater state-to-state uniformity, albeit an incomplete one.[5] As such, an understanding of UTSA is important in approaching DTSA, particularly for a litigator in New York where UTSA has never been adopted.

UTSA was originally published by the Uniform Law Commission (the same group that brought us the Uniform Commercial Code) in 1979, and later amended in 1985, for the purpose of providing a uniform act throughout the United States to create more predictability in the law of trade secrets for companies operating in multiple states. UTSA has since been enacted in varying forms—sometimes in whole, other times in part and, still others, with material changes to reflect certain aspects of a particular state's common law. As noted, New York and Massachusetts are the lone holdouts.

While there has been a recent push in New York (as well as Massachusetts) to enact some form of UTSA,[6] New York courts continue to rely upon and apply highly developed, albeit often complex, common law rules for trade secret protection. As explained below, UTSA is in many respects broader than the common law, both in terms of the protections afforded and the remedies provided to litigant victims of trade secret theft.

With respect to the scope of the protections afforded under UTSA, a trade secret is defined more broadly and with far less complexity than its common law counterpart. Specifically, New York common law defines a trade secret as any "formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it," and then applies the following six-factor balancing test to determine whether the information meets the definition:

> (1) the extent to which the information is known outside of the business; (2) the extent to which it is known by employees and others involved in the business; (3) the extent of measures taken by the business to guard the secrecy of the informa-

> tion; (4) the value of the information to the business and its competitors; (5) the amount of effort or money expended by the business in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[7]

UTSA, on the other hand, applies a far simpler definition and test for trade secret protection by defining a "trade secret" as "information…that (i) derives independent economic value…from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, **and** (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[8] While the purpose of the two definitions/rules are obviously the same (i.e., to protect information of value that is secret from competitors), the complexity and ambiguity of the New York rule leaves far more to interpretation (and litigation). While the New York rule may be good for litigators, such is often not the case for clients, as it leads to increased litigation costs and interjects greater uncertainty into the predictability of outcomes for business transactions and relations.

In addition, the New York rule, unlike UTSA, requires that the information be actually "used in one's business,"[9] which has been construed as a "continuous use" requirement for trade secret protection.[10] While courts have clarified that "continuous use" means only that the alleged trade secret cannot be "information as to a single or ephemeral event[] in the conduct of the business,"[11] the fact remains that this requirement would seemingly preclude protection of information pertaining to a past failed and/or abandoned secret process or formula that could nevertheless have economic value to a competitor. The rule under UTSA, on the other hand, is significantly broader in this respect and provides trade secret protection to any secret information, currently in use or long since abandoned, which derives any economic value.[12] While one could argue that the New York rule favors innovation by disincentivizing a company from squatting on new, unpatented technology, it also creates a loophole of sorts in the law by seemingly permitting a competitor to reap the benefits of another company's valuable research and development.

Not only does UTSA expand the scope of trade secret protection afforded by the common law, but it also provides additional remedies not otherwise available. For example, in the event that a UTSA plaintiff can establish that a defendant's misappropriation was willful or malicious, or if a defendant can establish that a plaintiff's claim was made in bad faith, the statute provides for attorneys' fees to the prevailing party.[13] Similarly, a plaintiff who establishes that a defendant's misappropriation was willful or malicious may be awarded "exemplary damages in an amount not to exceed twice any [damage] award" for actual loss.[14] Under the common law, a litigant is, of course, only entitled to its actual damages for any losses sustained and, in the absence of extraordinary circumstances or a "prevailing party" attorneys' fees provision in an employment or other contract, will not be awarded any attorneys' fees incurred in the litigation.

Finally, unlike New York law where an injunction prohibiting employment on the basis of "inevitable disclosure" is, at best, on shaky ground,[15] there exists a significant body of case law standing for the proposition that UTSA permits (and, in essence, codifies) "inevitable disclosure" to enjoin an employee from taking employment with a competitor.[16] While criticized by some other courts,[17] the fact that UTSA permits injunctive relief based upon both "actual and **threatened** misappropriation"[18] has given far more traction and credibility to the applicability of the "inevitable disclosure" to prohibit employment than what currently exists under New York law.

