

11-1074-cr
United States v. Agrawal

UNITED STATES COURT OF APPEALS

FOR THE SECOND CIRCUIT

August Term, 2011

(Argued: June 21, 2012 Decided: August 1, 2013)

Docket No. 11-1074-cr

UNITED STATES OF AMERICA,

Appellee,

v.

SAMARTH AGRAWAL,

Defendant-Appellant.

Before:

POOLER, RAGGI, and LYNCH, *Circuit Judges.*

On appeal from a judgment of conviction entered after a jury trial in the United States District Court for the Southern District of New York (Rakoff, *J.*), defendant challenges the legal sufficiency of charges that he violated the Economic Espionage Act, see 18 U.S.C. § 1832, and the National Stolen Property Act, see id. § 2314, particularly in light of our recent decision in United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012). He further challenges the sufficiency of the evidence to prove the § 2314 charge, complains of errors

in the jury charge, and argues constructive amendment of the indictment and prejudicial variance in proof.

AFFIRMED.

Judge Pooler concurs in part and dissents in part in a separate opinion.

MARSHALL A. MINTZ, Mintz & Oppenheim LLP, New York, New York, *for Defendant-Appellant*.

DANIEL W. LEVY (Thomas G. A. Brown, Justin S. Weddle, *on the brief*), Assistant United States Attorneys, *for* Preet Bharara, United States Attorney for the Southern District of New York, New York, New York, *for Appellee*.

REENA RAGGI, *Circuit Judge*:

Defendant Samarth Agrawal was entrusted by his former employer, the French bank Société Générale (“SocGen”), with access to confidential computer code that the bank used to conduct high frequency securities trades. Agrawal abused this trust by printing the code onto thousands of sheets of paper, which he then physically removed from the bank’s New York office to his New Jersey home, where he could use them to replicate SocGen’s trading systems for a competitor who promised to pay him hundreds of thousands of dollars. The question on this appeal is thus not whether Agrawal is a thief. He is. The question is whether Agrawal properly stands convicted for his thievery in the United States District Court for the Southern District of New York (Jed S. Rakoff, *Judge*) under specific federal laws, namely, the Economic Espionage Act (“EEA”), see 18 U.S.C. § 1832, and the National Stolen Property Act (“NSPA”), see id. § 2314.

Agrawal argues that the charges against him are legally insufficient to state offenses under these statutes, particularly in light of this court's recent decision in United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012) (reversing EEA and NSPA convictions on grounds of legal insufficiency). He further challenges the factual sufficiency of the evidence to support his NSPA conviction, complains of errors in the jury charge, and argues constructive amendment of the indictment and prejudicial variance in the proof. We reject these arguments and affirm the challenged conviction.

I. Background

A. Agrawal's Employment with Société Générale

The crimes at issue derive from Agrawal's employment between early 2007 and November 2009 at SocGen's New York offices. Agrawal began his career as a "quantitative analyst" in SocGen's High Frequency Trading ("HFT") Group. The HFT Group engaged in "index arbitrage," a process that seeks to profit by quickly exploiting fleeting differences in the prices of securities. Toward this end, the HFT Group used two computer trading systems, "ADP" and "DQS," to determine when to purchase and sell securities. Each system was made up of highly complicated computer code developed over the course of some years at a cost of several million dollars to SocGen. Using the ADP and DQS systems, the HFT Group executed trades that generated more than \$10 million in annual revenue for SocGen during 2007, 2008, and 2009.

As a quantitative analyst, Agrawal had no access to the code underlying the DQS or ADP systems. Rather, he developed "indicators" for others to use in refining the DQS system. Like other SocGen employees, however, Agrawal was required periodically to commit that neither during nor after his employment would he "disclose or furnish to any

entity . . . any confidential or proprietary information of [SocGen],” and that, upon termination, he would return all documents, papers, files, or other materials in his possession connected to SocGen. GX 3.

In April 2009, Agrawal was promoted to “trader” for DQS, a position that put him in charge of that system’s day-to-day operations. In this capacity, Agrawal spent several hours each week working with two SocGen computer programmers: Dominic Thuillier—who had written the underlying computer code for DQS—and Richad Idris. On June 12, 2009, Idris, following instructions from Agrawal’s supervisor, copied the DQS code into an electronic folder from which Agrawal could retrieve the data as necessary. In the process, Idris mistakenly also copied the code for three other systems, including ADP, into the folder, even though Agrawal was not authorized to have access to this additional code.

B. Agrawal Steals SocGen’s HFT Code and Offers To Duplicate Its Trading Systems for a Competitor

Unbeknownst to SocGen, Agrawal was then actively pursuing outside job opportunities. Toward that end, on June 8, 2009, he met with representatives of a New York-based hedge fund, Tower Research Capital (“Tower”). Agrawal told Tower that he was running one of SocGen’s two index arbitrage strategies, had a “complete understanding” of that strategy, and could help build a “very similar” system for Tower. Tr. 79.¹

On Saturday, June 13—five days after his meeting with Tower and the day after he acquired access to SocGen’s DQS code—Agrawal came into SocGen’s New York office,

¹ Less than a week before this meeting, a recruiter providing feedback by email on an interview Agrawal had had with another SocGen competitor, advised Agrawal to make clear to prospective employers that he possessed proprietary information. See GX 706.

printed out more than a thousand pages of the DQS code,² put the printed pages into a backpack, and physically transported the papers to his apartment in New Jersey. Three days later, on June 16, Agrawal again met with Tower partners to discuss replicating SocGen's HFT strategies for Tower. On July 10, Tower proposed to hire Agrawal for this purpose, offering him salary and bonuses exceeding \$500,000, plus 20% of profits generated by the anticipated DQS clone and 10% of profits from any ADP clone. Agrawal informally accepted Tower's offer in August 2009, but delayed disclosing this fact to SocGen for some months in order both to gain more experience with its HFT systems and to collect an anticipated bonus in October. Meanwhile, during August and September 2009, Agrawal copied and printed hundreds more pages of SocGen's HFT code—these pertaining primarily to the ADP code to which he had mistakenly been given access—and brought them to his home.

During these months, Agrawal also continued to meet with Tower partners, discussing the HFT systems he expected to develop for them and providing assurances that he could find out whatever information he needed about SocGen's systems to fill any gaps in his knowledge. At least one of those meetings was recorded by a Tower representative who was present.

Agrawal formally resigned from SocGen on November 17, 2009. In the week before

² SocGen had various methods in place preventing computers used to access HFT code from copying that information onto disks. Nevertheless, Agrawal was able to copy code onto paper by pasting parts into Microsoft Word documents to which he gave sequentially numbered names, such as "0.doc," "1.doc," and "2.doc," and then printing out those documents.

he gave notice, Agrawal deleted from SocGen's computer system the Word documents into which he had pasted DQS and ADP code, as well as the ADP code files that Idris had mistakenly copied for him. Agrawal's resignation triggered a leave period of several months, during which he was paid by SocGen but did little work for it. Although Agrawal was prohibited from working for any SocGen competitor while on leave, he continued to meet with Tower personnel, including the computer programmers who were to write the code that would replicate SocGen's two HFT systems. Agrawal provided Tower personnel with detailed handwritten descriptions of the HFT system he wanted them to build, including mathematical information derived from SocGen's code that he identified as "what is done in DQS." Tr. 621.³

C. Agrawal's Arrest and the Seizure of the Stolen Code

On April 19, 2010, the day Agrawal was to begin work at Tower, FBI agents arrested him at his home in New Jersey. Searches of his apartment resulted in the seizure of thousands of pages of carefully indexed and filed computer code pertaining to SocGen's two HFT systems. Agrawal admitted to an arresting agent that he had printed out the code and taken it home without disclosing that fact to his SocGen supervisors or receiving authorization to do so.

