# FOOL ME ONCE: *U.S. V. ALEYNIKOV* AND THE THEFT OF TRADE SECRETS CLARIFICATION ACT OF 2012

*Robert Damion Jurrens*[†]

On a warm, humid evening in July of 2009,[1] FBI agents swarmed an unassuming computer programmer named Sergey Aleynikov at Newark Liberty International Airport.[2] Returning from what he thought was a routine business trip to meet with his new employer in Chicago, Aleynikov was arrested and charged with stealing trade secrets from his former employer, multinational investment banking firm Goldman Sachs. On the eve of Independence Day, in an airport whose very name evokes images of freedom, Sergey Aleynikov faced a significant interruption of his own personal liberty. Aleynikov's theft of trade secrets led to charges under the Economic Espionage Act of 1996 ("EEA"), a rarely invoked criminal statute whose vagueness had been challenged by a number of high-profile cases.[3] Convicted in a jury trial in the Southern District of New York, Aleynikov faced ninety-seven months in federal prison.[4]

Fate intervened in the form of a "dangerous loophole"[5] in the EEA, and the Court of Appeals for the Second Circuit delivered a controversial opinion that ultimately freed Aleynikov and shocked Congress into action.[6] The Second Circuit held that the high frequency trading ("HFT") code stolen by Aleynikov was not a "product produced for [or] placed in interstate or



† J.D. Candidate, 2014, University of California, Berkeley School of Law.

1. *See History for Newark, NJ, Friday, July 3, 2009*, WEATHER UNDERGROUND, http://www.wunderground.com/history/airport/KEWR/2009/7/3/DailyHistory.html?req_city=Newark+International&req_state=NJ&req_statename=New+Jersey/.

2. U.S. v. Aleynikov (*Aleynikov I*), 785 F. Supp. 2d 46, 54 (S.D.N.Y. 2011).

3. *See infra* Section I.A.3.

4. *See Former Goldman Sachs Computer Programmer Sentenced in Manhattan Federal Court to 97 Months in Prison for Stealing Firm's Trade Secrets, New York Field Office*, FEDERAL BUREAU OF INVESTIGATION (Mar. 18, 2011), http://www.fbi.gov/newyork/press-releases/2011/former-goldman-sachs-computer-programmer-sentenced-in-manhattan-federal-court-to-97-months-in-prison-for-stealing-firm2019s-trade-secrets/.

5. 158 Cong. Rec. H00000-52, 2012 WL 6605649 (2012) (statement of Rep. Smith).

6. *Id.* ("The Second Circuit's Aleynikov decision revealed a dangerous loophole that demands our attention. . . . We must also take action in response to the Second Circuit's call and ensure that we have appropriately adapted the scope of the EEA to the digital age.").

foreign commerce," and therefore not subject to the EEA.[7] Though liberated from his federal conviction, New York State has since filed its own charges and continues to pursue the matter under state computer crime statutes.[8]

In the wake of the Second Circuit's controversial opinion in *U.S. v. Aleynikov*, Congress moved quickly and efficiently to close a gaping hole in the EEA. The Theft of Trade Secrets Clarification Act[9] ("TTSCA") lived up to its name, altering a few simple words in the EEA in an effort to fortify the only existing federal criminal cause of action for trade secret misappropriation. Congress addressed the Second Circuit's opinion directly, noting that the court had "held that the federal statute prohibiting the theft of trade secrets does not apply to computer source code in some circumstances."[10] Signed into law on December 28, 2012, the TTSCA ushers in a refreshed version of the EEA—one whose less-vague verbiage would almost certainly have sustained Aleynikov's conviction.

But the TTSCA left two important issues unresolved. First is the case of Samarth Agrawal, whose path is eerily similar to that of Aleynikov—computer programmer steals HFT code from financial services behemoth in New York City and gets convicted under the EEA—except that the Second Circuit has not yet handed down a decision in *U.S. v. Agrawal*.[11] Will the Second Circuit uphold *Agrawal* where it reversed *Aleynikov* simply due to unfortunate timing? Or will the U.S. Constitution's explicit prohibition of ex post facto laws leave him with a fighting chance to overturn his conviction?

Second, Congress failed to address the explicit lack of preemption in the EEA.[12] Though most states have enacted criminal laws regarding trade secret misappropriation that are substantially similar to the EEA, there is nothing protecting a defendant from conviction under both state law and the EEA.[13] Such was the case with Sergey Aleynikov, who eluded conviction under the EEA only to find himself hauled before a trial court judge under New York State charges.[14] And even if the Second Circuit strikes down Samarth

7. U.S. v. Aleynikov (*Aleynikov II*), 676 F.3d 71, 82 (2d Cir. 2012) (internal quotations omitted).

8. *See* Kim Zetter, *Goldman Sachs Programmer Back in Court on New Charges*, WIRED (Aug. 9, 2012 2:46 PM), *available at* http://www.wired.com/threatlevel/2012/08/sergey-aleynikov-new-charges/.

9. Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, 126 Stat 1627 (2012).

10. 158 Cong. Rec. H00000-52 (statement of Rep. Scott).

11. *See* U.S. v. Agrawal, No. 11-1074 (2d Cir. filed Dec. 30, 2011).

12. *See* 18 U.S.C. § 1838 (2012).

13. *See id.*

14. *See generally infra* Part II.

Agrawal's conviction, similar state charges almost certainly await him. Without preemption of state laws, defendants faced with charges under the EEA could also find themselves charged under state trade secret misappropriation statutes. And, given the borderless nature of the Internet, such a defendant could face charges under statutes in several different states.[15]

This Note analyzes the effect of the TTSCA, and argues that Congress should continue to cast a watchful eye on the EEA. Part I examines the EEA in detail, including its rocky history with the void for vagueness doctrine. Part II details the plight of Sergey Aleynikov and his arduous path through the federal court system, culminating in his recent arrest under New York State law. Part III examines the TTSCA's scope and the unintended concomitant confusion it created in *Agrawal*—tried under one version of the EEA, but likely to be decided under another ex post facto. Finally, Part IV analyzes potential outcomes in the *Agrawal* case and argues that federal preemption is crucial to the healthy operation of the EEA. In order to ensure justice under the EEA, federal preemption—rather than the uncertainty of a mixed bag of state statutes—is necessary.

## I. LEGISLATIVE BACKGROUND AND A BRIEF HISTORY OF THE EEA

Trade secret protection in the United States does not have strong roots in criminal law. In fact, misappropriation of a trade secret was historically the bailiwick of tort law.[16] Originally codified in the Restatement of Torts, much modern trade secret law still resides in civil courts.[17] In 1979, the National Conference of Commissioners on Uniform State Laws created a model statute for trade secret protection, known as the Uniform Trade Secrets Act ("UTSA").[18] The UTSA is a wholly civil statute and some version of it has been codified in forty-six states and the District of Columbia.[19]

Criminalizing the theft of classified commercial information emerged as a priority in American law in the mid-1960s.[20] Many states have since enacted

15. *See infra* Section III.B.

16. ROBERT P. MERGES, PETER S. MENELL, AND MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 35 (5th ed. 2009).

17. *See id.*

18. *Id.* at 36.

