H

United States District Court,
S.D. New York.
UNITED STATES of America,
v.
Sergey **ALEYNIKOV**, Defendant.

No. 10 Cr. 96(DLC).
Sept. 3, 2010.

Background: Defendant was charged with misappropriating computer source code used in high-frequency financial trading system. Defendant moved to dismiss each count of indictment.

Holdings: The District Court, Denise Cote, J., held that:
(1) system constituted "product" within meaning of Economic Espionage Act (EEA);
(2) source code constituted "goods" within meaning of National Stolen Property Act (NSPA); and
(3) Computer Fraud and Abuse Act (CFAA) applied only to unauthorized procurement or alteration of information.

Motion denied.

West Headnotes

[1] Larceny 234 5

234 Larceny
234I Offenses and Responsibility Therefor
234k4 Property Subject of Larceny
234k5 k. In general. Most Cited Cases
High-frequency financial trading system constituted "product" within meaning of Economic Espionage Act (EEA), for purposes of indictment alleging defendant's misappropriation of computer source code used in system; system was initially comprised of different computer programs, and programmers had subsequently developed and modified system by writing and altering source code of programs. 18 U.S.C.A. §§ 1832(a), 1839(3).

[2] Receiving Stolen Goods 324 2

324 Receiving Stolen Goods
324k2 k. Property and stealing thereof. Most Cited Cases
Computer source code used in high-frequency financial trading system constituted "goods" within meaning of National Stolen Property Act (NSPA), for purposes of indictment alleging defendant's misappropriation of source code; code would have been valuable for any firm seeking to launch or enhance high-frequency trading business, and thus would ordinarily have been subject of commerce. 18 U.S.C.A. § 2314.

[3] Telecommunications 372 1348

372 Telecommunications
372VIII Computer Communications
372k1347 Offenses and Prosecutions
372k1348 k. In general. Most Cited Cases
Criminal charge under Computer Fraud and Abuse Act (CFAA) applies only to unauthorized procurement or alteration of information. 18 U.S.C.A. § 1030(a)(2)(C).

***174** Joseph P. Facciponti, Rebecca A. Rohr, United States Attorney Office, New York, NY, for the United States.

Kevin H. Marino, John D. Tortorella, Marino Tortorella, P.C., Chatham, NJ, for Defendant.

OPINION & ORDER

DENISE COTE, District Judge:

Defendant Sergey **Aleynikov** (" **Aleynikov** ") has moved to dismiss each count in a three-count Indictment filed against him on February 11, 2010. **Aleynikov**, a former employee of Goldman Sachs & Co. ("Goldman"), is charged with misappropriating computer source code used in Goldman's high-frequency trading system. For the following reasons, the motion is granted in part.

BACKGROUND

As charged in the Indictment, Goldman is a global financial services firm engaged in, *inter alia*, high-frequency trading on securities and commodities markets, including the New York Stock Exchange ("NYSE") and NASDAQ Stock Market ("NASDAQ"). **Aleynikov** was a computer programmer employed by Goldman as a Vice President in its Equities Division from May 2007 until June 2009. In this position, **Aleynikov** was responsible for developing and maintaining some of the computer programs used to operate Goldman's high-frequency trading system. **Aleynikov** resigned in June 2009 to work for Teza Technologies, LLC ("Teza"), a company founded earlier that year. Teza offered **Aleynikov** the title of "Executive Vice President, Platform Engineering," in which position he would be responsible for developing Teza's own high-frequency trading business that would compete with Goldman.

***175** High-frequency trading, an activity in which various banks and financial institutions engage, involves the rapid execution of high volumes of trades in which trading decisions are made by sophisticated computer programs that use complex mathematical formulae known as algorithms. The algorithms use statistical analyses of past trades and current market developments. Goldman used a proprietary system of computer programs, which the Indictment calls the "Platform," to rapidly obtain information on the latest market movements, to process that information into a form that can be analyzed by the algorithms, and to execute the trading decisions reached by the application of the algorithms to that information. Together, the trading algorithms and Platform comprise Goldman's trading system (the "Trading System").

Goldman acquired portions of the Platform when it purchased the Hull Trading Company ("Hull") in 1999 for approximately $500 million. Since then, Goldman's computer programmers have developed and modified the computer programs that Goldman uses in its Trading System by writing and altering their source code. [FN1] Goldman has not licensed its Trading System or made it or its components available to the public, and has taken measures to protect the Trading System's source code. Among other things, Goldman employees must execute a confidentiality agreement and assign to Goldman the rights to any ideas or information developed during their employment. Goldman also limits access to the Trading System's source code only to Goldman employees who have reason to access that source code, such as the programmers working on the Trading System.

> FN1. The Indictment defines "source code" as "a series of programming instructions, in human-readable format, that specify the actions to be performed by a computer program."

During his employment at Goldman, **Aleynikov** was a member of a team of computer programmers responsible for developing and improving aspects of the Platform, including the Platform's interface with NASDAQ. On his last day of employment at Goldman, June 5, 2009, **Aleynikov** copied, compressed, encrypted, and transferred to an outside server in Germany hundreds of thousands of lines of source code for the Trading System, including trading algorithms that determine the value of stock options. The entity that operates the German server offers free and paid services to computer programmers who wish to store their source code projects. After transferring the source code to the German server, **Aleynikov** deleted the program he used to encrypt the files. He also deleted his "bash history," *i.e.*, the history of his most recent computer commands. That evening, and in the days that followed, **Aleynikov** accessed the German server and downloaded the source code to his home computer, and from there to other home computers and to a portable flash drive.

On July 2, **Aleynikov** flew to Chicago, Illinois, to meet with Teza. He brought with him a laptop computer and the flash drive containing source code for Goldman's Trading System, including

some of the source code that he copied and transferred to the German server on June 5.

The Indictment charges **Aleynikov** in three counts with theft of trade secrets in violation of 18 U.S.C. §§ 1832(a)(2) and (4); transportation of stolen property in interstate commerce, in violation of 18 U.S.C. § 2314; and unauthorized computer access and exceeding authorized access in violation of 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(i) -(iii). On July 16, 2010, **Aleynikov*176** moved to dismiss each of these counts. The motion became fully submitted on August 13.

DISCUSSION

A. Legal Standard

Aleynikov moves to dismiss all counts of the Indictment pursuant to Rule 12(b)(3)(B), Fed.R.Crim.P. Rule 12(b)(3)(B) provides that "at any time while the case is pending, the court may hear a claim that the indictment or information fails to invoke the court's jurisdiction or to state an offense." Fed.R.Crim.P. 12(b)(3)(B).

The law on determining the sufficiency of an indictment is well-settled. Under the Federal Rules of Criminal Procedure, the indictment "must be a plain, concise, and definite written statement of the essential facts constituting the offense charged" and must include the "statute, rule, regulation, or other provision of law that the defendant is alleged to have violated." Fed.R.Crim.P. 7(c)(1). There are also "two constitutional requirements for an indictment: 'first, [that it] contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, [that it] enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense.' " *United States v. Resendiz-Ponce*, 549 U.S. 102, 108, 127 S.Ct. 782, 166 L.Ed.2d 591 (2007) (quoting *Hamling v. United States*, 418 U.S. 87, 117, 94 S.Ct. 2887, 41 L.Ed.2d 590 (1974)); *see also United States v. Yannotti*, 541 F.3d 112, 127 (2d Cir.2008).

But, it is also well established that "an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime." *Yannotti*, 541 F.3d at 127 (citation omitted); *see also United States v. De La Pava*, 268 F.3d 157, 162 (2d Cir.2001). Thus, the indictment need only allege "the 'core of criminality' the government intend[s] to prove" at trial, and consequently, the indictment is "read ... to include facts which are necessarily implied by the specific allegations made." *United States v. Rigas*, 490 F.3d 208, 229 (2d Cir.2007) (citation omitted).

On a pretrial motion to dismiss, "the facts alleged by the government must be taken as true." *United States v. Velastegui*, 199 F.3d 590, 592 n. 2 (2d Cir.1999). It is not proper to weigh the sufficiency of the evidence underlying the indictment, unless the Government has already made "a full proffer of the evidence it intends to present at trial." *United States v. Perez*, 575 F.3d 164, 166 (2d Cir.2009) (citation omitted). This is because indictments are "not meant to serve an evidentiary function," but rather, "to acquaint the defendant with the specific crime with which he is charged, allow him to prepare his defense, and protect him from double jeopardy." *United States v. Juwa*, 508 F.3d 694, 701 (2d Cir.2007) (citation omitted).