³ SocGen programmer Thuillier, the author of the DQS code, described some of Agrawal's notes as "pseudo code" in that it was a "simplified rewriting of the code in human language." Tr. 493, 623 ("It's just written in plain English. But it explains the algorithm. And it's scanning down the real time calculation loop of the DQS satellite into details.").

D. Agrawal's Prosecution and Conviction

On May 13, 2010, a grand jury sitting in the Southern District of New York charged Agrawal in a two-count indictment with violations of the EEA and the NSPA. After detailing pertinent facts in 18 numbered paragraphs, the indictment charged the two crimes both generally and specifically. With respect to the EEA, the indictment alleged as follows:

From at least on or about June 12, 2009, up through and including in or about April 2010, in the Southern District of New York and elsewhere, SAMARTH AGRAWAL, 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), 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, AGRAWAL, while in New York, New York, without authorization copied, printed and removed from the offices of the Financial Institution proprietary computer code for the Financial Institution's high frequency trading business, with the intent to use that code for the economic benefit of himself and others.

Indictment ¶ 19. With respect to the NSPA, the indictment alleged as follows:

From at least on or about June 12, 2009, up through and including in or about April 2010, in the Southern District of New York and elsewhere, SAMARTH AGRAWAL, 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, AGRAWAL, while in New York, New York, without authorization, removed from the offices of the Financial Institution proprietary computer code for the Financial Institution's high frequency trading business, the value of which exceeded \$5,000, and brought that stolen code to his home in Jersey City, New Jersey.

Indictment ¶ 21.

At trial, Agrawal testified in his own defense. Judge Rakoff would subsequently characterize this testimony as effectively “admitt[ing] under oath all of the elements of the charges.” Tr. 1211. Notably, Agrawal admitted that he had printed out SocGen’s DQS and ADP code and had taken the printed paper copies to his New Jersey home. He acknowledged that such information was proprietary to SocGen and that, nevertheless, he had shared some of it with Tower in order to facilitate his getting a job with that entity. What he denied was that, at the exact time he transported each stack of copied code from New York to New Jersey, his intent was to steal or convert it. He maintained that at that time, he intended to use the code for SocGen’s benefit by following through on a supervisor’s request that he work from home on a project to combine elements of the DQS and ADP systems. Only later, in Agrawal’s telling, did he decide to convert the code for his own benefit and Tower’s.⁴

Even before Agrawal gave this testimony, Judge Rakoff had cautioned that there was no basis in either the indictment or the law for requiring the government to prove that Agrawal possessed culpable intent at the precise time he printed and removed the HFT code from SocGen’s New York offices. Insofar as Agrawal purported to locate that requirement in the indictment’s “to wit” clauses, Judge Rakoff observed that those clauses could not be read in isolation or divorced from the preceding 18 paragraphs of the indictment, which indicated that the charged conduct spanned the period from June 12, 2009, through April

⁴ Agrawal’s testimony was refuted by the supervisor of SocGen’s HFT Group, who stated that a combination of the two systems made no sense as they were “totally distinct.” Tr. 1037. On this appeal we review the evidence in the light most favorable to the prosecution and, therefore, assume that the jury rejected any claim that Agrawal’s possession was authorized. See United States v. Broxmeyer, 616 F.3d 120, 125 (2d Cir. 2010).

2010. As to the law, Judge Rakoff concluded that the EEA’s intent element could be satisfied by proof that Agrawal possessed the requisite intent to convert when he “removed the code or at any point thereafter when he was still in unauthorized possession of the computer code,” and so charged the jury. Tr. 1006 (emphasis added). In so instructing the jury, Judge Rakoff explained that “without authorization” meant that SocGen “did not approve the removal of the computer code by the defendant for his intended purpose. For example, an employer might approve an employee taking a trade secret home to work on it for the employer’s benefit; but if the employee then starts using the trade secret for his own benefit or the benefit of another, at that point the removal becomes unauthorized.” *Id.* at 1314. Agrawal did not challenge this interpretation of the EEA, but maintained that to charge it in light of the “to wit” clause effected a constructive amendment of the indictment.

Judge Rakoff had also proposed to charge the jury that to convict Agrawal of the EEA count, the government had to prove that, “as a factual matter, the computer code was related to a product that was, at least in part, produced for, or placed in, interstate or foreign commerce.” Appellee’s Addendum 13. The government remarked that it did not “know[] exactly what the defense is going to argue on this particular point, if anything” and, therefore, requested that the court charge this element by reference to both statutory options, i.e., that the computer code was “related to” or “included in” a product produced for or placed in interstate or foreign commerce. Tr. 885. The court agreed to do so, but observed that it did not foresee this jurisdictional element being “a matter that is going to be materially disputed in any event.” *Id.* at 885–86. The defense never contended otherwise.⁵

⁵ Judge Rakoff’s prediction proved correct. In summation, the government argued this point only by reference to the computer code being “related to,” not “included in,” a product

Nor did the defense object to Judge Rakoff's further instruction as to how the government could satisfy this EEA element: "[I]t is sufficient if the government proves that the purpose of the computer code was to effectuate securities trades, at least some of which were in interstate or foreign commerce." *Id.* at 1315. Indeed, Agrawal never suggested to either the district court or the jury that the government had failed to plead or prove that SocGen's HFT computer code was related to or included in a product produced for or placed in interstate commerce. Rather, when, at the close of all the evidence, Agrawal moved to dismiss the indictment pursuant to Fed. R. Crim. P. 29, he argued only that the two counts "as explicated by the Court's charge and by the evidence presented by the government in this case constitute[d] a prejudicial variance and a constructive amendment of the charges of the grand jury indictment" as reflected in the "to wit" clauses. *Id.* at 1214. The court denied the motion, and the jury found Agrawal guilty on both the EEA and NSPA crimes charged.

Thereafter, Judge Rakoff calculated Agrawal's Sentencing Guidelines to recommend a prison sentence in the range of 63 to 78 months. Instead, on February 28, 2011, the court exercised its discretion to impose a non-Guidelines sentence of concurrent 36-month prison

that was produced for or placed in interstate or foreign commerce:

The code, you didn't hear a lot about this, but the code was related to a product that was produced for or placed in interstate or foreign commerce. It is one of the requirements that Judge Rakoff will tell you about. There is plenty of interstate commerce here. You remember that one of the things the [HFT] system is designed to do is trade stocks, the indexes associated with those stocks and futures. A couple witnesses talked about where futures were traded on the America[n] Stock Exchange and not shockingly Chicago. That is plenty of interstate [commerce]. That is satisfied.

Tr. 1258 (emphasis added). The defense made no mention in summation of the EEA's jurisdictional element.

terms on the two counts of conviction. This timely appeal followed.

II. Discussion

A. Legal Sufficiency of the Charges

1. Standard of Review

Agrawal challenges the legal sufficiency of both counts of the indictment. As to Count One, he argues that, insofar as the trade secret at issue, SocGen’s computer code, was “included in” SocGen’s HFT systems, those internal, confidential systems cannot qualify as “product[s] . . . produced for or placed in interstate or foreign commerce” as required by the EEA. 18 U.S.C. § 1832(a)(2) (emphasis added). As to Count Two, Agrawal asserts that SocGen’s computer code is intangible property and, as such, not “goods, wares, or merchandise” as required by the NSPA. *Id.* § 2314. Neither argument was ever raised below.