19. *Id.*

20. *See* Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921, 930 (1989).

laws to combat acts involving computer data,[21] and more than half have enacted statutes that regulate trade secret misappropriation.[22] These statutes vary widely from state to state, and there is no one model for protection or punishment.[23] Prior to the enactment of the EEA in 1996, there was no federal cause of action for trade secret misappropriation.

### A. ECONOMIC ESPIONAGE ACT

The EEA makes trade secret theft a federal crime.[24] It is composed primarily of two sections that cover foreign and domestic intellectual property theft.[25] The first section criminalizes trade secret theft committed to benefit a foreign government, instrumentality, or agent (thus the "espionage" moniker).[26] The second section criminalizes the theft of trade secrets related

21. *See id.* at 931; *see, e.g.*, 18 U.S.C. § 1030(a)(5) (Supp. V 1987); ALASKA STAT. § 11:46.740(a)(2) (Supp. 1988); ARIZ. REV. STAT. ANN. § 13-2316(B) (1978); ARK. STAT. ANN. § 5-41-104(a) (Supp. 1987); CAL. PENAL CODE § 502(c)(1), (4) (West 1988); CONN. GEN. STAT. ANN. § 53a-251(e) (West 1985); DEL. CODE ANN. tit. 11, § 935(2)(a) (1987); FLA. STAT. ANN. § 815.04(1), (2) (West Supp. 1989); GA. CODE ANN. § 16-9-93(b) (1988); IDAHO CODE § 18-2202(2) (1987); ILL. REV. STAT. ch. 38, paras. 16D-3(a)(3), 16D-5(a)(2) (1987); IOWA CODE § 716A.3 (Supp. 1989); KY. REV. STAT. ANN. § 434.845(1) (Michie/Bobbs-Merrill 1985); LA. REV. STAT. ANN. § 14:73.2(A)(1) (West 1986); MD. ANN. CODE art. 27, § 45A(b)(1), (2) (1987); MICH. COMP. LAWS ANN. § 752.795 (West Supp. 1989); MINN. STAT. § 609.88(1)(a), (b) (1982); MISS. CODE ANN. § 97-45-9(1)(a) (Supp. 1988); MO. REV. STAT. § 569.095(1)(1), (2) (1986); MONT. CODE ANN. § 45-6-311(1)(b) (1987); NEB. REV. STAT. § 28-1345 (1985); NEV. REV. STAT. § 205.4765(1)(d)(f)(h) (1987); N.H. REV. STAT. ANN. § 638:17(iv)(b)(1), (2) (1986); N.J. STAT. ANN. § 2C:20-25(e) (West Supp. 1989); N.M. STAT. ANN. § 30-16A-4 (1989); N.Y. PENAL LAW § 156.25 (Mckinney 1988); N.D. CENT. CODE § 12.1-06.1-08(2) (1985 & Supp. 1989); OKLA. STAT. tit. 21, § 1953(1), (2) (Supp. 1988); OR. REV. STAT. § 164.377(3), (4) (Supp. 1988); R.I. GEN. LAWS § 11-52-3 (1981 & Supp. 1988); S.C. CODE ANN. § 16-16-20(1)(a) (Law. Co-op. 1985); S.D. CODIFIED LAWS ANN. § 43-43B-1(2), (3), (4) (1983 & Supp. 1989); UTAH CODE ANN. § 76-6-703(1), (2) (Supp. 1989); VA. CODE ANN. § 18.2-152.4(2), (3), (4), (5) (6) (1988); WIS. STAT. ANN. § 943.70(2)(a) (1), (2) (West Supp. 1989); WYO. STAT. § 6-3-502(a)(iii) (1988).

22. *See* Lederman, *supra* note 20; *see, e.g.*, ALA. CODE § 13A-8-10.4 (Supp. 1989); ARK. STAT. ANN. § 5-36-107 (Supp. 1987); CAL. PENAL CODE § 499c (West 1988); COLO. REV. STAT. § 18-4-408 (1986); CONN. GEN. STAT. ANN. § 53a-124 (West 1985); FLA. STAT. ANN. § 812.081 (West 1976 & Supp. 1989); GA. CODE ANN. § 16-8-13 (1988); MASS. ANN. LAWS ch. 266, § 30(4) (Law. Co-op 1980 & Supp. 1989); MINN. STAT. § 609.52(1), (2), (6), (8) (1982); NEB. REV. STAT. §§ 87-502 (Supp. 1988); N.Y. PENAL LAW §§ 155.00, 155.05, 155.30, 165.07 (McKinney 1988); OKLA. STAT. tit. 21, § 1732 (Supp. 1988); 18 PA. CONS. STAT. § 3930 (Supp. 1988); TENN. CODE ANN. § 39-3-1126 (1982); TEX. PENAL CODE ANN. § 31.05 (Vernon 1989); WIS. STAT. ANN. § 943.205 (West 1982 & Supp. 1989).

23. *See* Lederman, *supra* note 20.

24. 18 U.S.C. § 1831 *et seq.* (2012).

25. *Id.*

26. Section 1831 provides:

to or included in a "product that is produced for or placed in interstate or foreign commerce."[27]

---

(a) 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;

(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.

(b) Organizations.—Any organization that commits any offense described in subsection (a) shall be fined not more than $10,000,000.

*Id.*

27. Section 1832 provides:

(a) 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

(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;

(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.

The EEA's definition of trade secrets is substantially similar to that of the UTSA, and includes "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing"[28] that (1) the owner has attempted to keep secret, and (2) derives value from its secrecy.[29] There is no private cause of action contained in the EEA.[30] The EEA expressly states that it does not preempt any other trade secret laws, which leaves companies open to pursue federal or state actions.[31]

*1. Legislative History of the EEA*

The EEA was enacted in 1996 to assist prosecutors in stemming the theft of intellectual property from U.S. companies.[32] By the mid-1990s, thanks to burgeoning technological innovations and globalization of trade, Congress perceived theft of U.S. trade secrets by foreign entities to be a major issue.[33] Much of this theft was undertaken in the interest of foreign entities, many of

> (b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

*Id.* § 1832.

28. UNIF. TRADE SECRETS ACT ("UTSA"), § 1(4), 14 U.L.A. 438 (1996).

29. *See* 18 U.S.C. § 1839 (2012). It states:

> (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.

*Id.* § 1839.

30. Section 1836 states that the "Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter." *Id.* § 1836.

31. *Id.* § 1838; *see also* Zetter, *supra* note 8.

32. *See* H.R. Rep. No. 104-788, at 3–8, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4022–26.

33. *See id.* at 4022 ("More disturbingly, there is considerable evidence that foreign governments are using their espionage capabilities against American companies.").

which had allegedly hired former Cold War political spies whose talents played well in the world of industrial espionage.[34]

This international espionage legacy shaped the development of the early legislation, all of which dealt solely with theft by foreign entities. Section 1831 of the EEA is devoted entirely to this issue.[35] Section 1832 is nearly a carbon copy of 1831, but is devoted to domestic trade secret theft and appears to have been pasted on in haste.[36] In fact, "[c]oncerns that such a law might violate a number of international trade treaties to which the United States is a signatory caused the bill to be rewritten at the last minute to include both foreign and domestic theft of trade secrets."[37]

*2. Section 1832's Cryptic Requirement*

Possibly the most controversial nuance of § 1832 of the "old"[38] EEA was the requirement that trade secret be "related to or included in a product that is produced for or placed in interstate or foreign commerce." Absent from the original Senate bill, Congress later added the language to § 1832 but omitted it from § 1831.[39] As discussed in some detail in Part II, *infra*, courts have construed this phrase in contradictory ways. This language proved to be the key point on which the trial and appellate courts diverged in their interpretation of the EEA in the *Aleynikov* case.