An indictment may be dismissed, however, where it "fails to allege the essential facts constituting the offense charged." *United States v. Pirro*, 212 F.3d 86, 91 (2d Cir.2000). Indeed, "an important corollary purpose" of the requirement that an indictment state the elements of an offense "is to inform the court of the facts alleged, so that it may decide whether they are sufficient in law to support a conviction, if one should be had." *Russell v. United States*, 369 U.S. 749, 768, 82 S.Ct. 1038, 8 L.Ed.2d 240 (1962) (citing *United States v. Cruikshank*, 92 U.S. 542, 558, 23 L.Ed. 588 (1875)). Dismissal is required where the conduct alleged in the indictment as a factual basis for the offense is not actually prohibited by the language of the statute. ***177** *See, e.g., Pirro*, 212 F.3d at 91, 93

(affirming dismissal where Government's proposed proof would not establish a crime within the terms of the statute); *United States v. Pacione*, 738 F.2d 567, 572 (2d Cir.1984) (same); *United States v. Mennuti*, 639 F.2d 107, 113 (2d Cir.1981) (same), abrogated in part on other grounds, *Russell v. United States*, 471 U.S. 858, 105 S.Ct. 2455, 85 L.Ed.2d 829 (1985).

Oftentimes, the adequacy of an indictment will turn on the interpretation of statutory language. "Federal crimes, of course, are solely creatures of statute." *Dowling v. United States*, 473 U.S. 207, 213, 105 S.Ct. 3127, 87 L.Ed.2d 152 (1985) (citation omitted). "[S]tatutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." *United States v. Albertini*, 472 U.S. 675, 680, 105 S.Ct. 2897, 86 L.Ed.2d 536 (1985) (citation omitted). When the statutory language is clear, there is no need to examine the statutory purpose, legislative history, or the rule of lenity. *See Boyle v. United States*, --- U.S. ----, 129 S.Ct. 2237, 2246, 173 L.Ed.2d 1265 (2009); *see also United States v. Nelson*, 277 F.3d 164, 193 (2d Cir.2002).

B. Count One: Theft of Trade Secrets

Count One of the Indictment charges **Aleynikov** with theft of trade secrets in violation of 18 U.S.C. § 1832(a)(2) and (4):

> From at least in or about May 2009, up to and including on or about July 3, 2009, ... SERGEY **ALEYNIKOV**, the defendant, unlawfully, willfully, and knowingly, without authorization copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, and conveyed a trade secret, as that term is defined in Title 18, United States Code, Section 1839(3), and attempted so to do, with intent to convert such *trade secret, that was related to and included in a product that was produced for and placed in interstate and foreign commerce*, to the economic benefit of someone other than the owner thereof, and intending and knowing that the offense would injure the owner of that trade secret, to wit, **ALEYNIKOV**, while in New York, New York and elsewhere, without authorization copied and transmitted to his home computer Goldman's proprietary computer source code for Goldman's high-frequency trading business, with the intent to use that source code for the economic benefit of himself and his new employer, Teza.
>
> (Emphasis added.)

Aleynikov moves to dismiss Count One because the Indictment does not allege that the trade secret at issue here-the source code for Goldman's Trading System-is related to or included in a "product" that is "produced for or placed in interstate and foreign commerce." According to **Aleynikov**, a "product," as used in 18 U.S.C. § 1832(a), must be a tangible item of personal property distributed to and used by the commercial public. Because Goldman has never licensed or sold the Trading System, and has no intention of doing so, **Aleynikov** contends that the Trading System is not a "product produced for or placed in" commerce within the meaning of § 1832. **Aleynikov** does not dispute that the trade secret he allegedly stole is "related to or included in" the Trading System.

Describing the clause of § 1832(a) on which **Aleynikov's** motion depends as the "jurisdictional element" of the offense, the Government asserts that the Trading System is indeed a "product" within the meaning of § 1832 that has an "obvious and ***178** indisputable connection" to interstate and foreign commerce. The Government thus agrees with **Aleynikov** that the trade secret at issue in Count One is the source code, and that the relevant "product" is the Trading System. In addition to the facts outlined in the Indictment, the Government proffers that it expects to prove at trial that there are high-frequency trading systems that may be purchased by securities trading firms, and that Goldman maintains computers in the United States and elsewhere in the world that use its Trading Sys-

tem to conduct trading on world markets.

Section 1832 was enacted as part of the Economic Espionage Act of 1996, Pub.L. No. 104-294, 110 Stat. 3488 (1996) (the "EEA"). In relevant part, the EEA applies to anyone who,

> with intent to convert a *trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce,* to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly ... without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information.

18 U.S.C. § 1832(a)(2) (emphasis added). The EEA defines "trade secret" as

> 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.

18 U.S.C. § 1839(3). The statute carries a ten-year maximum term of imprisonment. 18 U.S.C. § 1832(a).

The EEA does not define the term "product." Where a term in a criminal statute is undefined, it must be given "its ordinary meaning." *United States v. Santos,* 553 U.S. 507, 128 S.Ct. 2020, 2024, 170 L.Ed.2d 912 (2008) (relying on the Oxford English Dictionary, Random House Dictionary of the English Language, and Webster's New International Dictionary to define the term "proceeds"); *see also United States v. Broxmeyer,* 616 F.3d 120, 125 (2d Cir.2010) (consulting dictionary definitions of "words of common usage that have plain and ordinary meanings"). The ordinary meaning of "product" is something that is the result of human or mechanical effort or some natural process. *See, e.g.,* The American Heritage Dictionary 1399 (4th ed.2000) ("Something produced by human or mechanical effort or by a natural process."); 12 Oxford English Dictionary 565 (2d ed.1989) ("That which is produced by any action, operation, or work; a production; the result."); The Random House Dictionary of the English Language 1148 (1970) ("[A] thing produced by labor; a person or thing produced by or resulting from a process, as a natural, social, or historical one; result."); Webster's Third New International Dictionary 1810 (1993) ("[S]ome thing produced by physical labor or intellectual effort: the result of work or thought."). FN2

> FN2. Black's Law Dictionary defines "product" more narrowly as: "Something that is distributed commercially for use or consumption and that is usually (1) tangible personal property, (2) the result of fabrication or processing, and (3) an item that has passed through a chain of commercial distribution before ultimate use or consumption." Black's Law Dictionary 1245 (8th ed.2004). This definition, however, appears to have been derived from the law of products liability and manufacturing contexts, as evidenced by the fact that it cross-references the entries for "manufacture" and "products liability." *See id.* As such, this definition does not represent the "ordinary meaning" of the term "product."

***179** [1] Applying the plain, ordinary meaning of "product," there is no doubt that the Trading

System is a "product" within the meaning of the EEA. The Trading System is "comprised of different computer programs," portions of which Goldman acquired when it purchased Hull for $500 million. Since 1999, Goldman's computer programmers have substantially developed and modified the Trading System by "writing and altering the 'source code' of those programs." The only difference between the Trading System and other computer software, like Microsoft Windows, is that Goldman does not presently intend to sell or license the Trading System. This characteristic does not, however, render the Trading System any less of a "product" within the meaning of the EEA.

Likewise, it is clear that the Trading System was "produced for" interstate commerce based on the plain, ordinary meaning of those terms. Indeed, 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. Goldman uses the Trading System to rapidly execute high volumes of trades in various financial markets, including the NYSE and NASDAQ, in which buy and sell orders for securities and commodities are placed electronically. The Trading System generates many millions of dollars in annual profits. Goldman's high-frequency trading activity, which is uniquely made possible by the Trading System, undoubtedly qualifies as interstate and foreign commerce. As such, the Trading System was "produced for" interstate and foreign commerce within the meaning of the EEA.