We generally review a challenge to the legal sufficiency of an indictment de novo. See United States v. Shellef, 507 F.3d 82, 104 (2d Cir. 2007). Where, as here, however, a defendant failed to raise a sufficiency objection in the district court and presents it for the first time on appeal, we review for plain error. See United States v. Cotton, 535 U.S. 625, 631 (2002) (applying plain-error review to defective indictment claim); United States v. Nkansah, 699 F.3d 743, 752 (2d Cir. 2012); United States v. Doe, 297 F.3d 76, 81 (2d Cir. 2002). Under that standard,

an appellate court may, in its discretion, correct an error not raised at trial only where the appellant demonstrates that (1) there is an error; (2) the error is clear or obvious, rather than subject to reasonable dispute; (3) the error affected the appellant’s substantial rights, which in the ordinary case means it affected the outcome of the district court proceedings; and (4) the error seriously affect[s] the fairness, integrity or public reputation of judicial proceedings.

United States v. Marcus, 130 S. Ct. 2159, 2164 (2010) (internal quotation marks omitted).

In attempting to demonstrate plain error, Agrawal is entitled to the benefit of our recent decision in United States v. Aleynikov, 676 F.3d 71. See United States v. Garcia, 587 F.3d 509, 520 (2d Cir. 2009) (instructing that whether error is “plain” is determined by reference to law at time of appeal); see also Henderson v. United States, 133 S. Ct. 1121, 1126 (2013) (holding that court of appeals is bound by law as it exists at time of appeal); Johnson v. United States, 520 U.S. 461, 468 (1997) (“[I]t is enough that an error be ‘plain’ at the time of appellate consideration.”). In Aleynikov, another dishonest employee, this one employed by Goldman Sachs, also stole proprietary trading code, in that case by uploading more than 500,000 lines of code to a third-party computer server in Germany, downloading the code from that server to his home computer, and then electronically copying some of the files to other computer devices that he owned. See 676 F.3d at 74. This court reversed defendant’s EEA conviction, holding that to the extent such code was “included in” the employer’s confidential trading system, that system was not “a product that is produced for or placed in interstate or foreign commerce,” as required by the EEA, 18 U.S.C. § 1832(a)(2), because the employer never intended to sell or license the system but, rather, went to great lengths to maintain its secrecy, see United States v. Aleynikov, 676 F.3d at 82. The court further reversed defendant’s NSPA conviction, holding that the code, stolen entirely in electronic form, was not tangible property, as necessary to qualify as “goods, wares, [or] merchandise” under 18 U.S.C. § 2314. See id. at 76–79.

While Aleynikov’s construction of the EEA and NSPA controls on the matters it decides, Agrawal’s case is distinguishable from Aleynikov in important respects that

preclude him from demonstrating plain error in the legal sufficiency of his indictment. We here briefly summarize what we explain further in this opinion.⁶

As to the EEA charge, in this case, neither the indictment nor the prosecution’s arguments or the court’s charge identified SocGen’s confidential HFT systems as the “product” relied on to satisfy the crime’s jurisdictional element. Rather, the record indicates that the relevant product was the publicly traded securities bought and sold by SocGen using its HFT systems. Because such securities satisfy the EEA’s jurisdictional element without raising the concerns identified in Aleynikov, Agrawal cannot demonstrate that any pleading insufficiency with respect to SocGen’s HFT systems affected his substantial rights, much less the fairness, integrity, or public reputation of judicial proceedings.

Insofar as Agrawal invokes Yates v. United States, 354 U.S. 298 (1957), to urge otherwise, faulting the indictment and charge for failing to specify that only securities, and not SocGen’s HFT systems, could satisfy the EEA’s product requirement, we similarly review only for plain error because no such objection was ever raised in the district court. Agrawal cannot demonstrate Yates error because neither the prosecution nor the court ever presented SocGen’s HFT systems to the jury as “products” satisfying the EEA’s jurisdictional element. In any event, any such error would not be “plain,” because the only

⁶ The overall tenor of the dissenting opinion is that, in affirming Agrawal’s conviction, we fail to respect the precedent set by the reversal in Aleynikov. That suggestion considerably over-reads the precedential force of Aleynikov. That case establishes that the jury instructions in Aleynikov permitted the jury to convict on a legally invalid theory. It does not, and cannot, establish that the kind of conduct in which Aleynikov and Agrawal engaged is intrinsically legal, and it does not address, let alone reject, the theory on which Agrawal was convicted. Neither the jury instructions nor the prosecution’s summation in this case proffered to the jury the theory on which Aleynikov’s conviction was based, and Agrawal did not seek any instruction specifically disavowing that theory. In short, nothing we say or do today is inconsistent with the reversal of Aleynikov’s conviction.

possible basis for treating confidential trading systems as products produced for or placed in interstate commerce was that such systems are used to buy and sell securities traded in interstate commerce. In short, no jury could find SocGen's HFT systems to qualify as EEA products (impermissibly, after Aleynikov), without first finding that the securities traded using those systems were such products. In these circumstances, any Yates error in failing to distinguish between the two possible products could not have affected either Agrawal's substantial rights or the fairness, integrity, or public reputation of judicial proceedings.

As to the NSPA charge, Agrawal's legal-sufficiency challenge fails at the first step of plain-error analysis. Because Agrawal—unlike Aleynikov—stole the computer code in a tangible rather than intangible form, i.e., printed onto thousands of sheets of paper, he cannot demonstrate any error, let alone plain error, in charging him with the theft of “goods, wares, [or] merchandise.” 18 U.S.C. § 2314.

2. Count One (EEA)

a. The Alleged Securities Publicly Traded Using SocGen's Confidential Computer Code Were Legally Sufficient To Satisfy the Product and Nexus Requirements of the EEA's Jurisdictional Element

The Electronic Espionage Act, as in effect at the time of Agrawal's indictment and conviction, stated in relevant part as follows:

Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret, knowingly—

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates or conveys such information; [or]

(3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

...
[is guilty of a crime].

18 U.S.C. § 1832 (emphasis added). The highlighted statutory language—the jurisdictional element of the statute—is the focus of Agrawal’s sufficiency challenge.

In United States v. Aleynikov, this court construed the phrase “a product that is produced for or placed in interstate or foreign commerce” as a “limitation” on the scope of the EEA, 676 F.3d at 79, signaling that Congress did not intend to invoke its full Commerce Clause power to criminalize the theft of trade secrets, see id. at 81–82 (citing Supreme Court cases distinguishing between legislation invoking Congress’s full power over activity substantially “affecting commerce” and legislation using more limiting language).⁷

⁷ Aleynikov’s identification of a congressional intent to limit the reach of the EEA has since been disavowed by Congress itself, which quickly amended the EEA to remove the purportedly limiting language and to clarify its intent to reach broadly in protecting against the theft of trade secrets. See Theft of Trade Secrets Clarification Act of 2012, Pub. L. No. 112-236, 126 Stat. 1627 (providing for EEA to be amended to strike phrase “or included in a product that is produced for or placed in” and to insert phrase “a product or service used in or intended for use in,” so that relevant language now reads: “Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce”); 158 Cong. Rec. S6978-03 (daily ed. Nov. 27, 2012) (statement of Sen. Leahy) (observing that Aleynikov decision “cast doubt on the reach” of EEA, and that “clarifying legislation that the Senate will pass today corrects the court’s narrow reading to ensure that our federal criminal laws adequately address the theft of trade secrets” (emphasis added)).

On this appeal, we have no occasion to construe the revised EEA. Rather, we are obliged to apply the EEA as it existed at the time of Agrawal’s conviction and as construed

Aleynikov explained that for a product to be “placed in” commerce, it must have “already been introduced into the stream of commerce and have reached the marketplace.” Id. at 80. Products “being developed or readied for the marketplace” qualified “as being ‘produced for,’ if not yet actually ‘placed in,’ commerce.” Id. But a “product” could not be deemed “produced for” commerce simply because its “purpose is to facilitate or engage in such commerce”; such a construction of the EEA’s product requirement would deprive the statutory language of any limiting effect. Id. at 80–81 & n.5 (noting that government had been “unable to identify a single product that affects interstate commerce but that would nonetheless be excluded by virtue of the statute’s limiting language”).

