Journal of Law & Commerce
Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

WHEN ACTUALLY READING THE LETTER OF THE LAW DOES MORE HARM THAN GOOD: *U.S. v. ALEYNIKOV*, TRADING ALGORITHMS, AND STATUTORY GAPS

Patrick Holland

WHEN ACTUALLY READING THE LETTER OF THE LAW DOES MORE HARM THAN GOOD: *U.S. v. ALEYNIKOV*, TRADING ALGORITHMS, AND STATUTORY GAPS

Patrick Holland[*]

I. INTRODUCTION—FRAMING THE ISSUES

In *United States v. Aleynikov* the Second Circuit first held that Goldman Sachs' computer source code used in high frequency trading (HFT) models did not fall under the statutory definition of a stolen "good," "ware," or "merchandise" under the National Stolen Property Act (NSPA).[1] Therefore the defendant's theft of the code did not violate the Economic Espionage Act (EEA).[2] Source code begins simply as human language.[3] It is composed of readable instructions physically typed in by a computer programmer, which are then translated into functioning code through a process called assembly.[4] *Aleynikov*'s holding sets the precarious precedent of acknowledging the tangible value of an intangible good, while simultaneously refusing to extend protection to that very good.[5] This contradiction highlights the inherent definitional flaws embedded within both the NSPA and the EEA. Both statutes possess an inability to serve as viable options for the curtailment of information technology theft. Author Matthew Allen posits that in an information technology driven marketplace non-tangible innovations are not only a sign of power, but are often the most valuable asset a company possesses.[6] *Aleynikov* illustrates the

---

[*] J.D., University of Pittsburgh School of Law, 2013.

[1] United States v. Aleynikov, 676 F.3d 71, 77 (2d Cir. 2012).

[2] *Aleynikov*, 676 F.3d at 82.

[3] Deborah F. Buckman, *Copyright Protection of Computer Programs*, 180 A.L.R. FED. 1 (2002).

[4] *Id.*

[5] *Aleynikov*, 676 F.3d at 82.

[6] Matthew P. Allen, *High Stakes Sleuthing: Handling Corporate and IP Espionage Matters in the Information Age*, 2012 WL 1670120 at 20 (2012).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

disconnect between the NSPA and the EEA regarding the protection afforded to intangible goods.

Part II of this note will give a general overview and evaluation of the Second Circuit's ruling in *Aleynikov*. This will give us our baseline rules that will drive forward our overall analysis. Part III will take on a historical perspective. It will track the evolution of different methods of intellectual property protection that have been applied to source code in the past. Part IV and V will dive into a substantive analysis of both the National Stolen Property Act and the Economic Espionage Act. An understanding of how these two statutes function, and have been interpreted by courts, will arm us with a better sense of how they can be improved to better protect source code. Finally in Part VI, this note will reach into the past to explain the importance of equitable judicial interpretation. Most importantly, this note will suggest the application of an enduring judicial maxim that could have counteracted the flaws in Second Circuit's decision.

A proper definition for the misappropriated source code in *Aleynikov* is especially important given the rise of high frequency trading systems on Wall Street.[7] Specially designed financial trading algorithms are comprised of source code that allows the system to decide aspects of trading order, timing, price, and the quantity to buy or sell, all without the need for human intervention.[8] The codes animating these trading algorithms are some of the most valuable pieces of property that a financial institution can own.[9] The lack of understanding that these codes are indeed protectable "goods" is worrisome in an industry that is so dependent on the use of cutting edge technology.[10]

In an attempt to remedy this issue, both the NSPA and the EEA need to be updated to reflect intangible source code as a protectable good. Different modes of intellectual property allow for source code's protection, so why should there be a statutory variation to muddy the already complex

---

[7] *See HFT Review*, HIGH FREQUENCY TRADING & ALGORITHMIC TRADING, *available at* http://www.hftreview.com/pg/blog/mike/read/5307/high-frequency-trading-algorithmic-trading/ (accessed Feb. 15, 2010) [hereinafter *HFT Review*].

[8] 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 (2011).

[9] *See* Allen, *supra* note 6, at 20.

[10] *See HFT Review*, *supra* note 7, *available at* http://www.hftreview.com/pg/blog/mike/read/5307/high-frequency-trading-algorithmic-trading/ (accessed Feb. 15, 2010).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

waters? Under current judicial holdings, the NSPA, and by extension the EEA, have been precluded "from becoming a potential recourse against source code theft."[11] The overly narrow definition of a "good" contained in the NSPA and the EEA, as highlighted by *Aleynikov*, calls for a legislative makeover tailored to expand the definition of a "good" to encompass source code.