The legislative history of the EEA confirms this interpretation. Put simply, "the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets." *United States v. Yang*, 281 F.3d 534, 543 (6th Cir.2002). Recognizing the increasing importance of "intangible assets" like trade secrets in the "high-technology, information age," the growing threat posed by the theft of such proprietary economic information, and the inadequacy of existing federal laws to protect trade secrets, Congress enacted the EEA to provide "a systematic approach to the problem of economic espionage." H.R.Rep. No. 104-788, at 4-7 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 4021, 4025; *see also* S.Rep. No. 104-359, at 6-11 (1996); *United States v. Hsu*, 155 F.3d 189, 194-95 (3d Cir.1998). As President Clinton stated upon signing the bill into law, the EEA was designed to "protect the trade secrets of *all businesses operating in the United States*, foreign and domestic alike, from economic espionage and trade secret theft." Statement by President William J. Clinton upon Signing H.R. 3723, 32 Weekly Comp. Pres. Doc. 2040 (Oct. 14, 1996), *as reprinted in* 1996 U.S.C.C.A.N. 4034, 4034 (emphasis added).

The EEA was intended "to bring together into a *single vehicle* the prohibition on the theft of trade secrets and proprietary information by both private individuals and corporations and by foreign governments and those acting on their behalf." 142 Cong. Rec. S12201, S12208 (daily ed. Oct. ***180** 2, 1996) (statement of Sen. Specter) (emphasis added). Accordingly, the EEA contains two provisions addressing the theft of trade secrets. The first, 18 U.S.C. § 1831, prohibits the theft of trade secrets by individuals with the knowledge and intent that the theft will benefit "any foreign government, foreign instrumentality, or foreign agent." 18 U.S.C. § 1831(a). The second, 18 U.S.C. § 1832, at issue here, prohibits the theft of trade secrets by individuals with the intent to benefit "anyone other than the owner thereof, and intending and knowing that the offense will[ ] injure the owner of that trade secret." *Id.* § 1832(a). The two sections, however, criminalize identical specified acts in connection with trade secrets. *Compare id.* § 1831(a)(1)-(5), *with id.* § 1832(a)(1)-(5).

Although both § 1831 and § 1832 guard against the same types of threats to trade secrets, albeit from actors with different motivations [FN3], **Aleynikov** interprets § 1832 to protect a narrower set of trade secrets than § 1831. Pointing to the lan-

guage in § 1832 requiring trade secrets to be "related to or included in a product that is produced for or placed in interstate or foreign commerce," which does not appear in § 1831 [FN4], **Aleynikov** argues that § 1832 applies only to trade secrets "relating to tangible products actually sold, licensed or otherwise distributed." In support of his narrower interpretation of § 1832, **Aleynikov** also draws on definitions of "product" from products liability law and related contexts. [FN5] **Aleynikov** also cites several trade ***181** secrets cases which he claims demonstrate that the EEA should be read to reflect a singular focus on trade secrets relating to tangible commercial products.

FN3. The EEA punishes violations of § 1831 more harshly than § 1832. Individuals convicted under § 1831 face up to fifteen years' imprisonment and may be fined up to $500,000, while those convicted under § 1832 face up to ten years' imprisonment and a fine. *See* 18 U.S.C. §§ 1831(a), 1832(a). Organizations are subject to harsher penalties under both sections. *See id.* §§ 1831(b), 1832(b).

FN4. The inclusion of the "product" language in 18 U.S.C. § 1832 is not explicitly addressed in the legislative record. The language appears to have originated in House Bill 3723, entitled "The Economic Espionage Act of 1996." *See* H.R. 3723, 104th Cong. (1996), *as reprinted in* H.R.Rep. No. 104-788, at 2, 1996 U.S.C.C.A.N, at 4021. In the Senate version of the legislation, the threat to trade secrets posed by "domestic" and "foreign" economic espionage was initially addressed in two separate bills, Senate Bill 1556, entitled "The Industrial Espionage Act of 1996," and Senate Bill 1557, entitled "The Economic Security Act of 1996." *See* 142 Cong. Rec. S12201, S12208 (daily ed. Oct. 2, 1996) (Statement of Sen. Specter) (discussing S. 1556 and S. 1557). The two Senate bills were ultimately merged and passed by the Senate using House Bill 3723 as the vehicle. *See id.*

> Notably, Senate Bill 1566, which "broadly prohibited the theft of proprietary economic information by any person," *id.*, did not include the "product" language that now appears in 18 U.S.C. § 1832. *See* S. Bill 1566, *as reprinted in* S.Rep. No. 104-359, at 3. Instead, to provide a basis for federal jurisdiction, Senate Bill 1556 included a specific "finding" that "the development and production of proprietary economic information involves every aspect of interstate commerce and business." *See* S.Rep. No. 104-359, at 1. No such finding appeared in House Bill 3723, which instead included the "product" language that now appears in § 1832. There is nothing in the legislative history to suggest, however, that Congress's adoption of House Bill 3723, rather than the Senate's version of the legislation, was intended to narrow the types of trade secrets protected by § 1832 compared to § 1831.

FN5. Specifically, **Aleynikov** relies on the definition of "product" from three sources: (1) Black's Law Dictionary which, as noted above, is drawn from the products liability context; (2) Section 19 of the Restatement (Third) of Torts: Products Liability, which defines "product" as "tangible personal property distributed commercially and used for consumption"; and (3) the Magnuson-Moss Warranty Act, 15 U.S.C. § 2301 *et seq.*, which defines "consumer product," in pertinent part, as "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes." 15 U.S.C. § 2301(1).

Aleynikov's restrictive interpretation of § 1832 is unpersuasive. Neither the text of § 1832, nor the legislative history of the EEA, indicate that Congress intended to restrict the scope of § 1832 to trade secrets related to tangible consumer products sold in commerce. First, nothing in the EEA's legislative history suggests that Congress intended § 1832 to address a narrower set of trade secrets than § 1831, or that Congress wished to limit § 1832's protection to particular industries or products.[FN6] To the contrary, the legislative history demonstrates that Congress intended for the EEA to provide "comprehensive" and "systematic" protection for trade secrets belonging to companies in the United States, not just manufacturers of tangible consumer products.[FN7] Thus, the more plausible explanation for the inclusion of the "product" requirement in § 1832 but not § 1831 is that Congress needed to supply a basis for federal jurisdiction for § 1832, whereas the jurisdictional nexus for § 1831 was provided by its focus on the actions of foreign governments.[FN8]

FN6. For instance, the Senate "Manager's Statement" for the EEA analyzes the differences between §§ 1831 and 1832, *see* 142 Cong. Rec. S12201, S12212, but makes no distinction between the scope of trade secrets protected by §§ 1831 and 1832. Instead, the only difference between the two sections noted in the Manager's Statement concerns *for whose benefit* the trade secret is stolen: "This legislation includes a provision penalizing the theft of trade secrets (Sec.1832) and a second provision penalizing that theft when it is done to the benefit of a foreign government, instrumentality, or agent (Sec.1831)." *Id.*

FN7. One of Congress's primary concerns in enacting the EEA was to address exactly the type of situation at issue here, namely "employees who leave their employment and use their knowledge about specific products or processes in order to duplicate them or develop similar goods for themselves or a new employer in order to compete with their prior employer." H.R.Rep. No. 104-788, at 7, 1996 U.S.C.C.A.N. at 4026. This concern, however, was not limited to manufacturers of tangible, consumer products. For instance, the Senate Report accompanying the bill that became the EEA cited the example of an employee of a computer firm that supplied "software technology to various government projects, primarily in NASA astrophysics activities" who had "transmitted that company's source code to another person in what appeared to be an attempt to appropriate the source code for his own personal use." S.Rep. No. 104-359, at 9. Under **Aleynikov's** interpretation of § 1832, such stolen source code for software provided only for government projects, rather than personal consumption, would not be protected by the EEA.

FN8. The EEA was enacted in 1996, the year after the Supreme Court's decision in *United States v. Lopez*, 514 U.S. 549, 115 S.Ct. 1624, 131 L.Ed.2d 626 (1995), in which the Court interpreted the Constitution to require the addition of a "jurisdictional element" to a federal gun possession statute in order to narrow its scope. *See id.* at 561-62, 115 S.Ct. 1624 (suggesting the addition of an "express jurisdictional element" requiring connection between weapon and interstate commerce would render statute constitutional under the Commerce Clause).