Aleynikov’s construction of the phrase “a product that is produced for or placed in interstate commerce” controls on this appeal. We note, however, that the reversal of Aleynikov’s EEA conviction was based on the application of that phrase to the particular “product” that was the basis of the jurisdictional allegation in his case. As we explain below, the present case was submitted to the jury on a very different product theory than that relied on in Aleynikov. Thus, the same construction that prompted reversal in Aleynikov leads to affirmance here.

In Aleynikov, the EEA charge was submitted to the jury on the theory that the trade secret converted by the defendant, i.e., the proprietary computer code, was “included in” a single product: Goldman Sachs’s confidential trading system. The jury instructions in

in Aleynikov. See Collins v. Youngblood, 497 U.S. 37, 41 (1990).

Aleynikov unambiguously stated that “[t]he indictment [in that case] charges that the Goldman Sachs high-frequency trading platform is a product,” and that the jury’s responsibility was to “determin[e] whether the trading platform was produced for or placed in interstate or foreign commerce.” United States v. Aleynikov, No. 10-cr-96 (DLC), Tr. 1546–47 (emphasis added). This had been the court’s and the parties’ understanding of the Aleynikov indictment from the start. In its opinion denying the defendant’s motion to dismiss the indictment, the court noted the parties’ agreement “that the trade secret at issue in [the EEA Count] is the source code, and that the relevant ‘product’ is the Trading System.” United States v. Aleynikov, 737 F. Supp. 2d 173, 178 (S.D.N.Y. 2010). It was on this understanding that this court held the Aleynikov indictment legally insufficient. As Aleynikov construed the phrase “a product that is produced for or placed in interstate or foreign commerce,” Goldman Sachs’s trading system could not constitute such a product because Goldman Sachs “had no intention of selling its HFT system or licensing it to anyone.” United States v. Aleynikov, 676 F.3d at 82. To the contrary, the value of the system depended entirely on preserving its secrecy. See id.

Agrawal submits that Aleynikov mandates the same conclusion here because the computer code at issue, like the code in Aleynikov, was included in a confidential HFT system. But this case differs from Aleynikov in an important respect. Here, neither the prosecution nor the district court presented the case to the jury on the theory that SocGen’s trading system was the “product” placed in interstate commerce. Nor did they suggest that

the EEA’s jurisdictional nexus was satisfied by computer code (the stolen trade secret) being “included in” that “product.” Rather, the record reveals that EEA jurisdiction was here put to the jury on a more obvious, convincing—and legally sufficient—theory that was not pursued and, therefore, not addressed in Aleynikov: that the securities traded by SocGen using its HFT systems, rather than the systems themselves, were the “product[s] . . . placed in” interstate commerce. Under that theory, the jurisdictional nexus was satisfied because SocGen’s stolen computer code “related to” the securities (the product) it identified for purchase and sale.

While Agrawal’s indictment did not state this theory in so many words, it did allege that SocGen engaged in “high-frequency trading in securities” on national markets “such as the New York Stock Exchange and NASDAQ Stock Market.” Indictment ¶¶ 1, 4. This effectively identified securities as products traded in interstate commerce.⁸ At trial, the

⁸ Agrawal does not contend that securities are not “products.” See Webster’s 3d New Int’l Dictionary 1810 (1986) (defining “product” as “something produced by physical labor or intellectual effort: the result of work or thought”); Dow Jones Co. v. Int’l Sec. Exch., 451 F.3d 295, 304 n.10 (2d Cir. 2006) (discussing “intellectual-property rights in the securities designed according to the plaintiff’s proprietary formulas”). Indeed, securities are routinely discussed as products by the Securities and Exchange Commission, the administrative agency principally charged with enforcing federal securities laws, see Asset-Backed Securities, SEC Release Nos. 33-9117, 34-61858, 2010 WL 1389116 (Apr. 7, 2010) (“Throughout this release, we refer to the securities sold through such vehicles as asset-based securities, ABS, or structured finance products.” (emphasis added)); by Congress, see 15 U.S.C. § 78c(a)(56) (defining “securities futures product” as “security future or any put, call, straddle, option, or privilege on any security future”); and by this and other courts, see Burns v. N.Y. Life Ins. Co., 202 F.3d 616, 618 (2d Cir. 2000) (referring to entity as “registered broker-dealer of securities products”); see also United States v. Laurienti, 611 F.3d 530, 542 (9th Cir. 2010) (discussing broker’s disclosure obligations “on client purchases of particular securities products”); Gurfel v. SEC, 205 F.3d 400, 400 (D.C. Cir. 2000) (observing that petitioner

prosecution offered evidence proving the allegation. Moreover, in summation, it argued that although little had been said about the requirement that the stolen computer code “relate[] to a product that was produced for or placed in interstate or foreign commerce,” the element was satisfied by evidence that SocGen’s trading system was designed to buy and sell “stocks and futures” on national exchanges. Tr. 1258. To be sure, in Aleynikov, the prosecution made a virtually identical argument, see United States v. Aleynikov, No. 10-cr-96 (DLC), Tr. 1485–86, but in that case, as we have already observed, the government and the court elsewhere specifically identified the trading system as the relevant product. Where, as here, no pleading, argument, or charge ever labeled SocGen’s trading system a product—much less the product produced for or placed in interstate commerce on which the government relied to satisfy the EEA’s jurisdictional element—the quoted government argument is more reasonably understood to identify the stocks and futures bought and sold on national exchanges as the products placed in interstate commerce. Indeed, the district court

“sold securities products to investors”). Nor is there any question that securities publicly traded on national exchanges—their marketplace—have been “placed in” interstate commerce. See United States v. Aleynikov, 676 F.3d at 80 (stating that product is “placed in interstate or foreign commerce” where it has “been introduced into the stream of commerce and has reached the marketplace”). To the extent our dissenting colleague, Judge Pooler, submits that securities not produced by SocGen could not satisfy the “product” element of the EEA count against Agrawal, see post at [8] n.6, we here reject that contention. Nothing in the statutory text, nor anything in Aleynikov’s construction of that text, requires that the “product” at issue in an EEA prosecution be produced by the owner of the misappropriated trade secret. The statute requires only that the stolen trade secret be related to or included in a product produced for or placed in interstate commerce, a requirement which can be satisfied without regard to whether the owner of the trade secret and the producer of the product are one and the same.

effectively clarified this point by referencing only securities as the relevant product in charging the jury on the EEA's jurisdictional element: "[I]t is sufficient if the government proves that the purpose of the computer code [*i.e.*, the trade secret at issue] was to effectuate securities trades, at least some of which were in interstate or foreign commerce." Tr. 1315. In contrast to Aleynikov, the court here made no mention of the confidential HFT system. Of course, the EEA further requires a nexus between the converted trade secret and the product produced for or placed in interstate commerce. See 18 U.S.C. § 1832(a) (requiring that trade secret "relate[] to" or be "included in" product). In Aleynikov, where the employer's HFT system was the sole product at issue, the prosecution contended that the stolen computer code was included in that product. Where, as here, the relevant product is publicly traded securities, the statute's "related to" provision comes into play: Was the stolen code related to traded securities? We answer that question "yes."