*3. Void for Vagueness Doctrine*

The lack of clear and consistent construction of the "old" EEA is evident in the frequent use of the void for vagueness doctrine by defendants in cases involving § 1832.[40] The void for vagueness doctrine states that a statute "must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties."[41] The doctrine demands that defendants receive ample notice that they are in violation of a

34. *See* U.S. v. Hsu (*Hsu II*), 155 F.3d 189, 194–95 (3d Cir. 1998) (citing the legislative history of the EEA).

35. *See* 18 U.S.C. § 1831. *See also* Robin L. Kuntz, Note, *How Not to Catch a Thief: Why the Economic Espionage Act Fails to Protect American Secrets*, 28 BERKELEY TECH. L.J. 901, 905–07 (2013) (offering an in-depth discussion of § 1831).

36. *See* 18 U.S.C. § 1832; James H. Pooley, Mark A. Lemley, & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 183 (1997).

37. *Id.* at 187.

38. When necessary, and for the purposes of clear delineation, this note will refer to the pre-TTSCA statute as the "old" EEA and the post-TTSCA statute as the "new" EEA.

39. *See* Pooley, James H. A.; Lemley, Mark A.; Toren, Peter J., *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 183 (1997).

40. *See* U.S. v. Krumrei, 258 F.3d 535 (6th Cir. 2001); U.S. v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005); U.S. v. Hsu (*Hsu I*), 40 F. Supp. 2d 623 (E.D. Pa. 1999).

41. Connally v. Gen. Constr. Co., 269 U.S. 385, 391 (1926).

given statute. Three frequently cited cases have attacked three different aspects of the "old" EEA under the void for vagueness doctrine: *U.S. v. Hsu*, *U.S. v. Krumrei*, and *U.S. v. Genovese.*

*U.S. v. Hsu* was one of the first cases tried under § 1832 of the EEA. In *Hsu*, defendant Kai-Lo Hsu was charged under the EEA in an alleged conspiracy to steal trade secrets from Bristol-Myers Squibb.[42] Hsu challenged the EEA as unconstitutionally vague in three important respects. First, Hsu argued that it failed to define the term "'related to or included in' a product produced for or placed in interstate or foreign commerce."[43] Second, Hsu asserted that the very definition of the term "trade secret" was vague because it did not define "reasonable measures" to maintain secrecy.[44] Third, Hsu argued, it did not define "generally known" or "readily ascertainable" to the public.[45]

The *Hsu* trial court noted that legislation creating "new" crimes is prone to attacks under the void for vagueness doctrine, acknowledging that the EEA criminalizes "conduct that heretofore was thought best left to the civil law of unfair competition and cognate jurisprudence."[46] The court then rejected the argument that the term "related to or included in a product that is produced for or placed in interstate or foreign commerce" was vague, noting that someone "well versed" in the processes of a particular industry could understand its application to that industry.[47] The court went on to reject Hsu's argument that the definition of "trade secret" was unconstitutionally vague, citing at one point the fact that the nearly identical definition used by the UTSA had withstood at least one void-for-vagueness attack.[48]

Two years later, in *U.S. v. Krumrei*, a defendant argued that the vagueness of the phrase "reasonable measures to keep such information secret" could potentially lead to arbitrary enforcement of the EEA.[49] In *Krumrei*, the defendant was accused of stealing intellectual property related to a process for applying hard coatings to laminate surfaces from Wilsonart International, Inc.[50] The Sixth Circuit, citing *Hsu*, noted that if a party knew that information was proprietary and knew that his actions were unlawful, then

42. *Hsu I*, 40 F. Supp. 2d at 623.
43. *Id.* at 626.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* at 627.
48. *Id.* at 628; *see also* People v. Serrata, 62 Cal. App. 3d. 9 (1976).
49. U.S. v. Krumrei, 258 F.3d 535, 538 (6th Cir. 2001).
50. *Id.*

the statute was constitutional as applied in that case.[51] Since Krumrei had admitted that he knew the intellectual property he was appropriating did not belong to him, and that he should have known—but "chose to ignore"—that his actions were illegal, the court found no basis for attacking the EEA based on vagueness.[52]

Finally, in *U.S. v. Genovese*, the court once again attacked the very definition of the term "trade secret" as vague.[53] In *Genovese*, the defendant allegedly downloaded, copied, and sold copies of Microsoft's then-unreleased Windows NT 4.0 and Windows 2000 operating systems.[54] Genovese argued that he found the code on the Internet, and could not have known either that the code was "not . . . generally known to . . . the public" or that Microsoft had taken "reasonable measures" to keep it secret.[55] The district court noted, however, that Genovese had referred to the code as "jacked," stating that others would have to "look hard" to find it elsewhere.[56] These facts, the court opined, indicated that Genovese was therefore on notice that Microsoft had not yet released the code to the public, and that its value was tied to its relative obscurity.[57] Applying the statute to the facts of the case, the court held that the EEA was not unconstitutionally vague and that Genovese knew or should have known that the code was a trade secret.[58]

Though the void for vagueness doctrine was not successfully argued in any of these cases, the fact that the doctrine has cropped up so frequently is both an indication that the "old" EEA was rarely invoked (and therefore provided little in the way of common law guidance) and that its content could be perceived as unclear or ambiguous.

## II. *U.S. V. ALEYNIKOV*

In December of 2010, a jury found Sergey Aleynikov guilty of two counts of theft of trade secrets under the "old" EEA, and interstate transportation of stolen property under the National Stolen Property Act of 1934[59]

51. *Id.* at 539.
52. *Id.*
53. U.S. v. Genovese, 409 F. Supp. 2d 253 (S.D.N.Y. 2005).
54. *Id.* at 255.
55. *Id.* at 257.
56. *Id.*
57. *Id.*
58. *Id.* at 258.
59. *See* 18 U.S.C. § 2314. The National Stolen Property Act ("NSPA") of 1934 combats interstate theft of goods. A product of Depression-era anti-bootlegging efforts, the NSPA deals explicitly with "stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting." *Id.*

("NSPA").[60] Over the course of the next year and a half, trial and appellate courts took starkly contrasting views of the application of the EEA and NSPA to Aleynikov's case.

Goldman Sachs employed Sergey Aleynikov as a programmer from May of 2007 to June of 2009, when he accepted an offer from a Chicago-based startup called Teza.[61] About two months prior to his last day at Goldman Sachs, Aleynikov began uploading proprietary data to an Apache Subversion[62] site on a German server.[63] He went out of his way to avoid detection, deleting his encryption key and attempting to clear his bash history.[64] The files he stole included, in the court's words, components "connecting to the various securities exchanges; reading the incoming price data; pricing algorithms; trading strategies; the infrastructure for routing the trading decisions back to the exchanges; and applications for monitoring the performance of all of these intricate parts of the trading system."[65]

Members of the Goldman Sachs security team noticed Aleynikov's theft of proprietary files shortly after he left the company, and immediately notified the authorities.[66] On July 3, 2009, the FBI arrested Aleynikov at Newark airport as he was returning from a meeting with Teza in Chicago.[67] He was carrying a thumb drive and laptop computer containing Goldman Sachs' proprietary source code.[68] The FBI later searched Aleynikov's home, and found that his personal desktop computer also held proprietary code.[69] While in Chicago, he had uploaded at least two files containing proprietary Goldman Sachs source code to a Teza server.[70] In an e-mail to his Teza

60. *See Aleynikov I*, 785 F. Supp. 2d 46, 55 (S.D.N.Y. 2011).