Furthermore, **Aleynikov's** interpretation of § 1832 would essentially add the word "consumer" before the word "product," even though that term does not appear in the text of the statute.[FN9] It would also be ***182** inappropriate to use a specialized definition of "product" drawn from products liability law for a statute whose purpose is to broadly

protect intellectual property. Unlike the law of products liability, which specifically addresses the physical harms that may be caused by tangible consumer goods, the law of intellectual property concerns both intangible and tangible items. As the legislative history of the EEA makes clear, Congress recognized that intangibles such as information, including that embodied in companies' "computer software," may be "the keystone to their economic competitiveness. They spend many millions of dollars developing the information, take great pains and invest enormous resources to keep it secret, and expect to reap rewards from their investment." H.R.Rep. No. 104-788, at 4, 1996 U.S.C.C.A.N. at 4023; *see also* S.Rep. No. 104-359, at 6. The fact that some, or even most, of the cases brought under § 1832 will involve trade secrets related to tangible products sold to consumers does not lead to the conclusion that intangible products, like Goldman's Trading System, are outside the scope of § 1832. FN10

FN9. Other criminal statutes demonstrate that where Congress intends to address consumer products specifically, it actually uses the word "consumer" to modify the word "product." *See, e.g.*, 18 U.S.C. § 1365 (criminalizing tampering with "consumer products"). Section 1365 defines the term "consumer product" as, *inter alia*, "any article, product, or commodity which is customarily produced or distributed for consumption by individuals, or use by individuals for purposes of personal care or in the performance of services ordinarily rendered within the household, and which is designed to be consumed or expended in the course of such consumption or use." *See id.* § 1365(h)(1). Had Congress intended to restrict the protection provided by 18 U.S.C. § 1832 to trade secrets that are related to consumer products, it could have done so by using the term "consumer product" instead of just "product."

FN10. Section 1832 has already been applied in at least one other case that did not involve a tangible consumer product. *See United States v. Nosal*, No. 08 Cr. 237(MHP), 2009 WL 981336 (N.D.Cal. Apr. 13, 2009) (names and contact information allegedly stolen from the database of an executive search firm).

Aleynikov's reliance on *General Dynamics Corp. v. United States*, 202 Ct.Cl. 347, 1973 WL 21349 (1973) (per curiam), is also misplaced. *General Dynamics* concerned whether certain costs associated with developing an experimental prototype aircraft that were incurred without any prototype contract with the federal government, *id.* at *10, were reimbursable under procurement contracts that the company did win from the federal government. The company had charged the fabrication and demonstration costs associated with the experimental aircraft to an overhead account that covered "selling costs," and then allocated those costs to 160 government cost-reimbursement contracts. *Id.* at *1. The court held that because the prototype aircraft was not a "product" within the meaning of the procurement contracts, the costs could not be recouped as "selling costs." *Id.* at *8-*9.

The court's decision in *General Dynamics* was based on an interpretation of "product" in the context of government procurement contracts and the Armed Services Procurement Regulations, and therefore sheds no light on the meaning of "product" in the context of 18 U.S.C. § 1832. Furthermore, if the *General Dynamics* court's interpretation of "product" were applied to the EEA, it would have the absurd result of excluding from the protection of § 1832 trade secrets related to prototypes, thus withholding the EEA's protection when it is needed most. At least one federal court has already rejected a similar argument. *See United States v. Hsu*, 40 F.Supp.2d 623, 625 n. 1 (E.D.Pa.1999) (trade secrets related to technology in research and development, but not yet commercially viable, covered by § 1832).

Aleynikov also cites three law journal articles to support his interpretation of § 1832. These commentaries, however, provide only a cursory, and nearly identical, analysis of the relevant language in § 1832 with no citation to any authority except § 1832 itself. Moreover, rather ***183** than directly supporting **Aleynikov's** interpretation of § 1832, the articles interpret the "product" language as removing from the ambit of § 1832 trade secrets that are related to pure services, or that represent "negative know-how" or information discovered, but not yet used, by a company. *See* James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996,* 5 Tex. Intell. Prop. L.J. 177, 200 (1997); Spencer Simon, *The Economic Espionage Act of 1996,* 13 Berkeley Tech. L.J. 305, 315 (1998); *see also* Rice Ferrelle, *Combating the Lure of Impropriety in Professional Sports Industries: the Desirability of Treating a Playbook as a Legally Enforceable Trade Secret,* 11 J. Intell. Prop. L. 149, 189 (2003) ("The EEA does not protect trade secrets related to services."). The Trading System, however, is none of these things.

With respect to the meaning of the phrase "produced for or placed in interstate or foreign commerce," **Aleynikov** relies on cases interpreting the Fair Labor Standards Act, 29 U.S.C. § 201 *et seq.,* which addresses labor standards in "industries engaged in commerce or in the *production of goods for commerce.*" 29 U.S.C. § 202(a) (emphasis added). **Aleynikov** contends that these FLSA cases demonstrate that it is not sufficient to show that a "product" relates to interstate or foreign commerce; rather, the product embodying the trade secret must itself "be intended to, or actually, move in interstate or foreign commerce."

Unlike the FLSA, however, § 1832 does not refer to the "production of *goods* for commerce," but rather more generally to any "*product* produced for" commerce. In any event, the FLSA also defines "goods" broadly to include, *inter alia,* "articles or *subjects of commerce* of any character, or any part or ingredient thereof." 29 U.S.C. § 203(i) (emphasis added).[FN11] **Aleynikov** does not dispute that the Trading System is a "subject of commerce." In addition, the Supreme Court has broadly interpreted the term "for commerce" in the context of the FLSA. *See, e.g., Alstate Const. Co. v. Durkin,* 345 U.S. 13, 15, 73 S.Ct. 565, 97 L.Ed. 745 (1953) (holding that employees who work in the production of materials to repair intrastate roads are engaged "in the production of goods for commerce" within the meaning of the FLSA). Thus, **Aleynikov's** reliance on FLSA cases is misplaced.[FN12]

FN11. Other terms defined in the FLSA are also consistent with a broad interpretation of the EEA's requirement that the "product" be "produced for or placed in" commerce. For example, the FLSA defines "commerce" as "trade, commerce, transportation, *transmission, or communication* among the several States or between any State and any place outside thereof." 29 U.S.C. § 203(b) (emphasis added). In addition, the FLSA defines "produced" as "produced, manufactured, mined, handled, or *in any other manner worked on* in any State." *Id.* § 203(j) (emphasis added).

FN12. The Second Circuit recognized long ago that the FLSA's jurisdictional element is broad enough to encompass businesses engaged in a variety of "intangible" activities, such as an insurance company's underwriting of insurance policies, *see Darr v. Mutual Life Ins. Co. of N.Y.,* 169 F.2d 262, 264 (2d Cir.1948), or a bank's "preparing, executing or validating bonds, shares of stock, commercial paper, bills of lading and the like," and "any activities necessary to the effectiveness of [such] documents even though, as an example, it be no more than registering a share or a series of bonds." *Bozant v. Bank of N.Y.,* 156 F.2d 787, 790 (2d Cir.1946).

Aleynikov also invokes the interpretations of § 1832 in the United States Attorneys' Manual and the Department of Justice's Prosecuting Intellectual Property Crimes manual. The sections of the manuals cited by **Aleynikov** principally address ***184** situations where the "product" at issue is still being developed and has not yet been sold to consumer, *see* U.S. Attorneys' Manual 9-59.100 (2004); U.S. Department of Justice, *Prosecuting Intellectual Property Crimes*, 160-61 (3d ed.2006) ("IP Manual"), and are thus inapposite. Furthermore, interpretations of statutory language that appear in agency manuals do not have the force of law and do not warrant deference under *Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984). *See Christensen v. Harris Cnty.*, 529 U.S. 576, 587, 120 S.Ct. 1655, 146 L.Ed.2d 621 (2000); *cf. United States v. Navarro*, 160 F.3d 1254, 1257 n. 4 (9th Cir.1998) (noting that the USAM does not have "the force of law").[FN13] In any event, to the extent that the guidance provided in the USAM and the IP Manual support **Aleynikov's** interpretation[FN14], they demonstrate only that the drafters of these manuals had in mind the generic trade secrets case.