In so doing, we note that Aleynikov never had to construe the EEA's "related to" or "included in" provision because it determined that Goldman Sachs's confidential HFT system was not a product produced for or placed in interstate commerce.⁹ Nevertheless,

⁹ As a result, any language in Aleynikov construing the nexus requirement is, of course, dictum. Our dissenting colleague nevertheless faults us for "fail[ing] to meaningfully address" language from Aleynikov—which she initially characterizes as a "hint," post at [9], but later upgrades to a "conclu[sion]," post at [10]—limiting the EEA to trade secrets "designed . . . to make" a product passing in commerce. United States v. Aleynikov, 676 F.3d at 82. This stray remark is dictum, and we decline to adopt it as holding. Indeed, to do so would preclude the EEA from reaching several types of trade secret that both the House and Senate Reports supplied as exemplary: to wit, "bid estimates [and] production schedules," post at [11]. Both of these are quintessentially protected by the EEA, but neither "make[s]" a product or "give[s] detailed instructions on how to create" a

Aleynikov is instructive for our own assessment of the nexus provision insofar as it cites the “basic interpretive canon” that a statute should be construed to give effect to “all its provisions, so that no part will be inoperative or superfluous.” 676 F.3d at 81 (internal quotation marks omitted). Consistent with this canon, the term “related to” cannot be construed as coextensive with “included in.” Rather, the nexus provision must be read to indicate that a trade secret may relate to a product placed in or produced for interstate commerce, without being included in that product.

As the Supreme Court has recognized, the ordinary meaning of “related to” is “broad”: “‘to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with.’” Morales v. Trans World Airlines, 504 U.S. 374, 383 (1992) (quoting Black’s Law Dictionary 1158 (5th ed. 1979)) (holding state airfare-advertisement rules preempted by federal statute as “relating to [air carriers’] rates, routes, or services”); see Shaw v. Delta Air Lines, Inc., 463 U.S. 85, 97 (1983) (observing that law “‘relates to’ an employee benefit plan, in the normal sense of the phrase, if it has a connection with or reference to such a plan,” and on this basis holding state statute preempted in part by ERISA). For this reason, the Supreme Court has cautioned that the term must be read in context. For example, where “related to” is used in legislation creating a discrete exception to a general rule, it may not be construed so expansively as to swallow the general rule. See, e.g., New York Conf. of Blue Cross v. Travelers Ins., 514 U.S. 645,

product, the limitations Judge Pooler attempts to locate in or derive from Aleynikov. Post at [11].

655 (1995) (declining to accord usual expansive meaning to term “related to” in construing ERISA preemption provision where general presumption against preemption would thereby be “read . . . out of the law”); Havana Club Holding, S.A. v. Galleon S.A., 203 F.3d 116, 123 (2d Cir. 2000) (declining to accord broad construction to term “related to” as used in statutory exception to prohibition because doing so would swallow much of prohibition). No such concern arises here, despite our colleague’s conclusory contention otherwise. See post at [10]. The EEA’s nexus provision creates no exception to an otherwise applicable general rule; rather, it signals Congress’s intent to exercise its Commerce Clause authority to address the theft of trade secrets. See generally S. Rep. No. 104-359, at 13-14 (1996) (stating intent to “promote the development and lawful utilization of proprietary economic information by protecting it from theft, unauthorized misappropriation or conversion”).

To be sure, in Aleynikov, the court concluded that Congress did not exercise its full Commerce Clause authority in the EEA because it limited the products that could satisfy the statute’s jurisdictional requirement to those “produced for or placed in” interstate commerce. The statutory text provides no similar basis for concluding that, once a product so produced or so placed is identified, Congress intended further to limit the EEA’s reach through a restrictive nexus provision. The use of so deliberately expansive a term as “related to” hardly signals such intent. Nor can it be inferred from the EEA’s legislative history. See generally H.R. Rep. No. 104-788 (indicating intent to protect not only trade secrets integral to “product,” such as “production processes” and “technology schematics,” but also trade

secrets some levels removed therefrom, such as “bid estimates” and “production schedules”). Accordingly, we conclude that the term “related to,” as used in the EEA’s nexus provision, is intended to reach broadly rather than narrowly, consistent with its usual meaning.¹⁰

On this appeal, we need not delineate the outer limits of that reach because we easily conclude that SocGen’s HFT code related to publicly traded securities in such a way as to bring the theft of the HFT code within the EEA. The code existed for the sole purpose of trading in securities, and its considerable value derived entirely from the existence of a market for securities. In short, the confidential code was valuable only in relation to the securities whose interstate trades it facilitated.

Because publicly traded securities thus satisfy the product and nexus requirements of the EEA’s jurisdictional element, Agrawal cannot satisfy the final two prongs of plain-error review in complaining of legal insufficiency in the pleading or proof of this element.

b. Agrawal Cannot Demonstrate Plain *Yates* Error

Rather than dispute that securities are products placed in interstate and foreign commerce or that SocGen’s HFT computer code related to such securities, Agrawal argues on this appeal that the government should not be permitted to rely on securities to defeat his legal sufficiency challenge to the EEA charge because securities were never specifically identified as the product relevant to EEA jurisdiction in the district court. Further, he asserts that to allow the government to argue that securities could support the EEA’s jurisdictional

¹⁰ Nothing in Congress’s recent amendment of the EEA, which establishes “related to” as the statute’s sole nexus requirement, see supra n.6, supports a different conclusion.

element even if SocGen’s HFT system could not, would run afoul of Yates v. United States, 354 U.S. at 311 (identifying error in conviction if “verdict is supportable on one ground but not on another, and it is impossible to tell which ground the jury selected”).

The first part of Agrawal’s argument rests on a mistaken factual premise. As we have discussed supra at [19–21], the record shows that the district court’s jury instructions specifically cast the jurisdictional issue by reference only to “securities, at least some of which were in interstate or foreign commerce,” Tr. 1315, with no mention of the confidential trading system. To the extent Agrawal faults the indictment for failing to specify securities as the jurisdictionally relevant product, this argument is unconvincing because the indictment does not specifically identify anything as the product relied on to satisfy the jurisdictional element.¹¹ If, as Agrawal now contends, SocGen’s confidential HFT system could not, as a matter of law, be the product supporting jurisdiction, he can hardly claim, in the absence of any pleading, argument, or charge identifying it as such, that he or the jury would reasonably have understood that system to be the alleged basis for jurisdiction rather than the securities that were repeatedly identified at trial as items traded in interstate commerce.¹²

¹¹ Judge Pooler asserts that the indictment “clearly allege[s] . . . that SocGen’s product was ‘the Financial Institution’s high frequency trading business.’” Post at 5 (quoting Indictment ¶ 19). In fact, the indictment never refers to the trading business as being SocGen’s “product” for EEA purposes. The quoted excerpt alleges only that Agrawal stole “computer code for the Financial Institution’s high frequency trading business,” a context that explains why the code was a trade secret, not that the “business” was a product. Nor can this excerpt be read “clearly to allege” that the HFT system was the relevant EEA “product.”

¹² In its initial brief on appeal, the government did argue that SocGen’s HFT system satisfied the product requirement of the EEA’s jurisdictional element. In a supplemental brief filed after Aleynikov, it submitted that the securities traded by the HFT system also

As for Agrawal’s Yates argument, we note that, before the district court, he never faulted the indictment for failing to specify the product establishing jurisdiction, never sought particulars on this point, and never suggested to the district judge that allowing the case to go to the jury without clarifying the specific product at issue risked Yates error. The reason for the omission is obvious from the record. Agrawal made what the district court characterized as “a calculated strategic call,” Sent. Tr. 32, effectively to concede “all elements of the [EEA] charge,” id. at 30, including jurisdiction, see Tr. 885–86 (recording Judge Rakoff’s prescient observation at charging conference discussion of EEA jurisdiction element that “[t]his is, I have a feeling, not a matter that is going to be materially disputed in any event”). Instead, he pursued a narrowly focused defense, i.e., that “not under the law generally but under the terms of the indictment,” he could not be found guilty because “at the moment he took the codes home, he had not yet formed an intent to give them to Tower.” Sent. Tr. 29 (recording Judge Rakoff’s characterization of defense theory). It is not surprising that, having failed to succeed on this theory, Agrawal belatedly attempts to identify other errors on appeal. But his unpreserved Yates challenge to securities as the products satisfying EEA jurisdiction, like his unpreserved challenge to SocGen’s HFT system as the product satisfying jurisdiction, is reviewable only for plain error. See United States v. Skelly, 442 F.3d 94, 99 (2d Cir. 2006) (declining to reverse on basis of unpreserved

satisfied the EEA’s product requirement. Our dissenting colleague highlights these developments. See post at [6]. The issue before us, however, is not what positions the government has taken after trial, but the legal sufficiency of the charge presented to the jury at trial, considered for plain error in light of Agrawal’s failure to object.