While UTSA affords broader protection to trade secrets and provides greater remedies to litigants than what exists under the common law, it has largely failed in its stated purpose of providing uniformity and predictability for trade secrets across state lines, as there remain two major holdouts (New York and Massachusetts) and numerous states which have adopted only variations of the "uniform" statute. As discussed below, DTSA, which is modeled after UTSA, goes a step further than UTSA by not only creating a federal civil claim for trade secret misappropriation on par with other intellectual property rights, but also providing greater protection and remedies than what exists under UTSA.

III. EEA, New York's *Aleynikov* Case, and DTSA

Given the lack of uniformity in trade secret law across state lines, DTSA was partly designed to provide an overarching umbrella statute to UTSA. More directly, however, DTSA was aimed at the limitations of the EEA by expressly amending that statute. Thus, an understanding of the EEA is also important since a New York commercial litigator may not have had much—if any—exposure to this federal criminal statute either.[19]

The EEA criminalizes "economic espionage" by a foreign[20] entity as well as domestic misappropriation for financial gain.[21] Notwithstanding the purpose and objectives of the EEA, its application has proven ineffective due to limited prosecutorial resources and problems with the textual limitations in the statute itself.

For example, the New York case of *United States v. Aleynikov*[22] exposed major holes in the EEA and the ability of the government to prosecute claims for trade secret theft. In *Aleynikov*, Sergey Aleynikov was a computer programmer employed by Goldman Sachs & Co. to develop computer source code for the company's trading system.[23] Aleynikov left Goldman Sachs to work for another company looking to develop a similar computer system.[24] He was offered over twice his salary ($400,000

to $1,000,000) to develop a similar system in a fraction of the time that it would usually take to develop such a system.[25]

On his last day at Goldman Sachs, Aleynikov encrypted and uploaded more than 500,000 lines of source code for Goldman Sachs' computer trading system.[26] After uploading the source code, Aleynikov deleted the history of his computer commands.[27] When he returned to his home in New Jersey, Aleynikov downloaded the source code from a remote server in Germany to his home computer.[28] Aleynikov then flew to Illinois to meet with his new employer, bringing a flash drive and a laptop containing portions of Goldman Sachs' source code with him.[29] When he flew home the next day he was arrested by the FBI at Newark International Airport.[30]

Following a jury trial in the United States District Court for the Southern District of New York, Aleynikov was convicted under Section 1832 of the EEA.[31] He was sentenced to 97 months of imprisonment followed by a three-year term of supervised release, and was ordered to pay a $12,500 fine. Aleynikov appealed. On April 11, 2012, the Second Circuit reversed Aleynikov's conviction, finding that his conduct did not constitute an offense under the EEA because the source code was not "related to or included in a product that is produced for or placed in interstate or foreign commerce," thus significantly undermining and weakening the EEA's ability to deter misappropriation of valuable trade secrets.[32]

In December 18, 2012, Congress amended the EEA to try to close the "Aleynikov loophole"' in a law referred to as the "Theft of Trade Secrets Clarification act of 2012."[33] That same year Congress also began working toward the creation of a federal civil claim for misappropriation of trade secrets. In 2012, Senators Herb Kohl, Christopher Coons, and Sheldon Whitehouse introduced, without success, the "Protecting American Trade Secrets and Innovation Act of 2012" in the 112th Congress. In 2014, a new bipartisan bill was introduced in the Senate by Senators Christopher Coons and Orrin Hatch in the 113th Congress, entitled "Defend Trade Secrets Act of 2014." An identical textual bill was also introduced in the House by Congressman George Holding, though under the name "Trade Secret Protection Act of 2014." While the Senate bill stalled, the House bill was unanimously passed by the House Judiciary Committee on September 17, 2014, but failed to come to the floor for a vote.

Finally, in July of 2015, identical textual bills were introduced simultaneously in the 114th Congress. This time both bills were entitled "Defend Trade Secrets Act of 2015." The House bill was introduced by Congressman Doug Collins. The Senate Bill was once again introduced by Senator Hatch. The 2015 version contained several modifications to the 2014 version in order to make it more palatable to past critics and bring it more in line with UTSA.[34] On April 4, 2016, the U.S. Senate passed the legislation with a unanimous vote of 87-0. On April 27, 2016, DTSA was approved by the U.S. House of Representatives by a vote of 410-2. As noted, President Obama signed DTSA into law on May 11, 2016.