FN13. The manuals themselves disclaim any precedential effect. The USAM states, in pertinent part:

> The Manual provides only internal Department of Justice guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal. Nor are any limitations hereby placed on otherwise lawful litigative prerogatives of the Department of Justice.
>
> USAM 1-1.100, 1997 WL 1943989. Likewise, the IP Manual states, in pertinent part:
>
> This Manual is intended as assistance, not authority. The research, analysis, and conclusions herein reflect current thinking on difficult areas of the law; they do not represent the official position of the Department of Justice or any other agency. This Manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. *See United States v. Caceres*, 440 U.S. 741, 99 S.Ct. 1465, 59 L.Ed.2d 733 (1979).
>
> IP Manual at xvii-xviii.

FN14. For instance, contrary to **Aleynikov's** interpretation of § 1832, the IP Manual states that "[t]he nexus to interstate or foreign commerce [in Section 1832] appears to have been intended *merely to allow federal jurisdiction.*" IP Manual at 160 (emphasis added).

Aleynikov next argues that interpreting § 1832 to protect trade secrets relating to the Trading System would "destroy the balance" of federal and state trade secrets prosecutions. He invokes the principle that " 'unless Congress conveys its purpose clearly, it will not be deemed to have significantly changed the federal-state balance' in the prosecution of crimes." *Jones v. United States*, 529 U.S. 848, 858, 120 S.Ct. 1904, 146 L.Ed.2d 902 (2000) (quoting *United States v. Bass*, 404 U.S. 336, 349, 92 S.Ct. 515, 30 L.Ed.2d 488 (1971)). Unlike in the cases on which **Aleynikov** relies, however, the interpretation of § 1832 adopted herein is not so broad as to convert a whole category of conduct traditionally proscribed only by the states into a federal offense. *See Jones*, 529 U.S. at 857, 120 S.Ct. 1904 (arson of private home); *Mennuti*, 639 F.2d 107, 113 (2d Cir.1981) (destruction of private residence); *United States v. Perrotta*, 313 F.3d 33, 37 (2d Cir.2002) (robbery and extortion of a person). **Aleynikov** does not deny that the Trading System has a strong and substantial connection to interstate and foreign commerce, unlike the private homes at issue in *Jones*, 529 U.S. 848, 120 S.Ct. 1904, and *Mennuti*, 639

F.2d 107, or the victim in *Perrotta*, 313 F.3d at 38, who only worked for a company engaged in interstate commerce.

Moreover, **Aleynikov's** argument that § 1832 should not be read to usurp a traditional area of state criminal law is belied by the legislative history which demonstrates that Congress intended for ***185** the EEA to provide a comprehensive "national scheme" to protect trade secrets in the face of "haphazard[ ]" protection under state laws. *See* S.Rep. No. 104-359, at 11-12; H.R.Rep. No. 104-788, at 6-7, 1996 U.S.C.C.A.N. at 4025. The enactment of the EEA was driven, in part, by Congress's finding that "State laws [did] not fill in the gaps left by Federal law." S.Rep. No. 104-359, at 11; H. Rep. 104-788, at 6-7, 1996 U.S.C.C.A.N. at 4025. While a majority of states had some form of civil remedy for the theft of trade secrets-either by adopting some version of the Uniform Trade Secrets Act, recognizing a tort for misappropriation of the information, or by enforcing contracts governing the use of the information-Congress found such civil remedies were "inadequate." *See* H.R.Rep. No. 104-788, at 6-7, 1996 U.S.C.C.A.N. at 4025; S.Rep. No. 104-359, at 11. Furthermore, "[o]nly a few States [had] any form of criminal law dealing with the theft of this type of information and most of the laws are misdemeanors, rarely used by State prosecutors." H.R.Rep. No. 104-788, at 7, 1996 U.S.C.C.A.N. at 4025; S.Rep. No. 104-359, at 11. Thus, Congress found that "a Federal criminal law [was] needed because of the international and interstate nature of this activity, because of the sophisticated techniques used to steal proprietary economic information, and because of the national implications of the theft." S.Rep. No. 104-359, at 12. Accordingly, the interpretation of § 1832 adopted herein will not lead to any improper encroachment on traditional state law prerogatives.

Lastly, **Aleynikov** argues that interpreting § 1832 to apply to trade secrets related to the Trading System would violate the rule of lenity. This argument fails. The rule of lenity is a rule of statutory construction of last resort that applies only when the statute is truly ambiguous. *See Barber v. Thomas*, --- U.S. ----, 130 S.Ct. 2499, 2508-09, 177 L.Ed.2d 1 (2010) ("[T]he rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute such that the Court must simply guess as to what Congress intended." (citation omitted)); *see also Moskal v. United States*, 498 U.S. 103, 108, 111 S.Ct. 461, 112 L.Ed.2d 449 (1990) ("[W]e have always reserved lenity for those situations in which a reasonable doubt persists about a statute's intended scope even *after* resort to the language and structure, legislative history, and motivating policies of the statute." (citation omitted)).

Having considered the text, purpose, and legislative history of the EEA, no such "grievous ambiguity or uncertainty" exists here. Nor is any guessing required to determine what the EEA means. While **Aleynikov** attempts to manufacture ambiguity by suggesting that § 1832 applies only to trade secrets related to consumer goods, "[t]he mere possibility of articulating a narrower construction ... does not by itself make the rule of lenity applicable." *Smith v. United States*, 508 U.S. 223, 239, 113 S.Ct. 2050, 124 L.Ed.2d 138 (1993); *see also Salinas v. United States*, 522 U.S. 52, 59, 118 S.Ct. 469, 139 L.Ed.2d 352 (1997) ("No rule of construction ... requires that a penal statute be strained and distorted in order to exclude conduct clearly intended to be within its scope." (citation omitted)). Thus, the rule of lenity is of no assistance to **Aleynikov** here. Accordingly, **Aleynikov's** motion to dismiss Count One of the Indictment is denied.

C. Count Two: Interstate Transportation of Stolen Property

Count Two of the Indictment charges transportation of stolen property in interstate or foreign commerce in violation of ***186** the National Stolen Property Act ("NSPA"), 18 U.S.C. § 2314:

> From in or about June 2009, up to and including in or about July 2009, ... SERGEY

> **ALEYNIKOV**, the defendant, unlawfully, willfully, and knowingly, transported transmitted, and transferred in interstate and foreign commerce *goods, wares, merchandise, securities, and money,* of the value of $5,000 and more, knowing the same to have been stolen, converted and taken by fraud, to wit, **ALEYNIKOV**, while in New York, New York, copied, without authorization, Goldman's proprietary computer source code for Goldman's high-frequency trading business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and carried that stolen code to a meeting with his new employer, Teza, in Chicago, Illinois.
>
> (Emphasis added.)

Aleynikov moves to dismiss Count Two because the source code that he is charged with having transported and transmitted in interstate and foreign commerce is not "goods, wares, merchandise, securities or money." He contends that the statute applies only to tangible items, and not to the theft of intangibles, such as the trade secrets embodied in the Trading System's source code.

The Government contends that the Trading System's source code is a valuable commodity that may be purchased and licensed by entities seeking to engage in high-frequency trading. It points out that the Indictment alleges that Goldman acquired some of the components of its Trading System when it purchased Hull in 1999 for $500 million. Accordingly, the Government argues that the stolen source code, or any intangible property, is covered by § 2314 if it is property that is "ordinarily the subject of commerce."

The NSPA provides for the imposition of criminal penalties upon any person who "transports 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." 18 U.S.C. § 2314. Although § 2314 does not define the terms "goods," "wares," or "merchandise," the Second Circuit has interpreted these terms broadly to signify " 'a general and comprehensive designation of such personal property or chattels as are *ordinarily a subject of commerce.*' " *In re Vericker,* 446 F.2d 244, 248 (2d Cir.1971) (Friendly, J.) (quoting *United States v. Seagraves,* 265 F.2d 876 (3d Cir.1959) (emphasis added)). "[U]nder some circumstances *mere papers* may constitute 'goods,' 'wares,' or 'merchandise' " as long as they are "ordinarily bought or sold in commerce." *Vericker,* 446 F.2d at 248 (citation omitted) (emphasis added).[FN15] In *Vericker,* however, the court held that stolen Federal Bureau of Investigation ("FBI") documents were not "goods" for purposes of § 2314 because the Government had failed to establish that such papers were "ordinarily bought or sold in commerce." *Id.*

> FN15. Other circuits have also interpreted § 2314 to cover documents containing trade secrets. *See United States v. Greenwald,* 479 F.2d 320 (6th Cir.1973) (documents containing secret chemical formulations); *United States v. Seagraves,* 265 F.2d 876 (3d Cir.1959) (geophysical maps used in oil exploration).