II. *UNITED STATES V. ALEYNIKOV*—OVERVIEW AND ANALYSIS

Sergey Aleynikov was a Goldman Sachs employee tasked with developing computer source code that could be used in their high frequency trading (HFT) system.[12] Specifically, Aleynikov's code would support infrastructure programs that used algorithms to determine which trades to make and when to do so.[13] A HFT system is capable of making large amounts of trades in fractions of a second, on the basis of market information provided to it by an algorithm that recognizes key market shifts.[14] Goldman so valued this information that it required employees to sign confidentiality agreements and refused any licensing overtures.[15]

In 2009, Aleynikov accepted a position with a Chicago-based start-up (Teza Technologies) that was interested in developing its own HFT system.[16] Teza gave Aleynikov six months to develop a HFT trading system, which usually take years for a team of programmers to construct.[17] On his last day at Goldman, Aleynikov encrypted and uploaded to a third party server 500,000 lines of source code that were used in Goldman's HFT system.[18] Specifically, the uploaded code contained key pieces that were used in Goldman's trading algorithms and market data connectivity evaluations.[19] After transferring the code from the third-party server to his

---

[11] Tamara J. Wayland, *Computer Technology—The National Stolen Property Act and Its Applicability to Property Rights in Computer Source Code—Do Rights Exist?*—United States v. Brown*, 925 F.2d 1301 (10th Cir. 1991)*, 11 TEMP. ENVTL. L. & TECH. J. 155, 169 (1992).

[12] *Aleynikov*, 676 F.3d at 73.

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.* at 74.

[17] *Id.*

[18] *Aleynikov*, 676 F.3d at 74.

[19] *Id.*

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

personal flash drive, Aleynikov traveled to Chicago claiming to have the needed tools to begin HFT construction.[20] Upon returning home the following day, Aleynikov was arrested for violating the Economic Espionage Act (EEA) by illegally converting a trade secret, with the intent to economically benefit another party.[21] He was subsequently charged with also violating the National Stolen Property Act (NSPA), which makes it a crime to "transport, transmit, or transfer in interstate or foreign commerce any goods, wares, merchandise, securities, or money of the value of $5,000 or more, knowing the same to have been stolen, converted, or taken by fraud."[22]

A. The Second Circuit's Ruling—The NSPA Argument

In regards to the NSPA-based claim, the court questioned whether "the source code that Aleynikov uploaded to a server in Germany, then downloaded to his computer devices in New Jersey, and later transferred to Illinois, constituted stolen 'goods'. . . ."[23] The Second Circuit reasoned that in order to constitute a violation under the NSAP a good must be stolen, and that good must be tangible property taken from its rightful owner.[24] The Second Circuit adopted a precedent articulated by the Supreme Court's ruling in *Dowling v. United States*, 473 U.S. 207 (1985) that concluded that a "computer program itself is intangible intellectual property . . . it alone cannot constitute goods, wares, merchandise, securities or moneys which have been stolen . . . for purposes of the NSPA."[25] Therefore, since the source code stolen by Aleynikov from Goldman Sachs was not tangible in nature, he could not be held liable for the theft of a "good" under the NSAP.

[20] *Id.*
[21] *Aleynikov*, 676 F.3d at 74; Economic Espionage Act, 18 U.S.C. § 1832(a) (2012).
[22] *Aleynikov*, 676 F.3d at 74; National Stolen Property Act, 18 U.S.C. § 2314 (2013).
[23] *Aleynikov*, 676 F.3d at 75.
[24] *Id.* at 76–77.
[25] *Id.* at 77; *see also* Dowling v. United States, 473 U.S. 207 (1985).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

B. The Second Circuit's Ruling—The EEA Argument

Aleynikov was charged with violating the second substantive provision contained in the EEA. This requires that the stolen product be "produced for" or "placed in" interstate or foreign commerce.[26] The Second Circuit ruled that Goldman's source code was neither "produced for" nor "placed in" interstate or foreign commerce, despite moving from New York, to New Jersey, and then to Chicago.[27] The court focused on the code itself rather than Aleynikov's actions with it. Since the code was highly secretive and only available to Goldman, the court concluded that it was never meant to enter or pass through commerce.[28] The HFT system at its inception was designed to solely benefit Goldman. Therefore, Aleynikov's source code theft, which was used for the system's function, was not a violation of the EEA's requirement that the HFT system be "produced for" or "placed in" interstate or foreign commerce.[29]