IV. DTSA's Key Provisions

Definition of "Trade Secret"

With the background and context of DTSA explained, we now turn to the key provisions of DTSA itself. In particular, DTSA uses the definition of "trade secret" found in the EEA, with a few slight modifications, as shown below:

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—
>
> (A) the owner thereof has taken reasonable measures to keep such information secret; and
>
> (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the ~~public, and~~ **another person who can obtain economic value from the disclosure or use of the information**. . . . [35]

As noted above, DTSA's definition tracks the most widely used state definitions under USTA,[36] and, significantly, is broader than the definition currently available under New York law.[37] The additional language added by the amendment (in bold) also creates greater protection by restricting the scope of trade secret discovery (and resulting loss of status) from the "public" in general to a smaller class which is essentially limited to competitors, bringing DTSA in closer conformity with USTA than exists under the EEA.[38]

"Misappropriation" may be established by showing acquisition of the trade secret by "improper means" or disclosure or use of the same where the person in possession of the trade secret (1) knew or should have known that the information was acquired by improper means or under circumstances giving rise to a duty of secrecy, or (2) prior to making a material change in position, the person in possession knew or should have known that the trade secret was disclosed by accident or mistake.[39] As under UTSA, "wrongful means" under DTSA includes theft, bribery, misrepresentation, breach, or inducement of a

breach of a duty to maintain secrecy, or espionage though electronic or other means. However, reverse engineering and independent derivation of the trade secret do not constitute improper means.[40]

Ex Parte Seizure

One of the most controversial aspects of DTSA, and a remedy not found in UTSA, is its allowance for a trade secret owner to seek ex parte seizure of trade secret materials under "extraordinary circumstances."[41] In order to obtain such an order, however, several onerous requirements must be met. As a preliminary matter, a court will not issue such an order unless the applicant meets the threshold requirement for issuance of an injunction, including irreparable injury and a balancing of the equities, as well as a finding by the court that an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order.

"One of the most controversial aspects of DTSA, and a remedy not found in UTSA, is its allowance for a trade secret owner to seek ex parte seizure of trade secret materials under 'extraordinary circumstances.'"

The applicant must then also show a likelihood of success in establishing that (1) the information is a trade secret; (2) the person against whom seizure would be ordered misappropriated the trade secret of the applicant by improper means (or conspired to do so); and (3) the person against whom seizure would be ordered has actual possession of the trade secret (described with reasonable particularity) and that the order is needed to prevent dissemination of the trade secret (which could render the trade secret without value). The applicant must also show that he has not publicized the requested seizure.[42] These requirements are similar to, but slightly more rigorous than, a showing required for the seizure of counterfeit goods under trademark law (i.e. the Trademark Act of 1946 or the Lanham Act).[43]

DTSA also provides detailed requirements for what a seizure order must contain, including (1) mandates for narrowly tailored seizures; (2) reasonable steps to avoid interruption of the business of third parties, as well as the defendant's legitimate business operations; (3) guidance to law enforcement on how to proceed in effecting the seizure; (4) a prompt hearing date following the order's issuance; (5) protection of the seized material; and (6) posting of a bond on the part of the petitioning party. A court must take custody of any seized materials and hold a seizure hearing within seven days. An interested party may file a motion to encrypt seized material. A party harmed by a wrongful or excessive seizure may move to dissolve or modify the order and may also seek relief against the applicant of the seizure order for any resulting losses.[44]

Damages (Including Exemplary Damages and Attorney's Fees)

DTSA allows for an award of damages for actual loss caused by the misappropriation of the trade secret, as well as damages for any unjust enrichment that is not addressed in computing damages for actual loss. In lieu of damages measured by any other methods, DTSA also permits for damages to be measured in terms of the imposition of a reasonable royalty for the defendant's unauthorized disclosure or use of the trade secret. Moreover, and most importantly for litigators and clients alike, if a plaintiff is able to show that the trade secret was "willfully and maliciously misappropriated," a court may award exemplary damages in "an amount not more than 2 times the amount of the damages awarded."[45] Finally, if (1) a claim of misappropriation is made in bad faith, (2) a motion to terminate an injunction is made or opposed in bad faith, or (3) the trade secret was willfully and maliciously misappropriated, a court may disregard the American rule for attorney's fees and award reasonable attorney's fees to the prevailing party.[46]