The market for such goods, wares, or merchandise may be licit or illicit. For instance, in *United States v. Bottone,* 365 F.2d 389 (2d Cir.1966), the Second Circuit held that copies and notes of stolen "papers describing manufacturing procedures" for pharmaceuticals, for which "European drug manufacturers were willing to ***187** pay five and six figures," were "goods" within the meaning of § 2314. *Id.* at 393. The court noted that the "lack of patent protection in certain foreign countries created a market for ... secret processes and furnished a substantial incentive for theft to disloyal employees and persons willing to do business with them." *Id.* at 391.

Applying *Bottone* and *Vericker,* courts in this district have held that § 2314 applies to confidential business information for which a market, legal or otherwise, exists.[FN16] *See, e.g., United States v.*

Farraj, 142 F.Supp.2d 484, 487 (S.D.N.Y.2001) (excerpt of trial plan); *United States v. Caparros*, No. 85 Cr. 990(JFK), 1987 WL 8653, at *3-*4 (S.D.N.Y. Mar. 25, 1987) (internal documents concerning business strategy, production information, and marketing plans, if existence of legitimate or black market could be proven); *cf. United States v. Kwan*, No. 02 Cr. 241(DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003) (travel agency's proprietary contact lists and rate sheets not "goods" because Government failed to prove at trial existence of market, "legal or otherwise," for such information). At least one other district court has similarly held that § 2314 covers confidential business information. *See United States v. Riggs*, 739 F.Supp. 414, 416-17, 420 (N.D.Ill.1990) (proprietary telephone company information contained in "911" computer text file).

FN16. In *Carpenter v. Untied States*, 484 U.S. 19, 108 S.Ct. 316, 98 L.Ed.2d 275 (1987), the Supreme Court construed the term "property" in the mail and wire fraud statute, 18 U.S.C. §§ 1341, 1342, to include a company's confidential information compiled in the course of its business. *See id.* at 26, 108 S.Ct. 316.

[2] In this case, the source code for Goldman's Trading System constitutes "goods" for purposes of § 2314, The source code, like the papers describing drug manufacturing procedures in *Bottone*, contains highly confidential trade secrets related to the Trading System. A market for such valuable trade secrets could readily be proven at trial. As alleged in the Indictment, Goldman itself paid approximately $500 million for components of the Platform when it purchased Hull. In addition, the Government has proffered that the source code would be valuable for any firm seeking to launch, or enhance, a high-frequency trading business. Accordingly, the source code may be viewed as "ordinarily a subject of commerce."

Aleynikov argues that source code does not constitute "goods" because it is "intangible intellectual property." He interprets § 2314 to require that a stolen item be not only commercial, but also "tangible," in nature. **Aleynikov's** attempt to graft a tangibility requirement onto § 2314 is unavailing.

First, even assuming that the source code is "intangible" property as **Aleynikov** asserts [FN17], the text of § 2314 makes no distinction between "tangible" and "intangible" goods, or between electronic and other modes of transfer across state and international lines. To the contrary, anyone who "transmits" or "transfers" stolen property, even if the mode of such transmission or transfer is not physical, violates § 2314. *See, e.g., United States v. Gilboe*, 684 F.2d 235, 238 (2d Cir.1982) ("The primary element of this offense, transportation, does not require proof that any specific means of transporting were used." ***188** (citation omitted)). [FN18] Thus, the statute clearly contemplates the possibility of stolen "intangible" property being "transmitted" or "transferred" across state lines. [FN19]

FN17. **Aleynikov's** depiction of source code as "intangible" is misleading. As the Second Circuit has held in the copyright context, computer source code is in fact embodied or fixed in a "tangible" medium, and therefore capable of copyright protection. *See, e.g., Medforms, Inc. v. Healthcare Mgmt. Solutions, Inc.*, 290 F.3d 98, 107 (2d Cir.2002).

FN18. In 1988, Congress amended § 2314 to include the term "transmits" to reflect its agreement with the Second Circuit and other courts which had held that the NSPA applies to money wire transfers, where the only interstate transportation took place electronically, and where there was no transportation of any physical property. *See* Anti-Drug Abuse Act of 1988, Pub.L. 100-690, § 7057(a), 102 Stat. 4181, 4402 (1988); *see also United States v. Piervinanzi*, 23 F.3d 670, 678 n. 6 (2d Cir.1994) (discussing the 1988 amendment to § 2314

).

FN19. While **Aleynikov** argues that the term "transmits" in § 2314 should be limited to wire transfers of money, he points to nothing in the text of the statute that requires such a restrictive reading.

Second, **Aleynikov's** reliance on Judge Friendly's observation in *Bottone* that "where no *tangible objects* were ever taken or transported, a court would be hard pressed to conclude that 'goods' had been stolen and transported within the meaning of § 2314." *Bottone,* 365 F.2d at 393 (emphasis added), is misplaced. **Aleynikov** neglects the second half of Judge Friendly's statement, which clarifies the type of situation the Second Circuit had in mind: "[T]he statute 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." *Id.* (emphasis added). Unlike the hypothetical case of a memorized formula, **Aleynikov** is accused of both electronically transmitting the stolen source code across international lines-by uploading it to a German server and downloading it to his home computer in New Jersey-and physically transporting it across state lines-by carrying it with him to Chicago on a flash drive and laptop.

The fact that **Aleynikov** copied, transmitted, stored, and transported the stolen source code in an electronic format-which is much more commercially valuable than a hard copy of the source code-does not remove his conduct from the purview of § 2314. *See, e.g., United States v. Alavi,* No. 07 Cr. 429(PHX), 2008 WL 1971391, at *2 (D.Ariz. May 2, 2008) (transportation of stolen software on laptop computer); *Farraj,* 142 F.Supp.2d at 490 (e-mail of electronic document across state lines); *Riggs,* 739 F.Supp. at 421 (internet transfer of electronic text file across state lines); *cf. United States v. Martin,* 228 F.3d 1, 14 (1st Cir.2000) (conspiracy to transport stolen software). As the Second Circuit observed in *Bottone,* the "physical form" in which the "intangible information" is transferred is "immaterial" to the § 2314 analysis; what matters is the commercial value of the intangible information contained therein. *Bottone,* 365 F.2d at 393-94 ("[W]hen the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial."). While *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.[FN20] Indeed, it would be absurd if an individual could skirt the statute simply by making an electronic copy of confidential business information, ***189** rather than a physical copy, and transport it across state lines using, for instance, a laptop, CD-ROM, or flash drive.[FN21]

FN20. **Aleynikov** does not dispute that, as long as it was ordinarily the subject of commerce, a hard copy (*i.e.*, printout) of the source code would constitute "goods" within the meaning of § 2314. According to the Indictment, the alleged stolen source code is "in human-readable format," and thus would still be commercially valuable if in hard copy.

FN21. This case is distinguishable from *United States v. Stafford,* 136 F.3d 1109 (7th Cir.1998), on which **Aleynikov** relies. In *Stafford,* the Seventh Circuit held that "comdata codes"-a sequence of numbers that truckers write down on a "comcheck," which are then cashed like a check while the truckers are on the road-were not "goods," but rather "information," and therefore stealing them did not violate § 2314. *Id.* at 1114-15. Unlike comdata codes, which the Seventh Circuit found "have no value in themselves," *id.* at 1115, the source code at issue here is of obvious commercial value, whether in hard copy or

electronic format.

