AN A.S. PRATT PUBLICATION
OCTOBER 2015
VOL. 1 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 1 | NUMBER 2 | OCTOBER 2015

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Aaron P. Simpson and Adam H. Solomon, *Dealmakers Ignore Cyber Risks at Their Own Peril*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [46] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2015–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The Defend Trade Secrets Act of 2015: Attempting To Make a Federal Case Out of Trade Secret Theft – Part I

By David R. Fertig, Christopher J. Cox, and John A. Stratford*

Recently, legislators in both houses of Congress introduced the Defend Trade Secrets Act, an amendment to the Economic Espionage Act that would create a private, civil cause of action for trade secret misappropriation under federal law. In this first part of a two-part article, the authors provide background on the issue and explain the proposed legislation. The second part of the article, which discusses criticisms and potential concerns about the proposed legislation and what trade secret owners and potential defendants need to know, will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report.

Private civil actions aimed at preventing or redressing the actual or threatened misappropriation of a company's trade secrets are governed primarily by state trade secret misappropriation statutes. Forty-eight states have adopted some form of the Uniform Trade Secrets Act ("UTSA"), but significant differences often exist in the specific enactments of the UTSA in different states. On July 29, 2015, however, legislators in both houses of Congress introduced the Defend Trade Secrets Act (the "DTSA"),[1] an amendment to the Economic Espionage Act (the "EEA") that would create a private, civil cause of action for trade secret misappropriation under federal law.

This is not the first time that Congress has attempted to pass a federal trade secret misappropriation statute and the DTSA, like its predecessors, has already engendered significant debate. The growth of unprecedented cybersecurity risks, however, together with a groundswell of public and bipartisan political support for federal legislation, suggests that the DTSA may finally result in a federal trade secret misappropriation law. Moreover, if adopted in its current form, the DTSA would provide trade secret owners with a potentially powerful new tool in their effort to combat trade secret theft and present both trade secret owners and potential targets of misappropriation claims with a host of important new considerations beyond those raised under the UTSA

* David R. Fertig is a partner in Weil, Gotshal & Manges LLP's Litigation Department in New York, representing clients in the finance, healthcare and life sciences, and technology sectors. Christopher J. Cox is a litigation partner in Weil's Silicon Valley office, where he leads the firm's California complex commercial litigation practice. John A. Stratford is a litigation associate in the firm's Silicon Valley office. The authors may be reached at david.fertig@weil.com, chris.cox@weil.com, and john.stratford@weil.com, respectively.

[1] H.R. 3326 and S. 1890.

laws. Accordingly, business executives and employees would be well advised to pay careful attention to the DTSA as the debate over federal trade secret law continues in Congress.

BACKGROUND

The UTSA was originally promulgated by the Uniform Law Commission and has now been adopted in some form or another by forty-eight states[2]– although its adoption has not been entirely consistent. For example, even among states whose trade secret laws are modeled on the UTSA, the law can vary with respect to, among other things: what constitutes a protectable "trade secret;" what is required to maintain a claim for misappropriation; the time within which a claim for misappropriation must be asserted; and the remedies available.[3]

Unlike other forms of intellectual property, such as patents, copyrights and trademarks, no federal common or statutory law exists that specifically authorizes a private, federal cause of action for misappropriation of trade secrets. Indeed, while the passage of the Economic Espionage Act of 1996[4] made the theft of trade secrets used in interstate commerce a federal crime, punishable by fine and/or imprisonment, the EEA does not authorize a private civil action in federal court by the aggrieved trade secret owner. And although the Computer Fraud and Abuse Act of 1986[5] (the "CFAA") was amended in 1994 to authorize a private, civil cause of action, it applies only when a misappropriator obtains "information from any protected computer" without authorization or by exceeding authorized access, and efforts to rely on that statute to prevent or redress *all* forms of actual or threatened misappropriation have yielded mixed results due to the view of certain federal courts that the CFAA applies only to true "hacking" activity, and not to simple "garden-variety" misappropriation by current or former employees.[6]

---

[2] New York and Massachusetts have not adopted the UTSA, choosing instead to rely on state common law principles.