61. *Id.* at 52.

62. Despite its rather ominous moniker, a "subversion" site is merely one that uses a software versioning and revision control system for the Linux-based open-source Apache web server platform. Aleynikov, an experienced developer, likely favored a Subversion server for its flexibility in moving and copying files.

63. *Id.* at 53. The geographic location of the server, while trivial in the borderless world of the Internet, seemed to be of some importance to the trial court—perhaps because of the invocation of a statute aimed squarely at international espionage.

64. *Id.* A bash history is a history of Linux commands used by a programmer during a single session or multiple sessions. It allows Linux users to quickly type in commands, and provides a relatively superficial record of a given user's activities on a Linux-based server. The fact that Aleynikov attempted to clear his bash history is an indication that he was covering his tracks.

65. *Id.* at 54.

66. *Id.*

67. *Id.*

68. *Id.*

69. *Id.*

70. *Id.* at 57

colleagues, he implied that the source code contained in the two files he uploaded was his own, tacitly taking credit for Goldman Sachs' proprietary work.[71]

### A. HIGH FREQUENCY TRADING

High frequency trading ("HFT") is a form of automated, algorithmic trading that involves the use of highly sophisticated computer programs to trade securities.[72] Firms that engage in such trading hold onto positions for seconds at a time, and generally end a trading day with no net positions.[73] Decisions are made through high-speed mathematical analysis of market data, taking advantage of trading opportunities that open up for fractions of a second.[74]

High frequency trading generates huge amounts of revenue for financial institutions, but it can also be a hazardous undertaking. HFT systems increase price volatility between the buy and ask spread of equities, and have allegedly led to more than one "flash crash" that put equity markets into abrupt tailspins.[75] There is a strong argument that HFT's effect on national and international financial markets necessitates federal intervention.[76] And while large trading institutions have the personnel and resources to develop their own trading systems, smaller start-ups might require much more time to achieve market readiness. This imbalance of opportunity could tempt smaller players to turn to theft as a more efficient option than in-house development of HFT systems—exactly the sort of shortcut that landed Aleynikov (and Agrawal) in court.

Currently, algorithmic trading accounts for an astounding 73% of all daily volume; however, only 2% of all trading firms engage in algorithmic

71. *Id.* The court's mention of Aleynikov's ill-gotten credit for the stolen files alludes to the lack of action taken against Teza.

72. *See* Nathan D. Brown, *The Rise of High Frequency Trading: The Role Algorithms, and the Lack of Regulations, Play in Today's Stock Market*, 11 APPALACHIAN J.L. 209, 209 (2012).

73. *Id.* A "position" simply refers to the amount of a security owned. In an HFT trade, the amount of time between the purchase and sale of an investment can be measured in seconds.

74. *Id.*

75. *See* David M. Serritella, *Recent Development: High Speed Trading Begets High Speed Regulation: SEC Response to Flash Crash, Rash*, 2010 U. ILL. J.L. TECH. & POL'Y 433, 439 (2010).

76. Though the SEC does regulate trading activity and algorithmic trading, some have suggested that the federal government lacks the necessary knowledge to monitor HFT. *See* Nina Mehta, *SEC Leads from Behind as High-Frequency Trading Shows Data Gap*, BLOOMBERG NEWS (Oct. 1, 2012), *available at* http://www.bloomberg.com/news/2012-10-01/sec-leads-from-behind-as-high-frequency-trading-shows-data-gap.html.

trading.[77] And small start-ups are hardly to blame for market aberrations. In fact, recent "flash crashes" have been attributed to miscues by very large institutions.[78] Teza founder Mikhail Victorovich Malyshev asserted during the *Aleynikov* trial that his start-up trading company would not have used Goldman's code had it been offered.[79] Malyshev wanted to "build the best high frequency company in the world" and felt that copying the existing system of an industry heavyweight was counter to that goal.[80] Malyshev's attitude exemplifies the independent, innovative spirit of many start-ups.[81]

While Teza is a start-up in a broad sense, Malyshev is an experienced algorithmic trader who brings years of experience—as well as significant monetary resources—to the table. Thus, start-ups with less experience and fewer resources might not be quite so ambitious or diligent. And while larger institutions normally have ample resources to develop HFT systems of their own, they might still be tempted to engage in industrial espionage to enhance their own algorithms. In the words of Francis Bacon, "[o]pportunity makes a thief."[82]

Regardless of the source of HFT technology development, its effect on worldwide markets is inescapable. Cases like *Aleynikov* and *Agrawal* show that misappropriation of algorithmic code is a viable concern for the financial industry. And recent "flash crashes" show that HFT's rapidly growing influence on world markets can lead to unintended consequences when systems falter. Federal regulation is therefore both necessary and justified.

### B. SOUTHERN DISTRICT OF NEW YORK

Aleynikov filed a motion to dismiss his conviction on the grounds that the HFT system whose code he stole was (1) not a good, ware, or merchandise as defined by the NSPA,[83] and (2) not "a product . . . produced for or placed in interstate or foreign commerce," and therefore not subject to

77. Brown, *supra* note 72, at 212.

78. *See id.* at 216.

79. *Aleynikov I*, 785 F. Supp. 2d 46, 57 (S.D.N.Y. 2011).

80. *Id.* at 53.

81. *See* Drew Hansen, *11 Lessons From Startups on Creating Hotbeds of Innovation*, FORBES.COM (Dec. 6, 2012), http://www.forbes.com/sites/drewhansen/2012/12/06/11-lessons-from-startups-on-creating-hotbeds-of-innovation/.

82. Generally attributed to a letter Bacon wrote to the Earl of Essex.

83. *See* 18 U.S.C. § 2314 (2012). The NSPA has generally been an ineffective tool in dealing with cases of intellectual property theft, particularly when something as intangible as computer code is involved. In *Aleynikov*, the court focused much of its analysis on the statute's use of the terms, "goods, wares, merchandise," which cannot easily be applied to something as abstract as intellectual property. *Aleynikov I*, 785 F. Supp. 2d. at 61.

the EEA.[84] Aleynikov argued that Goldman's HFT system was "a secret trading system that was developed for Goldman's internal use and for its' [sic] sole benefit."[85]

The Southern District of New York disagreed, denying Aleynikov's motion to dismiss and holding that the HFT code was a "good," "ware," or "merchandise" under the NSPA, based primarily on the fact that an illicit market for such code exists.[86] It further held that "the sole purpose for which Goldman purchased, developed, and modified the computer programs that comprise the Trading System was to engage in interstate and foreign commerce."[87] Since the system allowed Goldman to trade on national and international exchanges, the court reasoned, it was clearly a product produced for the purpose of interstate or foreign commerce and therefore subject to the EEA.[88]