Third, the Supreme Court's decision in *Dowling v. United States*, 473 U.S. 207, 105 S.Ct. 3127, 87 L.Ed.2d 152 (1985), does not support **Aleynikov's** interpretation of § 2314. In *Dowling*, the Court had no occasion to interpret the meaning of "goods, wares, [or] merchandise" because the defendant did "not contest that he caused the shipment of goods in interstate commerce." *Id.* at 214, 105 S.Ct. 3127. Instead, the *Dowling* Court was focused on whether phonorecords containing unreleased copyrighted vocal performances by Elvis Presley, for the use of which no license had been obtained (*i.e.*, "bootlegs"), were "stolen, converted or taken by fraud" for purposes of § 2314. *Id.* The Court held that where the only act charged involves infringement of an incorporeal, intangible property right or privilege, such as a copyright, there is no violation of § 2314. *Id.* at 226. *Dowling* is therefore distinguishable from cases where, as here, a defendant "transports, transmits, or transfers" the actual stolen "goods, wares, [or] merchandise," or, as in *Bottone*, 365 F.2d 389, copies thereof. FN22

FN22. The Second Circuit's discussion of *Dowling* in *United States v. Wallach*, 935 F.2d 445, 467 (2d Cir.1991), is not to the contrary. In *Wallach*, a case involving interstate transportation of checks obtained by fraud, the court observed that the *Dowling* decision rested on the distinction between the intangible "property rights of a copyright holder" and the "possessory interest of the owner of simple 'goods, wares, [or] merchandise.' " *Id.* (citation omitted). The court held that, unlike the copyrights in *Dowling*, the fraudulent checks "without a doubt" constituted property within the meaning of the statute. *Id.*

Aleynikov points to the Supreme Court's observation in *Dowling* that "cases ... prosecuted under § 2314 have always involved *physical* 'goods, wares, [or] merchandise' that have themselves been 'stolen, converted or taken by fraud.' " *Dowling*, 473 U.S. at 216, 105 S.Ct. 3127 (emphasis added). The tangibility of the stolen "goods, wares, [or] merchandise" was not dispositive, however, but rather whether there was "physical identity between the items unlawfully obtained and those eventually transported." *Id.* The Court stated that for purposes of § 2314, it did not "matter that the [stolen] item owes a major portion of its value to *an intangible component.* " *Id.* (emphasis added). Because the Government in *Dowling* did not allege that the defendant "wrongfully came by the phonorecords actually shipped" or that the bootlegged phonorecords "were 'the same' as the copyrights in the musical compositions that he infringed," there was no violation of § 2314. *Id.* at 214, 105 S.Ct. 3127. By contrast, in this case, the Indictment alleges that the item that **Aleynikov** physically stole is identical to the item that **Aleynikov** allegedly transmitted and transported in interstate and foreign commerce: the source code in its electronic format.

Aleynikov also relies on *United States v. Brown*, 925 F.2d 1301 (10th Cir.1991), in which the Tenth Circuit, relying on *Dowling*, held that a "computer program itself ***190** is an intangible intellectual property, and as such, it alone cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken within the meaning of [§] 2314." *Id.* at 1308. The Tenth Circuit's decision in *Dowling* is not binding on this Court, and, as other courts have found, is not persuasive because it misreads *Dowling*. *See Farraj*, 142 F.Supp.2d at 489; *Alavi*, 2008 WL 1971391, at *2. Among other things, *Brown* places undue emphasis on *Dowling* 's use of the term "physical," which, as discussed above, was not critical to the Court's decision. *Brown*, 925 F.2d at 1308-09. Moreover, *Brown* fails to acknowledge that after *Dowling*, Congress amended § 2314 in 1988 to add the term "transmits" to cover transfers of non-physical forms of stolen property. *See Piervinanzi*, 23 F.3d at 678 n. 6 ("[T]he amendment to § 2314 was designed to codify appellate court holdings that 18 U.S.C. § 2314 is not limited to the physical transportation of stolen or fraudulently ac-

quired money or property." (citation omitted)).

Lastly, **Aleynikov** argues that interpreting § 2314 to cover intangible property, such as confidential business information, would contravene Congress's purpose in enacting the EEA. This argument is without merit. As **Aleynikov** himself acknowledges, the EEA and the NSPA target completely different evils. The EEA criminalizes the *theft* of trade secrets, even if the trade secrets themselves are not transported across state or international lines. By contrast, the NSPA criminalizes the *transportation* of stolen property, not just trade secrets, across state or international lines, but not the theft of the property itself. Contrary to **Aleynikov's** contention, the fact that a defendant who steals trade secrets and then transports, transfers, or transmits them across state or international lines can be prosecuted for violating both 18 U.S.C. § 1832 and 18 U.S.C. § 2314 does not render the EEA "irrelevant." Likewise, **Aleynikov's** assertion that the interpretation of § 2314 adopted herein would "encroach" on traditional areas of federal and state regulation, such as insider-trading and misappropriation of trade secrets, is unpersuasive. While such federal and state laws may also protect confidential business information, they are not coterminous with § 2314, and their violation would not in every case warrant prosecution under § 2314. Accordingly, **Aleynikov's** motion to dismiss Count Two of the Indictment is denied.

D. Count Three: Unauthorized Computer Access

Count Three of the Indictment charges **Aleynikov** with unauthorized computer access and exceeding authorized access in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2) (C):

> In or about June 2009, ... SERGEY **ALEYNIKOV**, the defendant, unlawfully, intentionally, and knowingly, and for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States and of any State, *accessed a protected computer without authorization and exceeded authorized access*, which computer was used in and affecting interstate and foreign commerce and communication, and thereby obtained information from such protected computer the value of which exceeded $5,000, to wit, **ALEYNIKOV**, while in New York, New York, in violation of Goldman's policies and his confidentiality agreement with Goldman, accessed a computer server maintained by Goldman and copied Goldman's proprietary computer source code for Goldman's high-frequency trading***191** business, the value of which exceeded $5,000, uploaded the code to a computer server in Germany, and then downloaded it to his home computer, all with the intent to used that source code for the economic benefit of himself and his new employer, Teza.
>
> (Emphasis added.)

Aleynikov moves to dismiss Count Three because he neither accessed a Goldman computer without authorization, nor exceeded his authorized access when he allegedly accessed, copied, and uploaded the Trading System's source code to the German server and then downloaded it to his home computers. As the Indictment alleges, Goldman limited access to the Trading System's source code to those employees "who had reason" to access it, such as **Aleynikov**, who was "a member of a team of computer programmers responsible for developing and improving certain aspects of the Platform." **Aleynikov** argues that § 1030 does not encompass an employee's misuse or misappropriation of information that the employee has authority to access.

The Government concedes that **Aleynikov** was authorized to access the source code for the Trading System that he allegedly stole, but argues that a defendant's purpose or intention is a necessary component of the violation. According to the Government, the CFAA is therefore violated whenever an individual accesses information with authorization, but does so in violation of a confidentiality agreement or policies or other obligations that the indi-

vidual owes to the information's owner.

[3] The CFAA provides, in pertinent part, that anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer" commits a crime. 18 U.S.C. § 1030(a)(2)(C). The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). The CFAA does not, however, define the term "access without authorization" or "authorization."

Where a statutory term is undefined, it must be given its ordinary meaning. *Santos,* 553 U.S. 507, 128 S.Ct. at 2024; *Broxmeyer,* 616 F.3d at 124-25; *see also United States v. Morris,* 928 F.2d 504, 511 (2d Cir.1991) (holding that the word "authorization" for purposes of the CFAA is "of common usage, without any technical or ambiguous meaning," and therefore the district court "was not obliged to instruct the jury on its meaning"). "Authorization" is generally defined as the "act of authorizing" or "permission or power granted by an authority." *See, e.g.,* The Random House Dictionary of the English Language 100 (Unabridged ed.1970). The term "authorize," in turn, ordinarily means to grant authority or permission to do something. *See, e.g.,* The American Heritage Dictionary 121 (4th ed.2000) ("To grant authority or power to; [t]o give permission for; sanction."); 1 Oxford English Dictionary 799 (2d ed.1989) ("To give legal or formal warrant to (a person) to do something; to empower, permit authoritatively."); The Random House Dictionary of the English Language 100 (1970) ("[T]o give authority or official power to; empower; to give authority for; formally sanction (an act or proceeding)."); Webster's Third New International Dictionary 146 (1993) ("[T]o endorse, empower, justify, or permit by or as if by some recognized or proper authority."). Based on the ordinary meaning of "authorization," then, a person who "accesses a computer without authorization" does so without any permission at all. By contrast, a person who "exceeds authorized access" has permission to access the computer,***192** but not the particular information on the computer that is at issue.