Yates challenge in absence of plain error); United States v. Thomas, 54 F.3d 73, 79–80 (2d Cir. 1995) (reviewing forfeited Yates challenge for plain error). Agrawal cannot satisfy any of the requirements of plain error.

A Yates concern arises where disjunctive theories of culpability are submitted to a jury that returns a general verdict of guilty, and “[one] of the theories was legally insufficient.” United States v. Garcia, 992 F.2d 409, 416 (2d Cir. 1993). In such circumstances, “it is impossible to tell which ground the jury selected,” the legally sufficient ground or the insufficient one. Yates v. United States, 354 U.S. at 312.

Agrawal cannot demonstrate Yates error here because his conviction presents no such ambiguity. The jury was not presented with both a legally sufficient and an insufficient theory of jurisdiction. Rather, it was presented with a single sufficient theory: that SocGen’s stolen computer code was related to the securities it was used to trade, which securities were products “produced for or placed in” interstate commerce. See supra at [19–21]. To the extent Agrawal urges otherwise by arguing that the jury might nevertheless have relied on SocGen’s trading system as the relevant product, he points to nothing in the record to raise the argument above the merely speculative. Indeed, such speculation is unwarranted in light of Judge Rakoff’s instruction specifically casting the jurisdictional issue by reference only to securities. See id. at [21]. Thus, we identify no Yates error in this case.

Further, even if it might have been helpful, in hindsight, explicitly to instruct the jury that SocGen’s HFT system could not be the product supporting EEA jurisdiction—an

instruction Agrawal never sought—Agrawal points to no authority requiring such specificity and, thus, cannot demonstrate error that was “clear or obvious.” United States v. Marcus, 130 S. Ct. at 2164 (stating that second criterion of plain-error standard requires that error be “clear or obvious, rather than subject to reasonable dispute” (internal quotation marks omitted)). Even Aleynikov, in holding that confidential trading systems cannot, as a matter of law, qualify as products supporting EEA jurisdiction, nowhere states that an indictment must specifically disavow jurisdictional reliance on such a confidential system or that the court must so instruct the jury in the absence of a request to charge. And certainly Agrawal cites us to no case identifying Yates error based on insufficient theories of culpability that a jury might have conjured for itself even though they were not argued by the prosecution or charged by the court.

In any event, even if Agrawal could demonstrate (1) Yates error that (2) was “clear or obvious,” he cannot show “a reasonable probability that the error affected the outcome of [his] trial,” as necessary to demonstrate the requisite adverse effect on his substantial rights. Id. Much less can he show that the error seriously affected the fairness, integrity, or public reputation of judicial proceedings. This is because it would be impossible for a jury to find that SocGen’s HFT system was a product produced for interstate commerce without also finding that the securities traded through that system were products placed in interstate commerce. On this point, the government argued in summation that “one of the things [SocGen’s HFT] system is designed to do is trade stocks, the indexes associated with those

stocks and futures. A couple [of] witnesses talked about where futures were traded on the America[n] Stock Exchange and not shockingly Chicago. That is plenty of interstate [commerce].” Tr. 1258. In Aleynikov, this court ruled that a connection between a confidential trading system and publicly traded securities was legally insufficient to make the system itself a product produced for or placed in interstate commerce. Nevertheless, any impermissible finding here that such a trading system satisfied the EEA’s product requirement could only derive from a permissible finding that the securities traded by the system were themselves products placed in interstate commerce. Thus, there is no basis for concluding that any Yates error seriously affected the outcome of Agrawal’s trial.

For reasons already discussed, the conclusion that securities traded on national exchanges are products placed in interstate and foreign commerce is beyond dispute. So too the conclusion that computer code whose sole purpose is to identify the securities to be traded “relates to” those securities. In these circumstances, and with Agrawal having admitted under oath that he copied SocGen’s proprietary code, transported it interstate, and converted it without SocGen’s authorization to benefit himself and a SocGen competitor, we conclude that the evidence of Agrawal’s guilt is so “overwhelming” and “uncontroverted” that “there is no basis for concluding that the error seriously affected the fairness, integrity or public reputation of judicial proceedings. Indeed, it would be the reversal of a conviction such as this which would have that effect.” Johnson v. United States, 520 U.S. at 470

(alteration and internal quotation marks omitted); see United States v. Marcus, 130 S. Ct. at 2166; United States v. Cotton, 535 U.S. at 633.

We therefore reject Agrawal’s legal sufficiency challenge to the EEA charge in this case.

3. NSPA

The National Stolen Property Act states in relevant part as follows:

Whoever transports, transmits, or transfers 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 . . . [is guilty of a crime].

18 U.S.C. § 2314. In United States v. Aleynikov, this court carefully reviewed Supreme Court and circuit precedent construing the phrase “goods, wares, [or] merchandise” and concluded that “[s]ome tangible property must be taken from the owner for there to be deemed a ‘good’ that is ‘stolen’ for purposes of the NSPA.” 676 F.3d at 77. The theft of “purely intangible property embodied in a purely intangible format,” such as the trading system at issue in that case, does not state an offense under the NSPA. Id. at 78.

Relying on Aleynikov, Agrawal challenges the legal sufficiency of his NSPA charge, complaining that he too is accused of stealing computer code constituting only intangible property. The argument fails because it ignores Aleynikov’s emphasis on the format in which intellectual property is taken. In Aleynikov, the defendant stole computer code in an intangible form, electronically downloading the code to a server in Germany and then from that server to his own computer. See id. at 74. By contrast, Agrawal stole computer code

in the tangible form of thousands of sheets of paper, which paper he then transported to his home in New Jersey. This makes all the difference. See id. at 78 (citing approvingly to United States v. Martin, 228 F.3d 1, 14–15 (1st Cir. 2000) (stating that, although NSPA does not criminalize theft of purely intangible information, statute “does apply when there has been some tangible item taken, however insignificant or valueless it may be, absent the intangible component” (emphasis in original; internal quotation marks omitted))). As Aleynikov explained, a defendant who transfers code electronically never assumes “physical control” over anything tangible. Id. By contrast, a defendant such as Agrawal, who steals papers on which intangible intellectual property is reproduced, does assume physical control over something tangible as is necessary for the item “to be a ‘good’ . . . for purposes of the NSPA.” Id. at 77.¹³

This construction of the NSPA comports with our discussion of the statute in United States v. Bottone, 365 F.2d 389 (2d Cir. 1966) (Friendly, J.). We there concluded “that papers describing manufacturing procedures are goods, wares, or merchandise.” Id. at 393.

¹³ Agrawal submits that the indictment charged only that he transported “computer code,” with no mention of paper printouts. Indictment ¶ 21; see United States v. Stafford, 136 F.3d 1109, 1114–15 (7th Cir. 1998) (dismissing NSPA count under similar circumstances). Assuming without deciding that this omission was error that was plain, Agrawal cannot demonstrate that it affected either his substantial rights or the fairness, integrity, or public reputation of judicial proceedings, in light of overwhelming evidence that the computer code was stolen in a paper format and because Agrawal had ample notice of this fact before trial. Indeed, Agrawal could hardly claim otherwise in light of his post-arrest admissions to creating and transporting the paper copies of the code, his presence at the seizure of the papers from his home, and the government’s discovery disclosure of those papers.