C. Judge Calabresi's Concurrence: Illustrating the Problems Ahead

While not outwardly dissenting with the Second Circuit's strict textual rulings, Judge Calabresi's separate opinion highlights the possible difficulties that a decision of this nature can create. He stressed the importance of reading the law within the context of its purported goal.[30] The EEA was a legislative response to rulings handed down by the U.S. Supreme Court and the Tenth Circuit. Judge Calabresi notes that, '[w]hile the legislative history can be read to create some ambiguity as to how broad a reach the EEA was designed to have, it is hard for me to conclude that Congress, in this law, actually meant to exempt the kind of behavior in which Aleynikov engaged."[31] *Aleynikov* may technically be correct in its reading of the law, but this overly strict ruling is presented in a vacuum, devoid of any context. Judge Calabresi thought this matter to be so important that he urged Congress to return to the issue of the NSPA, in an

[26] 18 U.S.C. § 1832.
[27] *Aleynikov*, 676 F.3d at 82.
[28] *Id.*
[29] *Id.*
[30] *Id.* at 82 (Calabresi, J., concurring).
[31] *Id.* at 83; *see also* H.R. REP. NO. 104-788, at 6 (1996).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

effort to state unequivocally what he believed they meant to make criminal under the EEA.[32]

III. THE EVOLUTION OF INTELLECTUAL PROPERTY PROTECTION AND SOURCE CODE

In his treatise detailing the interplay between the ever-changing fields of technology and the law, Raymond Nimmer notes the inherit difficulty in treating software as a good when its subject matter and relevance are often intangible.[33] Source code's intangible nature may prohibit its inclusion under certain statutory definitions of a "good," but certain forms of intellectual property protection are available to give owners the protection their desire. It is important to understand the evolution of intangible intellectual property, and how our technology-based marketplace is forcing both the legislature and judiciary to reconsider the attributes of a "good."

A. Source Code as a Protectable Trade Secret

The Uniform Trade Secret Act (UTSA) is the current legal framework that 46 states have adopted to harmonize standards and remedies regarding misappropriation of a business' trade secret.[34] It codifies trade secret definitions and remedies that have evolved through the common law. § 1.4 of the UTSA defines "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.[35]

This conjunctive metric can be boiled down to whether the nature of the economically valuable information is confidential, and if so, what were the

---

[32] *Id.* at 83.

[33] Raymond T. Nimmer, *What law governs (goods, services, intangibles)—Goods or intangibles*, LAW COMPUTER TECH. (2012).

[34] *See Uniform Trade Secrets Act*, UNIFORM LAW COMMISSION, *available at* http://uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act.

[35] Uniform Trade Secrets Act § 1.4, *Trade Secret* (1985).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

precautions taken by the owner of said information to maintain its confidentiality? When faced with a trade secret misappropriation claim these two questions are fact intensive inquiries.[36]

For example, Goldman could first assert that the monetary windfall derived from its source code when applied to its trading algorithm was so valuable in the marketplace because it was unknown and coveted by other financial firms. To articulate this, they would present fact-specific information detailing their efforts to maintain the code's secrecy, like the confidentiality agreements signed by their employees. A well plead premise of this nature would possibly allow Goldman to use trade secret law to protect its valuable, but intangible property.[37] On a macro-level, trade secret law is "left to create a balance of interests, which allows the trade secret holder to share information with his employees or others while still maintaining the ownership and competitive advantage of that information in an increasingly information-based economy."[38]

B. Confidentiality Agreements and Restrictive Employment Covenants

Possibly the most used form of source code protection is the deployment of confidentiality clauses in employment contracts that restrict what a current or former employee can disclose to the public or future employers.[39] When the employer has taken the appropriate steps to protect its software or source code through a defined avenue of intellectual property, separate contractual agreements bind the employee into secrecy. The threat of litigation looms for an employee who breaches these contractual provisions. These agreements can be broad or extremely specific in construction.[40]

---

[36] Agency Solutions.Com, LLC v. TriZetto Group, Inc., 819 F. Supp. 2d 1001, 1021 (E.D. Cal. 2011).

[37] *See* Alan J. Tracey, *The Contract In The Trade Secret Ballroom—A Forgotten Dance Partner?*, 16 TEX. INTELL. PROP. L.J. 47, 48 (2007).

[38] *Id.*

[39] Jere M. Webb, *Advantages of Using Confidentiality Agreements*, A PRACTITIONER'S GUIDE TO CONFIDENTIALITY AGREEMENTS, *available at* http://www.stoel.com/Files/ConfidentialityAgreementGuide.pdf.

[40] *See generally* Tracey, *supra* note 37.