Section 1030(a)(2)(C) therefore addresses only the unauthorized procurement or alteration of information. The phrases "accesses a computer without authorization" and "exceeds authorized access" cannot be read to encompass an individual's misuse or misappropriation of information to which the individual was permitted access. What use an individual makes of the accessed information is utterly distinct from whether the access was authorized in the first place. The Government's theory that the CFAA is violated whenever an individual uses information on a computer in a manner contrary to the information owner's interest would therefore require a departure from the plain meaning of the statutory text.

The interpretation of § 1030(a)(2)(C) adopted herein is supported by persuasive precedent. While the Second Circuit has yet to squarely address the meaning of "without authorization" or "exceeds authorized access" as used in the CFAA, the Ninth Circuit and district courts in the Second Circuit have recently held that an employee with authority to access his employer's computer system does not violate the CFAA by using his access privileges to misappropriate information. *See LVRC Holdings LLC v. Brekka,* 581 F.3d 1127, 1130-31 (9th Cir.2009); *Univ. Sports Pub. Co. v. Playmakers Media Co.,* No. 09 Civ. 8206(RJH), 725 F.Supp.2d 378, 382-84, 2010 WL 2802322, at *3-*4 (S.D.N.Y. July 14, 2010); *Orbit One Commc'ns, Inc. v. Numerex Corp.,* 692 F.Supp.2d 373, 385 (S.D.N.Y.2010); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.,* No. 08 Civ. 3980(JS), 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009). Courts in other districts have also adopted this interpretation of the CFAA. *See, e.g., Shamrock Foods Co. v. Gast,* 535 F.Supp.2d 962, 965-66 (D.Ariz.2008); *Black & Decker Inc. v. Smith,* 568 F.Supp.2d 929,

934 (W.D.Tenn.2008); *Diamond Power Int'l, Inc. v. Davidson,* 540 F.Supp.2d 1322, 1343 (N.D.Ga.2007); *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Masuda,* 390 F.Supp.2d 479, 499 (D.Md.2005).

This interpretation of § 1030(a)(2)(C) comports not only with the plain meaning of the statutory text, but also with the overall structure and purpose of the CFAA. *See Orbit One,* 692 F.Supp.2d at 385-86 (observing that the CFAA's definition of "damage," which is limited to "impairment to the integrity or availability of data, a program, a system, or information," is consistent with a narrow Congressional intent in passing the CFAA-prohibiting people from "hacking" into someone else's computer system); *Jet One Group,* 2009 WL 2524864, at *6 (same). This interpretation is also consistent with the legislative history of the CFAA. *See Shamrock Foods,* 535 F.Supp.2d at 965-66 ("[L]egislative history confirms that the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."). FN23

FN23. Notably, in 1986, Congress amended the CFAA to substitute the phrase "exceeds authorized access" for the phrase "or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend." *See* S.Rep. No. 99-432, at 9, *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2486. By enacting this amendment, and providing an express definition for "exceeds authorized access," Congress's intent was to "eliminate coverage for authorized access that aims at 'purposes to which such authorization does not extend,' " thereby "remov[ing] from the sweep of the statute one of the murkier grounds of liability, under which a [person's] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." *Id.* at 21, 1986 U.S.C.C.A.N. at 2494-95.

***193** The Government argues that other courts have construed the CFAA more broadly to encompass use of a computer for an improper purpose, even if the access itself was lawful. In general, the cases on which the Government relies have applied agency principles to the CFAA to hold that an employee accesses a computer "without authorization" or "exceeds authorized access" within the meaning of § 1030 whenever the employee, without knowledge of the employer, possesses an adverse interest or breaches the duty of loyalty to the employer, thereby terminating her agency relationship. *See, e.g., United States v. John,* 597 F.3d 263, 271 (5th Cir.2010) (" 'authorization' may encompass limits placed on *the use* of information obtained by permitted access to a computer system and data available on that system ... at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime"); *Int'l Airport Ctrs., LLC v. Citrin,* 440 F.3d 418, 420-21 (7th Cir.2006) (defendant's "breach of his duty of loyalty terminated his agency relationship ... and with it his authority to access the laptop, because the only basis of his authority had been that relationship"); *EF Cultural Travel BV v. Explorica, Inc.,* 274 F.3d 577, 582-84 (1st Cir.2001) (defendant's use of "scraper" software to systematically glean tour company's prices from its website "exceeded authorized access," assuming program's speed and efficiency was attributable to defendant's breach of his confidentiality agreement with the company, his former employer). Certain courts in this district have adopted this reasoning. *See, e.g., Mktg. Tech. Solutions, Inc. v. Medizine LLC,* No. 09 Civ. 8122(LLM), 2010 WL 2034404, at *7 (S.D.N.Y. May 18, 2010); *Calyon v. Mizuho Securities USA, Inc.,* No. 07 Civ. 2241(RO), 2007 WL 2618658, at *1 (S.D.N.Y. Sept. 5, 2007); *Register.com, Inc. v. Verio, Inc.,* 126 F.Supp.2d 238, 252-53 (S.D.N.Y.2000). FN24

FN24. The Government attempts to characterize the Second Circuit's decision in *United States v. Morris*, 928 F.2d 504, as consistent with the line of cases that interpret the CFAA more broadly. In *Morris*, the defendant was a graduate student who used his access to a university's computer system to upload a malicious "worm," which spread throughout the internet, causing computers, including government computers, to crash. *Id.* at 505-06. The defendant was convicted under an earlier version of a different provision of the CFAA which made criminal the conduct of an individual who "intentionally accesses a Federal interest computer without authorization." *Id.* at 506. Although the defendant had authorization to access the university's computer system, the *Morris* court found that he acted "without authorization" because he exploited "a special and unauthorized access route into other computers" and thereby released the worm into "computers at which he had no account and no authority." *Id.* at 510. *Morris* is therefore distinguishable from cases where, as here, a defendant has explicit authorization to access all parts of a computer system, but misuses or misappropriates information contained therein. Accordingly, the Government's reliance on *Morris* is misplaced.

These cases are unpersuasive. First, they identify no statutory language that supports interpreting the CFAA to reach misuse or misappropriation of information that is lawfully accessed. Instead, they improperly infer that "authorization" is automatically terminated where an individual "exceed[s] *the purposes* for which access is 'authorized.' " *John*, 597 F.3d at 272 (emphasis added). But "the definition of 'exceeds authorized access' in § 1030(e)(6) indicates that Congress did not intend to include such an implicit limitation in the word 'authorization.' " ***194***LVRC*, 581 F.3d at 1133. The interpretation of the CFAA adopted in this line of cases would require an analysis of an individual's subjective intent in accessing a computer system, whereas the text of the CFAA calls for only an objective analysis of whether an individual had sufficient "authorization." While a confidentiality agreement or other policies or obligations owed to an employer may prohibit misuse of a company's internal computer system or misappropriation of confidential information therein, the plain text of the CFAA does not.

Furthermore, an interpretation of the CFAA based upon agency principles would greatly expand the reach of the CFAA to any employee who accesses a company's computer system in a manner that is adverse to her employer's interests. This would convert an ordinary violation of the duty of loyalty or of a confidentiality agreement into a federal offense. An employee does not lose "authorization" by accessing a computer with an improper purpose; rather, authorization is controlled by the employer, who may or may not terminate or restrict an employee's access privileges. *LVRC*, 581 F.3d at 1133.

In short, unless an individual lacks authorization to access a computer system, or exceeds the authorization that has been granted, there can be no violation of § 1030(a)(2)(C). The Government's argument that **Aleynikov**, who the Government concedes was authorized to access the Trading System's source code, violated § 1030(a)(2)(C) by misappropriating the source code must therefore be rejected. Accordingly, **Aleynikov's** motion to dismiss Count Three of the Indictment is granted.

CONCLUSION

Aleynikov's July 16 motion to dismiss the Indictment is denied with respect to Counts One and Two and granted with respect to Count Three. Count Three of the Indictment is dismissed.

SO ORDERED.

S.D.N.Y.,2010.

737 F.Supp.2d 173
(Cite as: 737 F.Supp.2d 173)

U.S. v. Aleynikov
737 F.Supp.2d 173

END OF DOCUMENT