[3] *See, e.g.*, Tex. Civ. Prac. & Rem. Code Ann. § 134A.002(6) (providing for definition of "trade secret" that explicitly includes customer and supplier lists and financial data); Or. Rev. Stat. § 646.461(1) (specifically providing that reverse engineering and independent development alone are not considered improper means of appropriating a trade secret); Cal. Civ. Proc. Code § 2019.210 (requiring plaintiffs under California's version of the UTSA to identify trade secrets with "reasonable particularity" before initiating discovery relating to the trade secret); Ga. Code Ann. § 10-1-766 (providing for five-year statute of limitations for trade secret claims); Ohio Rev. Code Ann. § 1333.66 (providing for four-year statute of limitations).

[4] 18 U.S.C. § 1831 *et seq.*

[5] 18 U.S.C. § 1030 *et seq.*

[6] *See, e.g., WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 206 (4th Cir. 2012) (affirming dismissal of CFAA claim where "although [the former employees] may have misappropriated information, they did not access a computer without authorization or exceed their authorized access").

Recognizing this, legislators and businesses increasingly have called for legislation that would create a private, federal civil cause of action for trade secret misappropriation so as to place trade secrets on the same footing as other valuable forms of intellectual property. Such legislation, proponents argue, would provide the uniformity lacking under the current patchwork of state statutory and common laws that make it difficult for U.S. businesses to craft consistent policies and obtain predictable and effective relief through the federal courts. Moreover, proponents have argued that a federal cause of action would make it easier for intellectual property owners to enforce their rights with respect to proprietary information by, among other things, providing them with access to a federal forum, granting them the ability to effectuate nationwide service of process, and allowing for more effective nationwide discovery.

Significantly, legislators in both houses of Congress have tried for years to enact legislation that would establish a federal right of civil action for trade secret misappropriation. In fact, bills similar to the DTSA—including the identically titled Defend Trade Secrets Act of 2014 (S. 2267) and the Trade Secrets Act of 2014 (H.R. 5233)—were introduced unsuccessfully in Congress just last year. Undeterred, however, a bipartisan coalition of legislators introduced the DTSA in both the Senate and the House of Representatives on July 29, 2015, insisting that "[s]tate-level civil trade secret laws alone have not been sufficient to stop interstate theft" and that "[c]urrent federal criminal law is insufficient."

The sponsors of the DTSA, which include such high-ranking legislators as Orrin Hatch (R-Utah), Chris Coons (D-Del), Dick Durbin (D-Ill.), Doug Collins (R-Ga.), and Jerrold Nadler (D-N.Y.), emphasized that, "[i]n today's electronic age, trade secrets can be stolen with [just] a few keystrokes."[7] Moreover, the sponsors lamented that trade secrets "increasingly are stolen . . . for the benefit of a foreign competitor," with the result that innovative U.S. businesses lose "hundreds of billions of dollars each year . . . to the theft of corporate trade secrets."[8] The sponsors thus urged that federal legislation is necessary to "empower companies to protect their trade secrets in federal court" and thereby "finally give[ ] trade secrets the same legal protections that other forms of critical intellectual property enjoy."[9]

THE PROPOSED LEGISLATION

In addition to providing trade secret owners with potential access to federal court when diversity of citizenship is lacking or when the CFAA is inapplicable, the DTSA has several primary goals, according to its sponsors. First, it would "[h]armonize U.S. law by. . . creat[ing] a uniform standard for trade secret misappropriation." Second, it

---

[7] Press Release, *Senate, House Leaders Introduce Bipartisan, Bicameral Bill to Protect Trade Secrets* (July 29, 2015), *available at* http://www.hatch.senate.gov/public/index.cfm/releases?ID=ad28f305-f73a-4529-84ba-ad3285b09d6e (hereinafter the "DTSA Press Release").

[8] *Id.*

[9] *Id.*

would "provide for injunctions" to "prevent disclosure" of trade secrets and "preserve evidence." And third, it would "provide for . . . damages to . . . account for the economic harm to American companies whose trade secrets are stolen."[10] With these aims in mind, the DTSA contains several noteworthy provisions.

Creation of a Private, Civil Cause of Action in Federal Court

First, the DTSA would insert a new subsection (b), entitled "Private civil actions," into Section 1836 of the EEA, which would then provide that: "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."[11] In addition, the DTSA would add a new section (c) to Section 1836 of the EEA, which would expressly provide that "[t]he district courts of the United States shall have original jurisdiction of civil actions brought under thus section." The DTSA thus would allow businesses and other trade secret owners to bring suit in federal court to enforce their intellectual property rights provided that the trade secret allegedly misappropriated (or threatened to be misappropriated) is "related to a product used in, or intended for use in, interstate or foreign commerce."