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

For example, a former employee could take confidential information *about the software* to his new employer, not the software itself. A broadly stated confidentiality agreement could foreclose disclosure of the source itself and also the information that went into building it. The goal of these restrictive agreements is to protect the parent company from the unauthorized use or disclosure by current or former employees (i.e. those who stand in a "confidential relationship" with the true owner of the information).[41] Author Daniel Friesen highlights nine claims that employers have successfully asserted when their confidential source code has been improperly disclosed in violation of a restrictive covenant: a copyright violation, trade secret theft, breach of contract, breach of fiduciary duty in violation of the ongoing duty of loyalty, tortuous interference of a prospective business advantage, civil conspiracy to injury one's business, fraud, unjust enrichment, and finally common law theft or conversion.[42]

C. Source Code as a Protectable Copyright

The 1980 amendments to the Copyright Act of 1976, specifically includes as protectable subject matter, "computer programs . . . only to the extent that they incorporate authorship in a programmer's original expression of ideas, as distinguished from ideas themselves."[43] The court in *Control Data Systems, Inc. v. Infoware, Inc.*, 903 F. Supp. 1316 (D. Minn. 1995) succinctly illustrates the application of this principal. In *Control Data*, the court held that the copying of 2,000 lines of operating system source code was sufficient to warrant injunctive protection.[44] This stemmed from the defendant building a duplicate computer that allowed customers to use application programs designed specifically to be used on the plaintiff's network.[45]

Copyrightable source code can come into being when a programmer writes a single original line of code; therefore complex code instructions

---

[41] Webb, *supra* note 39.

[42] Daniel Friesen, *Enjoining Former Employees from Taking Software*, 24 COLO. LAW. 1771, 1772 (1995).

[43] Subject Matter and Scope of Copyright, 17 U.S.C. § 101 (1980); *see also* Deborah F. Buckman, *Copyright Protection of Computer Programs*, 180 A.L.R. FED. 1 (2002).

[44] Control Data Systems, Inc. v. Infoware, Inc., 903 F. Supp. 1316 (D. Minn. 1995).

[45] *Control Data Systems, Inc.*, 903 F. Supp. at 1325.

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

can be covered by multiple copyrights given the individual values of each single line.[46] Generally, copyright is a preferred method of protection for the object code that goes into a program (i.e. the actual instructions that control what the computer will do).[47] The source code used to build the object code is usually assigned trade secret distinction.[48] It is important to understand that copyright, as a mode of protection is not foreclosed upon when applied to source code. The Copyright Office regards source code and object code as equivalent for purposes of registration.[49] An important limitation to copyright protection that one must be cognizant of is fair use. Section 107 of the Copyright Act codifies this limitation allowing certain copying of copyrighted material when it is necessary for uncovering basic ideas.[50]

IV. THE NATIONAL STOLEN PROPERTY ACT—A FAILURE TO PROTECT SOURCE CODE

The NSPA is the federal codification of statutes that protect personal property in the U.S. Over the years, courts have been unsure how far of a reach this piece of legislation should have, refusing to extend protection to owners of copyrightable computer programs.[51] The NSPA's scope has been expanded to include less tangible items like geophysical maps and chemical formulas.[52] The question remains why the legislative gap in terms of protection for source code? Overly strict textual interpretation has highlighted an inherent flaw in the legislation that demands immediate attention. Aleynikov's improper copying, and subsequent theft of Goldman's source code, for the benefit of a competitor clearly rings of bad faith on multiple levels. He survived criminal sanctions through the shrewd application of judicial precedents that have read the NSAP in an extremely

[46] Lee A. Hollaar, *Source Code and Object Code*, COPYRIGHT OF COMPUTER PROGRAMS, *available at* http://digital-law-online.info/lpdi1.0/treatise26.html.

[47] *Id.*

[48] *Id.*

[49] *See* United States Copyright Office, *Circular 61*, COPYRIGHT REGISTRATION FOR COMPUTER PROGRAMS, *available at* http://digital-law-online.info/lpdi1.0/treatise26.html.

[50] 17 U.S.C. § 107 (2012).

[51] *See generally* Wayland, *supra* note 11.