### C. COURT OF APPEALS FOR THE SECOND CIRCUIT

The Second Circuit took a more nuanced approach to construing both the NSPA and the EEA.[89] With regard to the NSPA, the court relied heavily on *Dowling v. U.S.*, a Supreme Court opinion in a "bootleg records" case from the mid-1980s.[90] There the Court noted that federal crimes are "solely creatures of statute," and that a federal indictment may be challenged if it fails to allege a crime that falls within the terms of the statute.[91] The circuit court noted that statutory construction should begin with the assumption that the ordinary meaning of the words used adequately expresses the legislative purpose.[92] Quoting *U.S. v. Bottone*, the court took the notion of a tangible good to its extreme and concluded that the NSPA "would presumably not extend to the case where a carefully guarded secret formula was memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed."[93] In short, common sense dictates that some tangible property must be stolen in order to invoke the NSPA. Since Aleynikov conducted his illicit business virtually by posting files

84. *Aleynikov I*, 785 F. Supp. 2d. at 60.
85. *Id.*
86. *Id.* at 61.
87. *Id.* at 60–61.
88. *Id.* at 61.
89. *See Aleynikov II*, 676 F.3d 71, 75–76 (2d Cir. 2012).
90. *Id.*; *see* Dowling v. U.S., 473 U.S. 207, 207 (1985).
91. *Aleynikov II*, 676 F.3d at 75 (quoting Dowling v. U.S., 473 U.S. at 213).
92. *Id.*
93. *Id.* at 77.

via file transfer protocol (and never stole so much as a thumb drive to transport the HFT code), no tangible property had been converted.[94]

With regard to construction of the term "a product produced for or placed in interstate or foreign commerce," the court first looked to the legislative history of the EEA, noting that the key phrase was not included in § 1831.[95] The court cited *Russello*, stating, "[w]here Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion."[96] Thus, the court opined that the requirement that products be "produced for" or "placed in" commerce must be read as terms of limitation.[97] The court further noted that the term in question was not included in the original Senate bill, a fact the court held to be an indication that the words of limitation were very deliberately placed in the act.[98]

The Second Circuit then took the district court to task for its overly broad interpretation of "produced for . . . interstate or foreign commerce," arguing that such phrases should not be construed "in a vacuum."[99] Interestingly, the court noted that the EEA was enacted the year after *U.S. v. Lopez*, a case that turned on the Supreme Court's construction of the term "substantially affected interstate commerce."[100] The temporal proximity to this landmark case was a clear indication, the court reasoned, that the drafters of the EEA intentionally avoided using language that would invoke the "outer limit of Congress's regulatory authority."[101]

Using this bit of legislative history and statutory construction as a backdrop, the court held that Goldman's HFT system was neither "produced for" nor "placed in" interstate or foreign commerce.[102] Goldman had no intention to sell or license the system, and it went to great lengths to maintain its secrecy. Since the HFT system itself never entered commerce, the court reasoned, theft of its source code did not rise to the level of an offense under

94. *Id.*
95. *Id.* at 79.
96. *Id.* at 79 (quoting Russello v. U.S., 464 U.S. 16, 23 (1983)).
97. *Id.* at 79–81.
98. *Id.*
99. *Id.* at 80.
100. *Id.* at 81 (quoting U.S. v. Lopez, 514 U.S. 549, 558–59 (1995)).
101. *Id.* at 81–82.
102. *Id.* at 82.

the EEA.[103] With that, the Second Circuit reversed the district court's judgment without remand.[104]

### D. ANOTHER BITE AT THE APPLE: STATE CHARGES

Aleynikov's legal woes did not end when the Second Circuit reversed his conviction. On August 9, 2012, Aleynikov was arrested and charged under two New York Penal Laws—both class E felonies punishable by jail sentences of two to five years.[105] New York Penal Law Article 156 contains multiple computer-related offenses covering a variety of causes of action including fraud, trespass, and tampering.[106] Enacted in 1986 to combat the "frightening spectre" of rising computer crime, Article 156 marked a significant modernization of New York State's criminal code.[107] Most notably, the statute defined "computer data" and "computer programs" as "property."[108] Section 156.30 criminalizes the reproduction or duplication of any computer data or computer program that results in economic damages in excess of $2,500.[109]

New York Penal Law also includes a technology-related article in section 165.07, which punishes the "unlawful use of secret scientific material."[110] Enacted in 1967, this little-used statute was only examined in detail in a single case involving the theft of a computer program—and even that case predates the Internet age.[111] Section 155.00 of the statute defines "secret scientific material" as anything that "records a scientific or technical process, invention, or formula" that is intended to be unavailable to anyone other than the rightful owner or those who have the consent of the rightful owner—in other words, a trade secret.[112] The use of the term "scientific or technical" evinces a broad interpretation, and seems to include both academic and commercial research and development.

---

103. *Id.*

104. *Id.*

105. *See* Zetter, *supra* note 8; Peter Lattman, *Former Goldman Programmer is Arrested Again*, N.Y. TIMES (Aug. 9, 2012), http://dealbook.nytimes.com/2012/08/09/ex-goldman-programmer-is-arrested-again/; *see also* N.Y. PENAL LAW § 156 (Mckinney 1988).

106. N.Y. PENAL LAW § 156 (Mckinney 1988).

107. *See* People v. Versaggi, 83 N.Y. 2d 123, 128 (N.Y. 1994).

108. *Id.*

109. N.Y. PENAL LAW § 156.30 (criminalizing the "[u]nlawful duplication of computer related materials in the first degree).

110. *Id.* § 165.07.

111. *See* People v. Russo, 131 Misc. 2d 677 (N.Y. 1986).

112. N.Y. PENAL LAW § 155.

On September 12, 2012, Aleynikov pled not guilty to the New York State charges, rejecting a plea deal that specified no jail time.[113] Aleynikov's lawyer warned the judge that he would move to dismiss the case, citing double jeopardy and claiming that state prosecutors had "no sense of decency."[114] Though withstanding a second trial for essentially the same acts smacks of double jeopardy, the assertion that the Second Circuit's dismissal constitutes full adjudication of the matter of Aleynikov's trade secret thievery directly contradicts the anti-preemption language of the EEA.[115]

## III. THE THEFT OF TRADE SECRETS CLARIFICATION ACT OF 2012

On November 27, 2012, with little fanfare, Senator Patrick Leahy[116] (D-VT) introduced the Theft of Trade Secrets Clarification Act of 2012 to the Senate.[117] The Act itself is quite brief, and declares simply:

> Section 1832(a) of title 18, United States Code, is amended in the matter preceding paragraph (1), by striking "or included in a product that is produced for or placed in" and inserting "a product or service used in or intended for use in".[118]

Senator Leahy's address focused on criticism of the *Aleynikov* reversal, and emphasized the need to help "American companies . . . protect the products they work so hard to develop."[119] At Senator Leahy's urging, the Senate passed this "commonsense legislation" without debate or dissent.

---

113. *See* Joseph Ax, *Ex-Goldman Programmer Rejects Plea Deal with NY – Lawyer*, THOMSON REUTERS (Sept. 27, 2012), http://newsandinsight.thomsonreuters.com/Legal/News/2012/09_-_September/Ex-Goldman_programmer_rejects_plea_deal_with_NY_-_lawyer/.