"Inevitable Disclosure Doctrine" Not Adopted

DTSA specifically states that an injunction issued thereunder cannot "prevent a person from entering into an employment relationship" and that any conditions placed on such a relationship must be based on more than "the information the [former employee] knows[.]"[47] Thus, DTSA makes clear that the "inevitable disclosure doctrine" will not apply in any circumstances under the statute. This doctrine, which exists under New York law, albeit on shaky ground, allows an employer to restrain a former employee from working for a competitor (at least temporarily) based on a showing that the former employee's knowledge of the employer's critical proprietary information is so comprehensive that the employer's trade secrets would inevitably be disclosed and used in the course of the former employee's new employment.[48] Needless to say, the clear language in DTSA would preclude a New York litigant from pursuing such an argument under the terms of the statute. This is not to say, however, that a litigant cannot seek an injunction with respect to the "conditions placed on such employment" (such as not contacting customers the employee dealt with), though the scope and breadth of such conditions

and restrictions will necessarily be fleshed out by the courts, hopefully in the near future.

Whistleblower Immunity Notice Requirement

Imbedded within the text of DTSA is a warning that a plaintiff will not be able to recover exemplary damages or attorney fees if it fails to include a "whistleblower immunity notice" in "any contract or agreement with an employee that governs the use of a trade secret or other confidential information," such as non-disclosure, non-solicitation, and non-competition agreements.[49] The notice must inform the employee (among other things) that he or she cannot be held liable under any trade secret law for the disclosure of a trade secret that is made (1) in confidence to a government official or to an attorney for the sole purpose of reporting a suspected violation of law or (2) in a document in a lawsuit or proceeding filed under seal.[50]

DTSA further provides, however, that an "employer shall be considered to be in compliance with the notice requirement. . .if the employer provides a cross-reference to a policy document provided to the employee that sets forth the employer's reporting policy for a suspected violation of law."[51] Significantly, this notice requirement also may extend to individuals who are independent contractors performing work for a company, as DTSA defines an "employee" to include "any individual performing work as a contractor or consultant for an employer."[52] The notice, however, appears to only be required with "individuals" and may not be required for a third-party company in a joint venture non-disclosure agreement or other such agreement.

V. Conclusion

By adding a private civil claim for theft of trade secrets, federal law now provides protection to trade secrets in a manner similar to other forms of intellectual property (such as trademarks, copyrights and patents). While the full impact of DTSA will not be fully known until after a body of federal case law is developed construing its many significant provisions, it is clear, even at this early stage, that the statute will provide litigants and practitioners in New York new and stronger protections and remedies not available under the common law or even the proposed UTSA legislation.

Although DTSA seeks to create uniformity in trade secret law across state lines, the failure of DTSA to preempt state law dilutes the effectiveness of this stated purpose.[53] This may mean that it will take much longer for uniformity to develop until a substantial body of federal case law is established. Ultimately, however, it is expected that greater uniformity (and predictability for business decisions) will emerge, either through development of jurisprudence or by direct amendment.

New York litigators should take note of DTSA's rejection of the "inevitable disclosure doctrine" as a predicate to obtaining injunctive relief to prevent employment, which is a departure from both UTSA and New York law. Although the relatively weak state of this doctrine in New York may not represent a significant issue (particularly given the upside of the stronger remedial provisions found in DTSA), it is a factor that should be considered in deciding whether to proceed under DTSA or solely in state court under New York common law.[54] It should also be noted that the availability of the federal forum provides mechanisms under the Federal Rules of Civil Procedure which may be broader than what may exist in state court practice, including the availability of expert discovery.[55]

Finally, DTSA's whistleblower immunity notice requirements means that your clients may need to review and revise their non-disclosure, non-solicitation, and non-competition agreements to not only maximize the protections available under DTSA, but also ensure they are consistent with other changes in the ever-evolving case law on the subject. Moreover, there is also the possibility that the failure to include the immunity notice could be interpreted as evidence of overreaching for purposes of refusing to "blue pencil" or reform a restrictive covenant.[56]