Further, we regarded it as settled that the unauthorized removal from a company's office of such papers, "made in the company's office, on its paper and with its equipment," sufficed to state an NSPA offense. Id. At issue in Bottone was whether an NSPA offense was stated where a defendant removed documents from a company's files, made photocopies at another location, and then restored the purloined originals to the files. In concluding that it was, we observed 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," but that "where tangible goods are stolen and transported and the only obstacle to condemnation is a clever intermediate transcription or use of a photocopy machine . . . the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial." Id. at 393–94.

Here, Agrawal produced paper copies of SocGen's computer code "in the company's office, on its paper and with its equipment." Id. at 393. The fact that the code had been in an intangible form before Agrawal, a SocGen employee, himself reproduced it on company paper is irrelevant. The papers belonged to SocGen, not Agrawal. When Agrawal removed this tangible property from SocGen's offices without authorization, and transported it to his home in New Jersey, he was engaged in the theft or conversion of a "good" in violation of the NSPA.

Had Agrawal stolen the code in intangible form, as the defendant in Aleynikov had done, and only later copied it onto paper or some other tangible medium, that would not be

enough to “transform the intangible property into a stolen good” so as to state an NSPA offense. United States v. Aleynikov, 676 F.3d at 78. Indeed, that conclusion is dictated not only by Aleynikov, but by Dowling v. United States, 473 U.S. 207 (1985). In that case, the Supreme Court held that the NSPA was not violated by the interstate transportation of “bootleg” phonograph recordings where neither the recordings themselves, nor any other tangible property, were themselves stolen or converted but, rather, they “embodied performances of musical compositions that Dowling had no right to distribute.” Id. at 214–15 (noting that government did not contend that defendant “wrongfully came by the phonorecords actually shipped or the physical materials from which they were made”). The Supreme Court reasoned that the NSPA “seems clearly to contemplate a physical identity between the items unlawfully obtained and those eventually transported, and hence some prior physical taking of the subject goods.” Id. at 216 (recognizing nevertheless that “courts interpreting § 2314 have never required, of course, that the items stolen and transported remain in entirely unaltered form”).

In this case, there is no question as to such physical identity or prior physical taking. At the moment Agrawal removed SocGen’s HFT code from SocGen’s office and transported it across state lines, the code was in the tangible form of thousands of sheets of paper. By comparison, at the moment of the code’s theft in Aleynikov, its form was intangible and remained so as it was transmitted from Goldman Sachs’s servers to a server in Germany and then to defendant’s own computer. The fact that the papers stolen by Agrawal derived

almost all of their value from the otherwise intangible intellectual property printed thereon does not alter the fact that the papers were “goods” whose theft is proscribed by the NSPA. Although the court was not required to decide in Aleynikov in what tangible formats the theft of intellectual property would constitute “a physical theft” for purposes of the NSPA, United States v. Aleynikov, 676 F.3d at 78 (discussing possibility of computer code’s being stolen on “compact disc or thumb drive”), it did recognize that “in virtually every case involving proprietary computer code worth stealing, the value of the intangible code will vastly exceed the value of any physical item on which it might be stored,” id. at 79; see United States v. Martin, 228 F.3d at 14–15. More to the point, in Dowling v. United States, the Supreme Court expressly stated that, as long as the stolen item qualifies as “physical ‘goods, wares, [or] merchandise,’” 473 U.S. at 216 (quoting 18 U.S.C. § 2314), it does not “matter that the item owes a major portion of its value to an intangible component,” id. This comports with our own decision in United States v. Bottone, which specifically rejected the argument that NSPA culpability could not exist where “the physical form of the stolen goods is secondary in every respect to the matter recorded in them.” 365 F.3d at 393–94.

In sum, while Dowling, Aleynikov, and Bottone instruct that the NSPA’s reference to “goods, wares [or] merchandise,” does not permit a defendant to be prosecuted under that statute for stealing intangible property in a purely intangible form, no such error is present in this case where the defendant stole complex computer code in the tangible form of thousands of sheets of paper.

We recognize that, in terms of moral culpability, there may be little to distinguish Agrawal from the defendant in Aleynikov. But it is Congress's task, not the courts', to define crimes and prescribe punishments. See Dowling v. United States, 473 U.S. at 214. Insofar as Congress decided that the NSPA should apply to the theft of goods, wares, or merchandise, *i.e.*, tangible property, a proper respect for Congress's choice may allow a defendant who steals intellectual property only in intangible form, as in Aleynikov, to avoid prosecution under the NSPA. But a defendant, such as Agrawal, who steals intellectual property in tangible form, will not be heard to complain of legal insufficiency when he is prosecuted for conduct that falls within congressionally defined parameters.

In sum, we conclude that Agrawal's legal insufficiency challenge to his NSPA charge fails for lack of any error, much less plain error.

B. Sufficiency of the Evidence Proving NSPA Crime

Agrawal submits that, even in the absence of legal insufficiency, his NSPA conviction must be reversed because the trial evidence was insufficient to support a guilty verdict. He carries a heavy burden in making this argument. Not only must we view the evidence in the light most favorable to the prosecution, drawing all inferences in its favor, *see United States v. Broxmeyer*, 616 F.3d 120, 125 (2d Cir. 2010), but also we must affirm the conviction if “any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt,” Jackson v. Virginia, 443 U.S. 307, 319 (1979) (emphasis in original).

Agrawal specifically argues that the evidence was insufficient to demonstrate that

there was a market for the stolen HFT code. Such a requirement is not expressly stated in the NSPA. Nevertheless, in construing the NSPA's "goods, wares, [or] merchandise" language, we have stated that these terms denote "such personal property or chattels as are ordinarily a subject of commerce." United States v. Vericker, 446 F.2d 244, 248 (2d Cir. 1971) (Friendly, C.J.). We there recognized that "mere papers" containing maps or chemical formulae could constitute goods or wares because they were "ordinarily subject[s] of sale or license." Id. (collecting cases). But we held that stolen FBI documents did not qualify because there was no evidence that such papers were "ordinarily bought and sold in commerce." Id.

In considering whether a market exists for an item, the question is not whether the market is legitimate. A black market will do. See United States v. Weinstein, 834 F.2d 1454, 1463 (9th Cir. 1987) (recognizing property to be subject of commerce if it can be sold "even on a thieves market"); see also United States v. Stegora, 849 F.2d 291, 292 (8th Cir. 1988) (applying "thieves' market" price as proper measure of good's value); United States v. Moore, 571 F.2d 154, 155 (3d Cir. 1978) (same). Nor is it necessary to show that SocGen itself planned to sell or license its code in the market. Plainly, it did not. Nevertheless, considerable evidence allowed a jury to find that a market did exist for the buying or licensing of trading systems such as SocGen's and the code on which they were based.

For example, SocGen programmer Thuillier testified to an occasion when a financial institution purchased a hedge fund in order to acquire its high frequency trading system,

thereby allowing the institution to engage in index arbitrage. See Tr. 651. The purchaser of a trading system necessarily also purchases the code on which the system is based. Indeed, without the code, there is no system.

Trial evidence permitted the jury to infer that Tower was looking to purchase SocGen's otherwise unavailable HFT code when it proposed to hire Agrawal to duplicate SocGen's trading systems. Indeed, Agrawal convinced Tower to hire him by representing that he had access to SocGen's code and could clone its trading systems. Toward this end, he gave Tower notes derived from SocGen's HFT code and stated that he had "a lot of things in actual[] print." Tr. 124. From this evidence, a jury could reasonably conclude that Agrawal was effectively offering to "sell" and Tower agreeing to "buy" the HFT code, with that transaction to be effected by Tower's hiring Agrawal. Such a "hire me, get the code" inference is reinforced by the fact that the compensation package Tower offered to Agrawal would have paid him a percentage of profits realized from the trading systems he would clone from SocGen's code.