114. *Id.*

115. *See infra* Section IV.B (providing a detailed discussion of preemption issues surrounding the EEA); *see also* U.S. v. Lanza 260 U.S. 377 (1922) (holding that the Fifth Amendment prohibition of double jeopardy applies only to second prosecutions for the same offense under the authority of the federal government).

116. Senator Leahy is no stranger to intellectual property reform; the Leahy-Smith America Invents Act (AIA)—the biggest overhaul of the U.S. patent system since 1952—bears his name.

117. 158 Cong. Rec. S6878-03, 2012 WL 5932548 (2012) (statement of Sen. Leahy).

118. Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat 1627 (2012).

119. 158 Cong. Rec. S6878-03, 2012 WL 5932548 (statement of Sen. Leahy). Interestingly, Senator Leahy's address appears to conflate the notion of interstate misappropriation with interstate commerce, noting that the Second Circuit felt that Aleynikov's theft did not satisfy the interstate commerce prong of the EEA "even though the defendant had copied the stolen code from his office in New York to a server in Germany; downloaded the code to his home computer in New Jersey; then flew to his new job in Illinois with the stolen source code in his possession . . . ." *Id.* This is an honest

In the House of Representatives, Representative Lamar Smith (R-TX)[120] introduced the Act, also focusing on the "dangerous loophole" revealed by the Second Circuit in *Aleynikov*.[121] Interestingly, rather than casting blame on the Second Circuit for its controversial decision, Representative Smith asked that the House "take action in response to the Second Circuit's call and ensure that we have appropriately adapted the scope of the EEA to the digital age."[122] Representative Jackson Lee (D-TX) echoed the sentiment, advocating protection for "proprietary software to be used internally" that is not part of a "commercial end product."[123] Though removing the confusing "product produced for or placed in" language and acknowledging services as well as products elevated the EEA beyond its past tendencies toward vagueness, two issues still remain: (1) the Second Circuit has yet to decide the fate of Samarth Agrawal, who was convicted under the "old" EEA, and (2) the persistence of an explicit lack of preemption.

### A. POTENTIAL CONFUSION IN THE SECOND CIRCUIT: *U.S. V. AGRAWAL*

The case of *U.S. v. Agrawal* presents a controversial companion piece to the catch-and-release case of *Aleynikov*.[124] The fact pattern is eerily similar to that of *Aleynikov*. Like Sergey Aleynikov, Samarth Agrawal was a programmer at a large financial services corporation who allegedly stole code for an HFT system with the intent of using that code to build an electronic trading algorithm for a start-up company.[125] Arrested in his New Jersey apartment on April 19, 2010—nine months after the FBI arrested Aleynikov—he was also tried and convicted in the Southern District of New York[126] and appealed his

misstatement, and one that is illustrative of the fact that the borderless nature of the Internet makes virtually all online activity—including commerce—an interstate affair.

120. Representative Smith, along with Senator Leahy, is the namesake of the Leahy-Smith America Invents Act ("AIA").

121. 158 Cong. Rec. H00000-52, 2012 WL 6605649 (statement of Rep. Smith).

122. *Id.* (statement of Rep. Jackson Lee).

123. *Id.* Representative Jackson Lee, like Senator Leahy, conflated interstate conversion with interstate commerce during her address. Again, this is an honest mistake that underlines the lack of geographic boundaries in the Internet age.

124. *See* Bill Singer, *No Foolish Consistency in Agrawal and Aleynikov But One Hell of a Stunning Reversal*, FORBES (Feb. 21, 2012), http://www.forbes.com/sites/billsinger/2012/02/21/no-foolish-consistency-in-agrawal-and-aleynikov-but-one-hell-of-a-stunning-reversal/.

125. Agrawal was employed by Société Générale, a large European bank with a significant U.S. presence. *Id.*

126. Agrawal's sentence of thirty-six months was lenient compared to Aleynikov's ninety-seven months. Where Aleynikov planned his theft for months in advance, Agrawal simply printed out code, placed it in his backpack, and took it home. The court reasoned that Agrawal's lack of premeditation warranted a sentence significantly lower than the Guidelines range of 97–121 months, whereas Aleynikov's behavior warranted a sentence within the Guidelines. In truth, Agrawal was a cooperative defendant who testified at trial

cased to the Second Circuit. Agrawal also argued that the code he stole was not a "good" under the NSPA, and that the HFT system was not "produced for or placed in interstate or foreign commerce" as defined by the "old" EEA.[127]

During oral arguments, the Second Circuit was quick to point out that Agrawal had printed out the stolen code, rendering it utterly tangible and therefore potentially subject to the NSPA.[128] This notion is both intuitive and comically antiquated—"tangible" code printed on a page is completely bereft of its inherent utility, whereas "intangible" code within a computer becomes dynamic and functional.[129] Interestingly, the court also expressed apprehension toward Agrawal's argument that the HFT system was not a product subject to the "old" EEA, noting that the jury instructions in the trial indicated that the source code was designed to help trade stocks.[130] This is, of course, not substantially different than the argument set forth in the *Aleynikov* trial. In *Aleynikov*, however, the Second Circuit went to great lengths to construe the EEA in such a manner as to dismiss the notion that HFT systems are "produced for or placed in interstate or foreign commerce." With the passage of the TTSCA, however, it will be difficult for Agrawal to argue that HFT code is not "a product or service used in or intended for use in" domestic commerce. This note addresses the complexities of Agrawal's situation under the revised statute in Section IV.B.

owned up to his actions. Aleynikov never testified. *See* Government Sentencing Memorandum, *Aleynikov I*, 785 F. Supp. 2d 46 (S.D.N.Y 2011) WL 1002237.

127. *See* Supplemental Reply Brief for Defendant, U.S. v. Agrawal, No. 11-1074, 2012 WL 1899803 (2d Cir. filed Dec. 30, 2011).

128. *See Ex-SocGen Trader: Taking of Bank Code Not a Crime*, REUTERS (June 21, 2012), http://in.reuters.com/article/2012/06/21/socgen-agrawal-idINL1E8HJ5RK20120621/. Federal law applied in this case only because Agrawal transported printouts of HFT code across state lines to his New Jersey apartment.

129. *See Aleynikov I*, 737 F. Supp. 2d 173, 188–89 (S.D.N.Y. 2010). The court noted that

> [w]hile *Bottone* concerned physical copies of stolen documents containing trade secrets, rather than electronic copies, such a distinction is of no practical significance given today's economic and technological realities. Indeed, it would be absurd if an individual could skirt the statute simply by making an electronic copy of confidential business information, rather than a physical copy, and transport it across state lines using, for instance, a laptop, CD–ROM, or flash drive.

*Id.*

130. *Ex-SocGen Trader: Taking of Bank Code Not a Crime*, *supra* note 128.