Endnotes

1. UTSA has been adopted in 48 States and the District of Columbia, but not in New York or Massachusetts. *See Uniform Law Commission: The National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act*, available at http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act.
2. The authors forecasted the passage of DTSA in the Commercial and Federal Litigation Section's *Newsletter*, Winter 2014, Vol. 20, No. 3, page 7, *Federal Trade Secret Legislation Moves Forward*, available at http://www.nysba.org/WorkArea/DownloadAsset.aspx?id=54068.
3. 18 U.S.C. §§ 1831 *et seq*.
4. *See Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Senate Judiciary Comm., Subcomm. on Crime and Terrorism*, 113th Cong. (2014) (statement of Randall C. Coleman, Assistant Director, Counterintelligence Division, FBI); *see also* Robin L. Kuntz, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets*, 28 Berkeley Technology Law Journal Issue 4 (2013).
5. As discussed below, DTSA does not expressly preempt USTA.
6. New York is currently considering a bill, Senate Bill 3770, to adopt UTSA without significant modifications. It is currently in committee. *See* https://www.nysenate.gov/legislation/bills/2015/s3770. Massachusetts has also recently moved closer to adopting UTSA. Massachusetts House Bill H4434, which adopts UTSA, unanimously passed the House and was transmitted to the Senate Rules Committee. *See* "Massachusetts Senate Votes for Tough Noncompete Bill and Adoption of Uniform Trade Secrets Act," (July 14, 2016), available at https://faircompetitionlaw.com/2016/07/14/massachusetts-senate-votes-for-tough-noncompete-bill-and-adoption-of-uniform-trade-secrets-act/.
7. *Ashland Management v. Janien*, 82 N.Y.2d 395, 407 (1993) (quoting Section 757 of the Restatement of Torts, comment b).
8. Uniform Trade Secrets Act § 1(4) (emphasis added).
9. *Janien*, 82 N.Y.2d at 407.
10. *See, e.g., Lehman v. Dow Jones & Co.*, 783 F.2d 285, 297-298 (2d Cir. 1986).