[52] *See* United States v. Seagraves, 265 F.2d 876 (3d Cir. 1959); United States v. Greenwald, 479 F.2d 320 (6th Cir. 1973).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

static fashion. The source of this problem can be traced back to the Tenth Circuit's decision in *United States v. Brown*.[53] *Brown* and its progeny's overly strict reading of the NSPA deny the marketability and value of intangible goods, like computer source code, leaving copyright as the predominant method of remedy. This failure ignores the distinction that exists between criminal theft and the infringement upon one's legally protected copyright.[54]

A. United States v. Brown—*The Origin of the Problem*

Defendant Brown, while employed at The Software Link (TSL), was allowed access to a computer program (PC-MOS/386) that permitted advanced microcomputer functions.[55] Brown soon left TSL and became embroiled in an FBI investigation regarding the theft of the PC-MOS/386 source code.[56] After investigation, authorities found hard evidence that Brown had copied and transferred the source code to another person in New Mexico.[57] The U.S. charged Brown with violating 18 U.S.C §§ 2314, 2515 of the NSPA.[58] Both the District Court and the Court of Appeals in applying the Supreme Court's ruling in *Dowling* dismissed Brown's charges because they held "that crimes involving mere copyright infringements do not fall under the ambit of 'physical goods, wares, [or] merchandise' required by section 2314."[59] The issuing facing the Tenth Circuit was whether stolen computer source code could satisfy the "physical" requirement of § 2314, as articulated by *Dowling*.

The government argued that when Brown scrawled pieces of the code onto notebook paper and copied pieces onto a disk that he had satisfied the tangibility requirement in *Dowling*.[60] Moreover, they asserted that Brown knew the secretive nature of the source code by pointing to the fact that employees were not permitted to ever remove it from TSL, and no one

[53] United States v. Brown, 925 F.2d 1301 (10th Cir. 1991).
[54] *See* Wayland, *supra* note 11, at 165–69.
[55] *Brown*, 925 F.2d at 1302.
[56] *Id.* at 1303.
[57] *Id.*
[58] *Id.*
[59] *See* Wayland, *supra* note 11, at 156.
[60] *Brown*, 925 F.2d at 1305–07.

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

outside of TSL even knew of the code's existence.[61] This created a distinction from *Dowling*, which dealt with the reproduction of items that were easily accessible to the public.[62] They reasoned that the secretive nature of the code necessitated a special type of protection under the NSPA. The Tenth Circuit rejected all of these arguments, deciding rather to honor the *Dowling* precedent. They ruled that § 2314 of the NSPA applied only to physical goods, wares, or merchandise; purely intellectual property falls outside of the Act's purview.[63] Brown escaped conviction because the court focused on the source code's inherently intangible nature as a way to disqualify it from NSPA protection. It is this overly narrow reading of the law that has allowed other individuals, like Aleynikov, to escape punishment for their criminal actions.

B. The NSPA—Interpretation and Legislative Intent

The ever-increasing value of source code as a commodity requires that the legislative gaps contained in the NSPA be updated to reflect a more modern interpretation of what constitutes a good or wear. *Brown* and *Aleynikov* rule that because computer source code is intangible, and only becomes tangible when copied onto a hard drive or disk, the code itself is not a good under the NSPA. This formulation is an outmoded differentiation of what a good is in 2013. Some academics have defended the conservative judicial reading of the NSPA claiming that "in the context of computer code, the copyright laws do much to protect the owner where the Act lulls."[64] To counter this, others point to dicta in *United States v. Wright*, 791 F.2d 133 (10th Cir. 1986) that stated the "NSPA has a broad purpose. Congress intended the Act [to] be a deterrent to the commission of interstate crime, and it should be interpreted in light of that intent."[65] It is in this vein that the NSPA should be understood, and therefore expanded to cover the types of illegal activity committed by Aleynikov.

---

[61] *Id.* at 1306.
[62] *Id.*
[63] *Id.* at 1307–09.
[64] Chad A. McGowan, *Stolen Software, Data Files and the National Stolen Property Act*, 8 AUG. S.C. LAW. 38 (1996).
[65] United States v. Wright, 791 F.2d 133, 137 (10th Cir. 1986).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

One could argue that an expansion of the NSPA's definition of a "good" to include goods that are non-physically rendered or intangible is a moot argument when copyright protection for source code is available. This argument does have merit, but its logic is somewhat negated by the increasing dependence on information technology and computer coding. In *United States v. Riggs*, 739 F. Supp. 414 (N.D. Ill. 1990) the court held that the electronic interstate transfer of misappropriated propriety information from 911 text files fell within the scope of the NSPA.[66] The *Riggs* court cautioned "reading a tangibility requirement into the definition of goods, wares, or merchandise might unduly restrict the scope of § 2314, especially in this modern technological age."[67]

The importance of strict judicial readings of the law cannot be understated, but that very legislation itself must be a reflection of changing economic and technological times. While the judiciary has properly applied the tangibility requirements for the NSPA's application in the past, these requirements need to be modified so the NSPA can be used in conjunction with copyright protection as applied to source code. Overly strict judicial readings can be counteracted if Congress enacts "specialized legislation to combat the theft of source code and computer programs rather than modify current copyright law."[68] Adding this arrow to a property owner's quiver will strengthen an owner's ability to protect their valuable computer source code from theft or other criminal activity.