### B. A DANGEROUS LACK OF PREEMPTION

Section 1838 of the EEA states:

> This chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret . . . .[131]

In short, there is no federal preemption where the EEA is invoked. This collides with the uncomfortable fact that most states have enacted their own criminal trade secret misappropriation laws.[132] For this reason, it is neither uncommon nor prohibited for a defendant to escape conviction under the EEA only to be charged with similar state causes of action.[133]

In the Internet age, state law is simply insufficient to handle technology whose wide-ranging nature defies traditional geographic jurisdiction. Justice Brandeis once observed, "a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[134] However, the Internet stretches the limits of these "laboratories" with its non-linear, borderless ubiquity.[135] The notion that states can experiment with regulatory policies without adversely affecting activities outside their jurisdiction is in direct conflict with an online world whose access is unlimited by the bounds of geographic jurisdiction.[136] Most substantial Internet activities are, in fact, subject to liability and personal jurisdiction in most or all states.[137]

In spite of the ineffectiveness and inappropriateness of state laws in matters of Internet technology, and in spite of Representative Smith's stated goal of adapting "the scope of the EEA to the digital age,"[138] the TTSCA did nothing to remedy the EEA's explicit lack of preemption. The little legislative history that exists does not indicate that preemption was ever discussed during the drafting of the TTSCA. Ultimately, Congress passed up an opportunity to revise § 1838 of the EEA to address its lack of harmony with the needs of the digital age.

---

131. 18 U.S.C. § 1838 (2012).

132. *See supra* Part I.

133. *See* Zetter, *supra* note 8.

134. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932).

135. *See generally* Peter S. Menell, *Regulating "Spyware": The Limitations of State "Laboratories" and the Case for Federal Preemption of State Unfair Competition Laws*, 20 BERKELEY TECH. L.J. 1363, 1375 (2005).

136. *See id.*

137. *See id.*

138. 158 Cong. Rec. H00000-52, 2012 WL 6605649 (2012) (statement of Rep. Smith).

## IV. ANALYSIS

### A. DID THE TTSCA FIX THE EEA?

One of the stated goals of the TTSCA was to "take action in response to the Second Circuit's call" in the *Aleynikov* decision.[139] Disturbed by the narrowness of the holding in *Aleynikov*, Congress sought to broaden the language in the statute to avoid ambiguity.[140] The result is a statute that is purpose-built to convict Sergey Aleynikov—and it almost certainly would have commanded and sustained Aleynikov's conviction. But will the "new" EEA result in more convictions? Is this a significant step in the right direction?

Only time will tell. The "old" EEA saw few prosecutions, and even fewer convictions. This lack of use was largely the result of its former lack of clarity. In theory, the changes brought about by the TTSCA should attract the attention of prosecutors who might have shied away from it in years past. However, the lack of publicity and fanfare surrounding the TTSCA does not inspire confidence. Lawmakers submitted the TTSCA to the Senate the Tuesday after Thanksgiving, and President Obama signed it into law the Friday after Christmas—which also happened to be the last Friday of 2012.[141] Quietly rushing the statute through the system during the holiday season is hardly a recipe for enhanced notice. Nevertheless, prosecutors at the Department of Justice were likely paying close attention, and it is their actions that will determine the ultimate success of the "new" EEA.

### B. SHOULD AGRAWAL BE HELD TO A HIGHER STANDARD?

The purpose-built nature of the "new" EEA is an unfavorable development for Samarth Agrawal. The fact pattern in the *Agrawal* case is virtually identical to that in *Aleynikov*. His appeal to the Second Circuit already appeared to be on shaky ground before the TTSCA was signed.[142] And under the revised EEA, it seems almost certain that his conviction will be upheld. But is this a fair outcome? Should *Agrawal* be held to a higher standard than *Aleynikov*?

---

139. *Id.* (statement of Rep. Smith).

140. *Id.* (statement of Rep. Jackson Lee).

141. *See Statement by the Press Secretary on H.J. Res. 122, H.R. 3477, H.R. 3783, H.R. 3870, H.R. 3912, H.R. 5738, H.R. 5837, H.R. 5954, H.R. 6116, H.R. 6223, S. 285, S. 1379, S. 2170, S. 2367, S. 3193, S. 3311, S. 3315, S. 3564, and S. 3642*, THE WHITE HOUSE (Dec. 28, 2012), http://www.whitehouse.gov/the-press-office/2012/12/28/statement-press-secretary-hj-res-122-hr-3477-hr-3783-hr-3870-hr-3912-hr-.

142. *See supra* Section III.A.

*1. Providing Ample Notice*

The Second Circuit's majority opinion in *Aleynikov* closes with a succinct summation of the lack of notice provided by the EEA:

> The conduct found by the jury is conduct that Aleynikov should have known was in breach of his confidentiality obligations to Goldman, and was dishonest in ways that would subject him to sanctions; but he could not have known that it would offend this criminal law or this particular sovereign.[143]

The message is clear: Aleynikov violated his employee agreement with Goldman and behaved dishonestly, but his conduct would not normally rise past the level of civil sanctions. Goldman, like any multi-national financial institution, has strict confidentiality policies that forbid employees from disclosing the company's proprietary secrets during the course of their employment. It further prohibits any use of such proprietary information (such as the source code stolen by Aleynikov) once employment terminates. Under typical circumstances, upon discovering Aleynikov's breach of his employment agreement, Goldman's sole legal cause of action would be to fire Aleynikov and sue him under civil law. Such a suit would likely involve an injunction and damages, and would lack any criminal element.

But the fact remains that a federal criminal statute prohibiting trade secret theft did exist at the time that Aleynikov and Agrawal committed their misdeeds. Then why has the EEA done a historically poor job of putting alleged misappropriators on notice? The answer lies primarily in the statute's ambiguity. Prosecutors, faced with a vaguely worded statute that might or might not apply to certain fact patterns, have shied away from using the "old" EEA.[144] The dearth of convictions under the EEA is evidence of this trend.[145] And with little jurisprudence to draw from—and very little public knowledge of the EEA—potential thieves like Aleynikov and Agrawal might not realize that their actions are putting them in the crosshairs of federal

143. *Aleynikov II*, 676 F.3d 71, 82 (2d Cir. 2012).

144. *See* R. Mark Halligan, *Protection of U.S. Trade Secret Assets: Critical Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL. PROP. L. 656, 667 (2008) ("Since the enactment of the EEA, there have been less than sixty prosecutions, mainly section 1832 prosecutions. Most of these prosecutions were filed in the Northern District of California . . . . Justice Department statistics confirm that approximately 80% of the eighty six federal judicial districts nationwide have had no EEA prosecutions." (internal citations omitted)).

145. *See* Susan W. Brenner & Anthony C. Crescenzi, *State Sponsored Crime: The Futility of the Economic Espionage Act*, 28 HOUS. J. INT'L L. 389, 432 (2006) (stating that as of 2006, there have been forty-seven people prosecuted in thirty-four cases under the Economic Espionage Act).

criminal law. While this does not excuse their actions, it points out the possibility that they "could not have known that it would offend this criminal law or this particular sovereign."[146]

The passage of the TTSCA does little to alleviate this lack of notice, though it does provide clearer language for future thieves to heed. There is little doubt that Aleynikov and Agrawal knew that the HFT code they were stealing was proprietary, and that it was "a product or service used in or intended for use in" commerce. Still, given the lack of fanfare surrounding the passage of the TTSCA discussed in Section IV.A, *supra*, it seems unsafe to assume that trade secret thieves are any better informed of the law now than they were under the "old" EEA.