Adoption of UTSA Definitions of "Trade Secret" and "Misappropriation"

In furtherance of its stated goal of "harmonizing" the national patchwork of trade secret protection laws, the DTSA would define the terms "trade secret" and "misappropriation" in a manner virtually identical to the way those terms are typically defined in the UTSA. Indeed, the DTSA would adopt the definition of "trade secret" already found in the EEA, and thus broadly protect "all forms and types of financial, business, scientific, technical, economic, or engineering information, including . . . plans, . . . formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible. . ." provided that (i) "the owner thereof has taken reasonable measures to keep such information secret" and (ii) "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."[12] In addition, like the UTSA, the DTSA would define the term "misappropriation" in a way that would permit trade secret owners to sue *not only* for the actual or threatened "disclosure or use" of their trade secrets "without express or implied

---

[10] *Id.*

[11] DTSA (S. 1890, 114th Cong.), § 2(a) (2015).

[12] 18 U.S.C. § 1389(3). *Compare* Uniform Trade Secrets Act § 1(4) (Uniform Law Comm'n 1985) (hereinafter, the "UTSA") (defining "trade secret" as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, 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.").

consent," *but also* for the "acquisition" of their trade secrets by "a person who knows or has reason to know that [they] w[ere] acquired by improper means."[13]

Remedies & Statute of Limitations

In furtherance of its stated goal of "provid[ing] for . . . damages to . . . account for the economic harm to American companies whose trade secrets are stolen," the DTSA, like the UTSA and the trade secret laws of most states, would expressly permit aggrieved trade secret owners to recover damages for any misappropriation, measured either by actual loss, unjust enrichment, and/or a reasonable royalty for the use of the stolen trade secret. In contrast to the UTSA and the laws of most states, however, the DTSA would also go further and provide for a potential award of *treble* damages if the misappropriation is found to be "willful" and "malicious."[14] In addition, the DTSA would provide a relatively generous limitations period, permitting civil actions for trade secret misappropriation to be instituted up to "5 years after the date on which the misappropriation . . . is discovered or by the exercise of reasonable diligence should have been discovered."[15] By contrast, the UTSA as adopted in most states provides for a considerably shorter three-year statute of limitations.[16]

***Ex Parte* Seizure Procedures**

Finally, in furtherance of its stated goal of "provid[ing] for injunctions" to "prevent disclosure" of trade secrets and "preserve evidence," the DTSA—in what is perhaps its most controversial feature—would provide trade secret owners not only with the right to seek injunctive relief to enjoin any actual or threatened misappropriation,[17] but with the right to request an *ex parte* seizure of any property "necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[18]

---

[13] DTSA § 2(b)(3). *Compare* UTSA § 1(2) (defining "misappropriation" as "(i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use, knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who had utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his [or her] position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.").

[14] DTSA § 2(b)(3)(C). Under the UTSA, a plaintiff may recover exemplary damages in an amount up to only two times its damages in the event the misappropriation is found to be willful and malicious. UTSA § 3(b).

[15] DTSA § 2(d).

[16] UTSA § 6. *But see*, Ga. Code Ann. § 10-1-766 (providing for 5-year limitations period); 765 Ill. Comp. Stat. 1065/7 (providing for 5-year limitations period); Mo. Rev. Stat. § 417.461 (providing for 5-year limitations period).

[17] DTSA § 2(b)(3)(A).

[18] DTSA § 2(b)(2).

Indeed, the DTSA provides that, "based upon an affidavit or verified complaint" "clearly" showing, among other things, that a temporary restraining order "would be inadequate" because the person against whom seizure is sought (or persons acting in concert with such persons) would "destroy, move or hide" the property in question, the court may, "upon *ex parte* application," issue an order "providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action."[19]

* * *

The second part of this article, which discusses criticisms and potential concerns about the proposed legislation and what trade secret owners and potential defendants need to know, will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*.

[19] *Id.* The *ex parte* applicant also would have to make a showing akin to that traditionally required to obtain injunctive relief, including a demonstration that: (a) it is likely to succeed on its misappropriation claim; (b) in the absence of the requested seizure, it would suffer immediate and irreparable injury; and (c) the balance of harms weighs in its favor.