C. Prosecutorial Failure to Charge Aleynikov Under the NSPA?

Perhaps the true burden of responsibility for opening this legislative can of worms can be laid at the feet of the U.S. attorneys that charged Aleynikov under the NSPA. The Act itself clearly states in § 2314 that it will only apply to physical goods, and makes no mention of intangible goods.[69] One possible explanation for the government's actions is overconfidence in the case they were presenting. Aleynikov clearly had stolen highly secretive source code from Goldman and smuggled it to a new

[66] United States v. Riggs, 739 F. Supp. 414, 424 (N.D. Ill. 1990).
[67] *Riggs*, 739 F. Supp. at 421.
[68] *See* Wayland, *supra* note 11, at 169.
[69] 18 U.S.C. § 2314.

employer in Illinois. Prosecutors may have viewed this as an opportunity to present a case that would force the Second Circuit to enlarge the acceptable definition of a "good" under the NSPA. Gambling for a looser definition may have allowed Aleynikov to escape conviction. Since source code did not come under the legislative definition articulated by the NSPA, the EEA was not violated since the good was not "produced for" or "placed in" interstate or foreign commerce.[70] The U.S. attorneys must have been trying for a game changing decision from the Second Circuit that would judicially solidify source code as protectable under the NSPA. There seems to be no other way to color their choice to employ such a risky strategy.

V. ECONOMIC ESPIONAGE ACT—OVERLY NARROW READING OF A GENERAL PROHIBITION?

To add further insult to injury, the U.S. government's EEA claim against Aleynikov was also summarily dismissed. The indictment charged him with violating § 1832(a) of the EEA for the unauthorized taking, copying, or receiving of trade secrets in the domestic context.[71] The EEA's main concern is to combat interstate and foreign economic espionage primarily through the theft of valuable corporate trade secrets.[72] The Act serves to protect trade secrets that are of value to U.S. businesses against the type of actions that Aleynikov and others like him perpetrated. The increased understanding of source code, and how it fits into the greater scheme of a business's infrastructure, has made it easier than ever to steal confidential material.[73] The EEA functions as a safeguard for this type of valuable information.

A. EEA § 1832(a)—A Losing Battle for the Government

The general domestic prohibition in the EEA imposes fines or jail time on anyone who knowingly converts or conspires to convert:

---

[70] *Aleynikov*, 676 F.3d at 78.
[71] 18 U.S.C. § 1832(a).
[72] *See* Tracey, *supra* note 37, at 47–48; 18 U.S.C. § 1832(a).
[73] *Id.*

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

> [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 . . . .[74]

On December 28, 2012, Congress altered the language of § 1832(a) somewhat by inserting "a product or service used in or intended for use in" to replace "or included in a product that is produced for or placed in."[75] The EEA had less established case law than that of the NSPA, so even more emphasis is placed upon a careful reading of the statute and how it is construed. The Second Circuit's reasoning hinges upon it's reading of the two separate, but related, categories contained in § 1832(a): "produced for commerce" and "placed in commerce."[76] It seems counter intuitive that the EEA's main purpose is to protect American businesses from theft of their trade secrets by foreign or domestic entities; when the Second Circuit's reading of the law allows Aleynikov to escape responsibility for the very actions the Act was meant to protect against.[77] It remains to be seen if the legislative modification on December 28, 2012 is sufficient to remedy this issue.

The Second Circuit read a limitation in § 1832(a)'s language that becomes key in the court's reasoning. The limitation is that the misappropriated product must be either "produced for" or "placed in" interstate of foreign commerce.[78] The court notes that this particular language is absent from § 1831's broader foreign-entity prohibition.[79] It is this limitation that the court uses to subvert the true intention of the Act for the sake of a strict textual interpretation. The court explains that products "placed in" commerce have already been introduced into the stream of commerce and have reached the marketplace.[80] Conversely, products that are "produced for" commerce are still being developed prepared fully for

---

[74] 18 U.S.C. § 1832(a).
[75] P.L. 112-236, Dec. 28, 2012.
[76] 18 U.S.C. § 1832(a).
[77] *See generally* Allyson A. McKenzie, United States v. Kai-Lo Hsu*: An Examination of the Confidentiality Provision in the Economic Espionage Act: Is it Suitable to Maintain the Use and Effectiveness of the EEA?*, 25 DEL. J. CORP. L. 309 (2000).
[78] *Aleynikov*, 676 F.3d at 80.
[79] *Id.*
[80] *Id.*