*2. The TTSCA and the* Ex Post Facto *Clause*

Article I, Section 9 of the U.S. Constitution declares, "No Bill of Attainder or *ex post facto* Law shall be passed."[147] In 1798, the Supreme Court of the United States ruled that an ex post facto law was one that "makes an action, done before the passing of the law, and which was innocent when done, criminal; and punishes such action."[148] In *Weaver v. Graham*, the Supreme Court held that two factors must be met in order for a criminal law to be considered in violation of the Ex Post Facto Clause: (1) it must apply to events that happened before the enactment of the statute, and (2) it must disadvantage the offender.[149] The Court explained the rationale behind enforcement of the clause in *Beazell v. Ohio*:

> The constitutional prohibition and the judicial interpretation of it rest upon the notion that laws, whatever their form, which purport to make innocent acts criminal after the event, or to aggravate an offense, are harsh and oppressive, and that the criminal quality attributable to an act, either by the *legal definition of the offense* or by the nature or amount of the punishment imposed for its

146. *Aleynikov II*, 676 F.3d at 82.

147. U.S. CONST., art. I, § 9, cl. 3 (emphasis added).

148. Calder v. Bull, 3 U.S. 386, 390 (1798). Describing ex post facto laws, Chief Justice Marshall wrote,

> With very few exceptions, the advocates of such laws were stimulated by ambition, or personal resentment, and vindictive malice. To prevent such, and similar, acts of violence and injustice, I believe, the Federal and State Legislatures, were prohibited from passing any bill of attainder, or any ex post facto law.

*Id.* at 389. Though the enactment of the TTSCA lacks any element of "personal resentment, and vindictive malice," its application in *Agrawal* would nevertheless be retrospective and arguably unconstitutional.

149. Weaver v. Graham, 450 U.S. 24, 29 (1981).

> commission, should not be altered by legislative enactment, after the fact, to the disadvantage of the accused.[150]

In other words, it would be unfair to punish an offender for an act that was not an offense when it was committed.

When Samarth Agrawal committed his act of thievery, the "old" EEA was still in effect.[151] That version contained the controversial phrase, "product produced for or placed in interstate or foreign commerce." The *Aleynikov* court held that the HFT code was incompatible with that phrase, reversing his conviction—and inspiring the enactment of the TTSCA. In *Agrawal*, the misappropriated trade secrets in question also took the form of HFT code. In theory, the Second Circuit established a precedent in *Aleynikov* that should be followed by the court in *Agrawal*. The *Aleynikov* court ruled, in essence, that the theft of HFT code was "innocent when done"—not a criminal act under the "old" EEA at the time it occurred. However, as discussed in Section III.A, *supra*, the *Agrawal* court expressed reluctance to follow *Aleynikov* during oral arguments, and left the door open to a contrary holding. Intra-circuit splits are not uncommon, and it would not be unheard of for the Second Circuit to find a way to distinguish *Agrawal* from *Aleynikov*.

The passage of the TTSCA adds a new wrinkle to the *Agrawal* situation. The language of the TTSCA was crafted in response to *Aleynikov*. Since *Agrawal's* fact pattern is virtually identical, it is highly probable that Agrawal's conviction would be upheld under the "new" EEA. But if the Second Circuit cites the "new" EEA and upholds Agrawal's conviction, would that amount to a violation of the *Ex Post Facto* Clause? After all, the TTSCA did alter the "legal definition of the offense" as admonished in *Beazell v. Ohio*.

However, it is unlikely that the Second Circuit will need to cite the "new" EEA, as it has already expressed doubt that *Agrawal* should be reversed under the "old" EEA. It is more likely that the court will simply refuse to follow *Aleynikov* and submit a distinguishing opinion. In that event, Agrawal could appeal to the Supreme Court to grant certiorari and try to force a reversal by way of *Aleynikov's* precedent. That route seems both remote and moot, as the Court seems unlikely to get involved in the interpretation of a recently modified trade secret misappropriation criminal statute. Thus, Samarth Agrawal's hope for a reversal appears to be hamstrung by poor

150. Beazell v. Ohio, 269 U.S. 167, 170 (1925) (emphasis added).

151. President Obama signed the TTSCA into law on December 28, 2012, more than three years after Agrawal's alleged misdeeds. Though the "old" EEA was rarely invoked, cases involving trade secret misappropriation that occurred prior to December 28, 2012, might yet be brought to trial.

timing, a controversial holding in *Aleynikov*, and an efficient response from Congress.

### C. IS FEDERAL PREEMPTION NECESSARY?

Perhaps the most disturbing feature of the *Aleynikov* saga is that the final chapter remains unwritten. While the Second Circuit reversed his conviction under the EEA, the State of New York awaits its opportunity to convict Aleynikov. The lack of federal preemption under the EEA is troubling in that it clouds the fate of thieves like Aleynikov. HFT is an Internet activity, and the HFT code that Aleynikov stole performs its trading tasks within a virtually ubiquitous electronic world. The facts in *Aleynikov* paint a complex picture: Russian-born programmer steals code from a computer system in New York, uploads it to a server housed in Germany, and delivers to his new employer in Chicago. While New York State law might apply to Aleynikov's theft, so might Illinois law. Depending on the complexity of a case of trade secret theft, many states and their respective laws might be involved. In those cases, the legal environment engendered by the Internet would create a situation where the laws of the most restrictive state would rule the day.[152]

The ubiquity of the Internet begs for something less provincial than state laws to regulate its activities.[153] In the context of cases like *Aleynikov*, state law is simply too varied and inconsistent. Furthermore, subjecting people like Aleynikov to the laws of dozens of states creates a confusing web of conflicting standards and punishments. Unfortunately, this web of confusion is further complicated by the fact that the EEA expressly states that it does not preempt any state laws.

Why would the EEA include such explicit rejection of its own powers of preemption? Perhaps because, as noted in Part I, *supra*, trade secret misappropriation has long been the province of state civil causes of action. But the EEA goes a step further and specifies that it preempts no *criminal* laws, either. Perhaps Congress did not wish to interfere with laws regarding intrastate trade secret misappropriation. However, the EEA explicitly relates to "*interstate* or foreign commerce," and should not preempt state causes of action that would not otherwise fall under the umbrella of the EEA. The EEA is the product of modern concerns, and should take into account the ubiquity of the Internet and its role in most contemporary acts of trade secret misappropriation. Congress would do well to consider the modern nature of the type of domestic trade secret theft the EEA purports to address.

152. *See* Menell, *supra* note 135, at 1375–76.
153. *See id.* at 1415–18.

## V. CONCLUSION

The TTSCA directly addresses the request of Judge Calabresi's concurring opinion in *Aleynikov* that "Congress will return to the issue and state, in appropriate language, what I believe they meant to make criminal in the EEA."[154] However, its passage leaves the *Agrawal* court in an uncomfortable state of limbo, and the issue of preemption remains unresolved. Until the Second Circuit provides a satisfactory holding in the *Agrawal* case, Congress should keep a watchful eye on the EEA and the courts that enforce it. In the meantime, Congress should seriously consider striking the explicit lack of preemption from § 1838 of the EEA. If the TTSCA has truly cleaned up the language of the EEA in a manner that will empower prosecutors to enforce it, then Congress should not allow state laws to be used as safety nets to catch those thieves who evade punishment through "dangerous loopholes" in federal law.

154. *Aleynikov II*, 676 F.3d 71, 83 (2d Cir. 2012).