11. *Id.; see also Zylon Corp. v. Medtronic, Inc.*, 2015 N.Y. Misc. LEXIS 1276 (N.Y. Co. Sup. Ct. 2015).
12. Uniform Trade Secrets Act § 1(4).
13. Uniform Trade Secrets Act § 4.
14. Uniform Trade Secrets Act § 3(b).
15. *See, e.g., Janus et Cie v. Kahnke*, 2013 U.S. Dist. LEXIS 139686 (S.D.N.Y. 2013) (rejecting claim of inevitable disclosure in the absence of a noncompete or evidence of actual misappropriation).
16. *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995).
17. *Kelly Services v. Greene*, 535 F.Supp. 2d 180, 188 (D. Me. 2008) (rejecting argument that the MUTSA (Michigan Uniform Trade Secrets Act) permits an injunction based on "inevitable disclosure").
18. Uniform Trade Secrets Act § 2(a) (emphasis added).
19. Some New York litigators may be familiar with the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which does provide a private right of action. However, that statute is fairly limited in application to cases involving computers of the federal government or certain financial institutions or where the crime is interstate in nature. The statute is more commonly aimed at computer "hacking" rather than directly at theft of trade secrets (which also do not always reside on a computer). It is usually difficult to apply this statute to situations where an employee (such as in the *Aleynikov* case discussed below) accesses his employer's computer in the process of uploading trade secret data since the access to the computer itself was not necessarily "unauthorized."
20. *See* 18 U.S.C. § 1831(a).
21. *See* 18 U.S.C. § 1832(a).
22. *United States v. Aleynikov,* 676 F3d 71 (2d Cir. 2012).
23. *Id.* at 74.
24. *Id.*
25. *Id.*
26. *Id.*
27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. Aleynikov was charged with violating 18 U.S.C. § 1832 (trade secret theft), not § 1831 (economic espionage).
32. *Id.* at 74. 18 U.S.C. § 1832 (trade secret theft) imposes a limitation not found in § 1831 (economic espionage): "Whoever, with intent to convert a trade secret, that is related to or included in a product that is **produced for or placed 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. . .without authorization. . . downloads, uploads, ... transmits,. . .or conveys such information" is guilty of a federal offense, and may be imprisoned for up to 10 years. *Id*. § 1832(a) (emphasis added). The Second Circuit found that evidence of this limitation was lacking with respect to the source code.
33. S. 3642 (112th Congress). Aleynikov would subsequently be prosecuted under state law, which would continue for several years, and also ultimately fail. Litigation continues over payment of Aleynikov's legal fees, with a decision as recently as July 13, 2016. *See Jef Feeley "Goldman Sachs Wins Fight Over Ex-Programmer's Legal Fees,"* available at http://www.bloomberg.com/news/articles/2016-07-13/former-goldman-sachs-programmer-loses-fight-over-legal-fees.
34. *See* Substitute Amendment EHF16041 and Leahy-Grassley Amendment ALB16037.
35. *See* 18 U.S.C. § 1839 (3) and (4); 114 P.L. 153, 130 Stat. 376 at 380-381 (deletions shown by strikethrough and additions shown in bold).
36. The language of the proposed Section 279-N(D) of the UTSA bill currently pending in New York (S.3770), proposed new Article 17-B of the New York Business Corporation Law, is nearly identical.
37. *See* Restatement of Torts §757, requiring actual and continuous use.
38. Both the Court of Appeals for the Seventh Circuit, in *United States v. Lange*, 312 F.3d 263, 267 (7th Cir. 2002), and the Court of Appeals for the Third Circuit, in *United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998), have identified the potential significance of this difference between UTSA and the EEA. The Senate Judiciary Committee noted that it did not intend for DTSA definition of a trade secret to be meaningfully different from that generally used in states that have adopted UTSA.
39. 114 P.L. 153, 130 Stat. at 381. "Misappropriation" and "improper means" are also defined identically to the definitions used by most states under UTSA.
40. *Id.*
41. *Id.* at 376.
42. *Id.* at 376-377.
43. *See* Section 34 of the Lanham Act, 15 U.S.C. § 1116(d)(4)(B).
44. 114 P.L. 153, 130 Stat. at 377-379.
45. A treble damages provision was included in the 2014 version of DTSA but was replaced with a double damages provision in the 2015/2016 version adopted.
46. *Id.* at 379-380.
47. *Id.*
48. *See, Willis of N.Y., Inc. v. DeFelice*, 299 A.D.2d 240, 242, 750 N.Y.S.2d 39 (1st Dept. 2002) (citing *EarthWeb, Inc. v. Schlack*, 71 F. Supp. 2d 299 (S.D.N.Y. 1999)).
49. 114 P.L. 153, 130 Stat. at 384-385.
50. *Id.*
51. *Id.* at 385.
52. *Id.*
53. The lack of express preemption, means that New York litigators may still simultaneously assert both DTSA and common law theft of trade secret claims, which may also result in increased litigation costs.
54. The statute of limitations under DTSA is three years; *see* 114 P.L. 153, 130 Stat. at 380, which is consistent with the limitations period for misappropriation of trade secrets in New York. *See* CPLR 214(4).
55. Recent amendments to New York's Commercial Division Rules, however, are narrowing the gap between federal and state practice in cases subject to those rules. *See* 22 N.YC.R.R. § 202.70.
56. *See Columbia Ribbon & Carbon Mfg. Co., Inc. v. A-1-A Corp.*, 42 N.Y.2d 496, 398 N.Y.S.2d 1004, 369 N.E.2d 4 (1977); *BDO Seidman v. Hirshberg*, 93 NY2d 382, 388-389, 712 NE2d 1220, 690 NYS2d 854 (1999); *Brown & Brown, Inc. v. Johnson*, 115 A.D.3d 162, 980 N.Y.S.2d 631 (4th Dept. 2014).

Heath J. Szymczak and Bradley A. Hoppe are members in Bond Schoeneck & King, PLLC's Litigation Department and have extensive experience in protecting companies from trade secret theft, particularly from former employees. Messrs. Hoppe and Szymczak have developed an innovative Trade Secret Protection Audit which systematically reviews a company's agreements, policies and protocols, as well as its physical and electronic security measures.