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

consumer consumption.[81] Since Goldman's system was not "produced for" or "placed in" any commerce stream, it fell outside of the EEA's scope. To support this conclusion, the Second Circuit mentions that Goldman had no intentions of ever disclosing this source code to anyone.[82] The secrecy surrounding the code barred it from ever truly entering or passing in commerce to the consumer. Therefore, since Aleynikov's actions revolved around a theft of code that was not "produced for" or "placed in" interstate or foreign commerce, the EEA was inapplicable.[83]

B. Defending the District Court's Interpretation of § 1832(a) of the EEA

Aleynikov's premise for his defense was that Goldman's source code used in their HFT algorithm does not constitute a product produced for or placed in interstate or foreign commerce. This stemmed from the secrecy surrounding the code, which was to be used solely for Goldman's internal benefit.[84] By applying a plain meaning to "produced for" interstate or foreign commerce, the District Court ruled that Goldman's source code was the exact type of product that the EEA was supposed to protect.[85] The court illustrates the interstate nature of the code by pointing out that Goldman would use their trading algorithm to execute high volumes of financial trades in numerous markets around the world.[86] They dismissed Aleynikov's plea to narrowly construe § 1832(a) to cover only tangible consumer products sold in commerce. The District Court avoids the problem warned of in Judge Calabresi's concurrence of reading the EEA in a legislative vacuum. The District Court acknowledged the growing importance of computer source code in financial marketplaces. Pulling from the legislative history surrounding the Act, its becomes clear that Congress intended for the EEA to comprehensively protect trade secrets belonging to U.S. companies, not just the manufacture of tangible consumer products.[87]

---

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] United States v. Aleynikov, 737 F. Supp. 2d 173, 177 (S.D. N.Y. 2010).
[85] *Id.* at 177.
[86] *Id.*
[87] *See* H.R. REP. NO. 104-788, at 4–7 (1996); S. REP. NO. 104-359, at 6–11 (1996).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

One could argue that the District Court's analysis of § 1832 is broader than what the statute intended. This argument may have merit, but it fails to take into account the political, economic, and pragmatic factors that go into an evaluation of the law. These factors cannot be ignored when a judicial opinion is handed down. Changing societal norms and business practices drive both the legislature and the judiciary to protect interests that the populous currently view as important. The issue surrounding Aleynikov, and the EEA's application to his case, may have more to do with the recalibration of legislation, as opposed to flawed judicial reasoning. Bad law will only produce bad results when that law is tested by hard cases like this one. The District Court seemed to be aware of this fact, and changing business norms, when they held that Aleynikov violated § 1832(a). The court recalls a principal espoused by the Supreme Court in *Salinas v. United States*, 522 U.S. 52 (U.S. 1997) that notes, "[n]o rule of construction . . . requires that a penal statute be strained and distorted in order to exclude conduct clearly intended to be within its scope."[88] The Second Circuit's overly technical reading of § 1832(a) of the EEA does just that; denying Goldman's trade secret the protection that the EEA was supposed to provide.

C. The Need for Modifications to Strengthen the EEA

The change to a more global economy, based upon massive amounts of information being transferred at high speeds, necessitates legislation to reflect such a shift. Technological information functions "as currency of the new millennium" and its protection has been equated with our country's national security.[89] The current rule that a business's intangible misappropriated trade secret that is not "placed in" or "produced for" interstate or foreign commerce falls outside the EEA's protection is an untenable position. For example, corporations like Google have been built primarily on intellectual property that is secret to the Google brand. The Second Circuit's ruling in *Aleynikov* pertaining to the EEA is so strictly construed that it disables the Act from being able to satisfy its original

[88] Salinas v. United States, 522 U.S. 52, 59 (U.S. 1997).
[89] *See* Allen, *supra* note 6, at 20.

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

legislative intent.[90] The proper application of legislation requires that its intent be satisfied, while also acknowledging the shifts in a particular field that the legislation was meant to protect.

Circling back to Judge Calabresi's concurrence for the Second Circuit can be especially instructive in our evaluation. While agreeing with the majority "that the text of the EEA is such that it would require stretching to cover Aleynikov's acts," he stresses that law must be read in context to include the entirety of the statute and the "mischief" those statues were enacted to combat.[91] He reasons that the EEA was a legislative retort to the Supreme Court in *Dowling* that held the NSPA did not cover intellectual property.[92] The EEA was meant to function as a shield to protect corporations and a legislative gap filler to cover intellectual property. The utility of the EEA is handicapped by the decision in *Aleynikov*. When speaking about the EEA, Judge Calabresi concludes, "it is hard for me to conclude that Congress, in this law, actually meant to exempt the kind of behavior in which Aleynikov engaged."[93] The newly enacted language modification in late 2012 may have achieved this. But until this new language is judicially interpreted, *Aleyinkov*'s shadow looms large.

