

Articles

Amendments to the Economic Espionage Act Broaden Trade Secret Protection

January 2013

White & Case Technology Newsflash

Daren M. Orzechowski, Meredith Louis

Technology Newsflash

Protecting and enforcing trade secrets in the United States has historically been challenging. Recent amendments to the Economic Espionage Act of 1996¹ (the "EEA"), which criminalizes theft of trade secrets, broaden the scope of prohibited conduct and enhance maximum penalties for offenders. The amendments signal an increased government interest in trade secret protection, which is likely in recognition of the important role trade secrets play in our nation's economy. These amendments could rekindle discussions of establishing a private civil cause of action under the EEA in the near future, something the amendments did not create.

As originally drafted, the EEA criminalized two broad categories of trade secret theft: theft or misappropriation of trade secrets to benefit a foreign government, instrumentality, or agent² (also referred to as "economic espionage") and theft or misappropriation of trade secrets "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" and with the intent to cause injury.³ The EEA also covers knowing possession, receipt, or purchase of stolen or misappropriated trade secrets falling into either category, as well as attempting or conspiring with others to commit a covered offense.⁴ Maximum penalties for violating the EEA, as originally drafted, range from a \$500,000 fine and fifteen years imprisonment for individual offenders convicted of economic espionage, or a \$10 million fine for corporate offenders,⁵ to a \$250,000 fine coupled with ten years imprisonment for individual offenders, or a \$5 million fine for corporate offenders, convicted of misappropriating trade secrets related to a product.⁶ The EEA also provides for forfeiture of any property or proceeds derived from the stolen or misappropriated trade secrets, as well as any property used or intended to be used to commit or facilitate such theft or misappropriation.⁷

The recently enacted Theft of Trade Secrets Clarification Act of 2012 expanded the scope of the EEA, clarifying that it applies to trade secrets relating to both products and services used in commerce.⁸ The amendment was passed in response to a recent decision of the United States Court of Appeals for the Second Circuit involving a prosecution against a former Goldman Sachs employee for alleged theft of the source code for a proprietary high-frequency trading system.⁹ In a strict construction of the statute, the court held that as originally drafted, the EEA only criminalized theft of trade secrets covering products "produced for or used in commerce."¹⁰ Therefore, the statute did not encompass the defendant's actions as the trading system at issue was used exclusively for internal purposes and neither produced any goods sold in commerce nor was it ever sold or licensed to third parties.¹¹ The amendment closes this unintended loophole by adding explicit language to the EEA clarifying that it encompasses theft of trade secrets "related to a product *or service* used in *or intended for use*" in commerce.¹² The amendment has the potential to increase the number of enforcement actions in the hardware, software and financial sectors, each of which rely heavily on trade secret protection for, among other things, internal processes or methods of doing business or gathering information that may not qualify for patent protection.

Additionally, the most recently proposed amendment, which was passed by Congress on January 1, 2013 and is currently awaiting the President's signature,¹³ will further amend the EEA by increasing fines for individual and corporate offenders.¹⁴ Specifically, the amendment, known as the Foreign and Economic Espionage Penalty Enhancement Act of 2012, will increase maximum fines for individuals convicted of misappropriating trade secrets for the benefit of a foreign government or agent from \$500,000 to \$5 million, while increasing maximum fines for organizations from \$10 million to "the greater of \$10 million or three 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."¹⁵ Further guidance on trade secret valuation methods for purposes of calculating such fines is left open for judicial determination. The amendment also includes a mandate to the U.S. Sentencing Commission to review and, if appropriate, amend the Federal sentencing guidelines applicable to individuals convicted of economic espionage and/or transmitting or attempting to transmit a misappropriated trade secret outside of the U.S.¹⁶

The increased penalties, once enacted into law and when coupled with the expanded scope of the EEA, significantly enhance remedies available to a broader range of businesses that rely upon trade secrets. This renewed focus on trade secret protection may lead to an increase in the number of federal criminal cases brought under the EEA. However, while the EEA creates a limited civil cause of action allowing the Attorney General to seek injunctive relief against offenders,¹⁷ it does not currently provide for a private cause of action. Rather, individuals and organizations seeking to protect against trade secret theft are still left to pursue civil actions at the state level for trade secret misappropriation and other business torts, which can be challenging from an evidentiary as well as an enforcement standpoint. Until a federal private cause of action is available, companies victimized by trade secret misappropriation may wish to help the government build a criminal case under the EEA in addition to taking whatever civil action they may deem appropriate.

1 - Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-39 (2012).

2 - 18 U.S.C. § 1831(a).

3 - 18 U.S.C. § 1832(a).

4 - 18 U.S.C. §§ 1831(a)(3)-(5) and 1832(a)(3)-(5).

5 - 18 U.S.C. § 1831(a)-(b).

6 - 18 U.S.C. §§ 1832(a)-(b), 3571(b)(3).

7 - 18 U.S.C. §§ 1834, 2323(b).

8 - Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (2012).

9 - *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. 2012).

10 - *Id.* at 82.

11 - *Id.*

12 - Theft of Trade Secrets Clarification Act of 2012, S. 3642, 112th Cong. § 2 (2012) (emphasis added).

13 - H.R. 6029 (112th): Foreign and Economic Espionage Penalty Enhancement Act of 2012, Overview, GOVTRACK.US (Jan. 15, 2013), govtrack.us/congress/bills/112/hr6029.

14 - Foreign and Economic Espionage Penalty Enhancement Act of 2012, H.R. 6029, 112th Cong. § 2(a) (2012).

16 - H.R. 6029 § 2(b).

17 - H.R. 6029 § 3(a).

19 - 18 U.S.C. § 1836(a).

This article is provided for your convenience and does not constitute legal advice. It is prepared for the general information of our clients and other interested persons. This article should not be acted upon in any specific situation without appropriate legal advice, and it may include links to websites other than the White & Case website. White & Case LLP has no responsibility for any websites other than its own, and does not endorse the information, content, presentation or accuracy, or make any warranty, express or implied, regarding any other website.

This article is protected by copyright. Material appearing herein may be reproduced or translated with appropriate credit.