VI. AN ALTERNATIVE APPROACH TO READING AND APPLYING THE LAW—*HEYDON*'S CASE

The problem created by the *Aleynikov* decision could be remedied if an alternative form of judicial interpretation was applied. Instead of plain meaning, or the "Golden Rule," which allows judges to depart from the strict wording of the law to avoid an "absurd result," guidance could be gleaned from *Heydon*'s Case.[94] This old English rule of legislative interpretation created in 1584 requires judges to look over "four tasks" to ensure that the gaps within the law are covered.[95] Justice Coke described the four tasks as four specific questions a judge needs to consider in the process of legislative interpretation:

---

[90] *See* H.R. REP. NO. 104-788, at 4–7 (1996).
[91] *Aleynikov*, 676 F.3d at 82 (Calabresi, J., concurring).
[92] *Id.*
[93] *Id.*
[94] *Heydon*'s Case, 76 Eng. Rep. 637 (Ct. Exchequer 1584).
[95] *Id.*

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

> What was the common law before the making of the Act? What was the mischief and defect for which the common law did not provide? What remedy the Parliament hath resolved and appointed to cure the disease of the commonwealth? And the true reason of the remedy . . . . [96]

The primary goal of the rule is to eliminate the potential "mischief" that a statute was originally aimed to remedy.[97] This gives judges the needed latitude to "consider [the] four contextual aspects of a statute when deciding how to interpret that statute."[98] Despite its age, the Supreme Court has endorsed this view and applied it in numerous decisions.[99]

The mischief that the NSPA and the EEA were enacted to combat was the theft a business's valuable trade secrets. Simply allowing Aleynikov to walk away from his blatant theft and attempted interstate transaction because of a legislative technicality cannot be allowed. Application of the *Heydon* principal demonstrates that the Second Circuit's decision has not fulfilled all four tasks. Their decision is devoid of context in favor of an overly restrictive reading. If anything, their decision invites more mischief and misappropriation if an Aleynikov-like individual can tiptoe the balance struck by the court. It seems surreal to build protective measures that penalize the type of actions that Aleynikov perpetuated, and then deconstruct these measures to a point where they are incapable of fulfilling their actual intent. *Heydon*'s Case offers an alternative approach to legislative analysis that the Second Circuit may have been better served in undertaking.

VII. CONCLUSION

The NSPA and the EEA are not beyond salvage; instead both can be transformed into powerful weapons that protect intangible intellectual property. The traditional forms of intellectual property are always available

---

[96] *Id.*

[97] U.S. Legal Definitions, "Mischief Rule Law & Legal Definition," *available at* http://definitions.uslegal.com/m/mischief-rule/.

[98] Robin Kundia Craig, *The Stevens/Scalia Principal and Why It Matters: Statutory Conversations and a Cultural Critical Critique of the Strict Plain Meaning Approach*, 79 TUL. L. REV. 955, 1035 (2005).

[99] *See generally* Pierson v. Ray, 386 U.S. 547 (1967); Hamilton v. Rathbone, 175 U.S. 414 (1899); Smith v. Townsend, 148 U.S. 490 (1893).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu

to businesses in an attempt to protect their property. This does not detract from the fact that our economy is moving further into an information technology based model. Yariel Flores asserts that the "overlapping of protections increases the development, production, and sales cost of software."[100] With technology based start-ups littering the business landscape like never before, it is instrumental that we adequately protect the valuable intangibles that they produce.

The overly strict legislative reading committed by the Second Circuit not only subverts the true purpose of the NSPA and the EEA; it also clouds an area of the law that demands clarification. Allowing a former Goldman Sachs employee to steal valuable, confidential source code and then attempt to pass it along to his new employer, is an action that cannot be condoned. The legislative modification to the EEA in late 2012 is a positive step, but work remains, especially concerning the NSPA. Definitive and unambiguous statements need to be made in the area of source code protection. While Aleynikov may have escaped punishment under the NSPA and the EEA because of a strict interpretation by the court, his actions demonstrate that wholesale changes need to be made to deter similar actions from occurring in the future.

[100] Yariel Flores, *The Computer Software "Dilemma." The Time for the "Computer Software Bill" Has Arrived*, 50 REV. DER. P.R. 147, 169 (2010).

Vol. 32, No. 2 (2014) ● ISSN: 2164-7984 (online) ● ISSN 0733-2491 (print)
DOI 10.5195/jlc.2014.63 ● http://jlc.law.pitt.edu