This record, viewed in the light most favorable to the government, was sufficient to permit a reasonable jury to find that there was a market for computer code such as that stolen by Agrawal. We therefore reject his evidentiary sufficiency challenge to his NSPA conviction as without merit.

C. Jury Instructions

Agrawal submits that numerous errors in the district court's jury instructions require

vacatur of his conviction. As to the EEA count, he argues that (1) the district court's instruction on "intent" was incorrect as a matter of law, and (2) a "knowledge" instruction was wrongfully omitted from the charge. As to the NSPA count, Agrawal complains that the district court (1) failed to submit to the jury the question of whether goods, wares, or merchandise were stolen; (2) failed to instruct the jury on how to determine whether the \$5,000 value element was satisfied; and (3) improperly charged on the requisite interstate commerce nexus.

Had Agrawal raised these objections in the district court, warranting de novo review on appeal, he would carry a heavy burden in urging vacatur. Not only would he have to demonstrate that he requested a charge from the district court that accurately represented the law in every respect, but also he would have to show that the charge given was erroneous and caused him prejudice, a matter decided by looking not only to the challenged instruction, but to the charge as a whole. See, e.g., United States v. Applins, 637 F.3d 59, 72 (2d Cir. 2011). Because Agrawal did not raise any of the charging errors about which he now complains in the district court, as required by Fed. R. Crim. P. 30(d) (requiring party who objects to jury charge to inform district court of "specific objection and the grounds for the objection"), see United States v. Masotto, 73 F.3d 1233, 1237 (2d Cir. 1996), his burden on appeal is heavier still because we will review only for plain error, which is not evident here, see Fed. R. Crim.

P. 30(d), 52(b); United States v. Cain, 671 F.3d 271, 287 (2d Cir. 2012) (reviewing unpreserved challenge to jury instruction for plain error).

1. EEA Count

a. Intent Instruction

Agrawal contends that the district court erred as a matter of law by effectively instructing the jury that, “if Agrawal formed an intent to convert [SocGen’s HFT] code after he had copied and/or removed it, that intent could somehow relate back to the initial act and render it criminal.” Appellant Br. 25. He further maintains that this objection was preserved in the district court, so as to warrant de novo, rather than plain-error, review. Both arguments are defeated by the record.

As to the second argument, the record shows that Agrawal never objected to the district court’s charge as a misstatement of law, i.e., he never submitted that the language of § 1832 admitted guilt only upon proof of a defendant’s intent to convert at the time he copied or removed a trade secret. Rather, he maintained that such a narrow instruction was compelled by the fact that the “to wit” clause of the indictment limited the government to this theory of culpability. See Tr. 1009, 1098. That argument may have raised a constructive amendment challenge to the charge, a point we discuss infra at Part II.D (rejecting constructive amendment argument), but it did not alert the district court to any claim that its instruction misconstrued the EEA. We thus review only for plain error. See Fed. R. Crim. P. 30(d).

Contrary to Agrawal’s contention, the district court did not charge the jury that a subsequently formed intent could relate back to otherwise innocent conduct and render it

criminal. What Judge Rakoff charged was that, in addition to other identified elements of an EEA crime, the government had to prove, beyond a reasonable doubt,

that when [Agrawal] removed the code [from SocGen's offices], or at any point thereafter when he was still in unauthorized possession of the computer code, the defendant formed the intent to convert the code to the economic benefit of himself or others, knowing or intending that this would injure Société Générale.

Tr. 1313–14.

This instruction comports with the language of the EEA, which makes it a crime for a defendant to engage in a range of listed conduct “with intent to convert a trade secret . . . 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.” 18 U.S.C. § 1832. Consistent with this statutory scheme, Judge Rakoff's instruction referenced two proscribed actions—the unauthorized removal of a trade secret from its owner's offices and the unauthorized possession of that trade secret—either of which could support an EEA conviction, provided that when the defendant engaged in that removal or possession, he had formed the requisite intent to convert. See id. § 1832(a)(1), (a)(3).

As the record evidence demonstrated, Agrawal's unauthorized removal of computer code printouts and his unauthorized possession of those printouts began on the same date. But while the prohibited removal was concluded on discrete days, Agrawal's unauthorized possession continued uninterrupted for some ten months, even after he resigned from SocGen. In these circumstances, the district court correctly recognized that, as a matter of law, the government could carry its burden on the element of intent if it proved the requisite

mens rea “when [Agrawal] removed the code, or at any point thereafter when he was still in unauthorized possession of the computer code.” Tr. 1314.

Whatever constructive amendment complaints Agrawal may have about the charge’s reference to “possession” not alleged in the indictment’s “to wit” clause, see infra at Part II.D, there is no merit to his argument that it misstates the law. In sum, because we identify no legal error in this charge, we necessarily identify no plain error.

b. Failure To Submit Knowledge to Jury

Agrawal faults the district court for not charging the jury that the government was required to prove beyond a reasonable doubt that when he took any actions proscribed by the EEA, he did so with knowledge that those actions were not authorized by SocGen. This forfeited argument fails at the final step of plain-error analysis in light of overwhelming evidence that Agrawal possessed the requisite knowledge not only when he removed the code from SocGen’s office and brought it to his home, but thereafter when he transmitted parts of it to Tower. An FBI agent testified to Agrawal’s post-arrest admissions that he printed SocGen’s HFT computer code onto papers and then transported those papers in a knapsack to New Jersey, knowing that he was not specifically authorized to do so. While on the one hand, Agrawal told the agent that he thought SocGen would have approved his actions in order to further his work, on the other hand, he stated that he did not tell his supervisors what he had done because “he was afraid to do so.” Tr. 803.¹⁴ More damning still, Agrawal

¹⁴ Insofar as Agrawal submitted that his expectation of employer approval was reasonable given co-workers’ admissions that they had taken code printouts home, the circumstances were so distinguishable that, when viewed in the light most favorable to the

testified at trial that he knew that the code in his possession was proprietary to SocGen and that he, nevertheless, shared some of that proprietary information with Tower personnel, knowing that it was wrong to do so.

Agrawal disputes the relevancy of this last testimony, maintaining that knowledge, like intent, had to be proved with respect to the particular conduct alleged in the “to wit” clause, *i.e.*, his copying and removal of SocGen’s code. We reject this argument for the reasons stated in our discussion of defendant’s constructive-amendment challenge. *See infra* Part II.D. In any event, in light of Agrawal’s admissions that he knew various of his actions with respect to SocGen’s code were unauthorized, as well as the other overwhelming evidence of his guilt, we conclude that a failure to correct possible error in an omitted knowledge charge would not here seriously affect the fairness, integrity, or public reputation of judicial proceedings. *See United States v. Cotton*, 535 U.S. at 632–33; *Johnson v. United States*, 520 U.S. at 462.

2. NSPA Count

a. Failure To Submit Question of “Goods, Wares [or] Merchandise” to Jury

Although Agrawal never requested that the district court submit to the jury the question of whether the government had proved the NSPA’s “goods, wares, [or] merchandise” requirement, he now argues that it was legal error not to do so. Even if we assume, without deciding, that the omission satisfies the first two prongs of plain-error

prosecution, we would have to assume that a reasonable jury rejected Agrawal’s contention. *See United States v. Broxmeyer*, 616 F.3d at 125.

review, the argument fails the final two criteria. For reasons discussed supra at Part II.B, the paper copies of the code stolen by Agrawal so plainly constitute “goods” as to allow us confidently to conclude that there is no reasonable probability that the failure to submit the question to the jury affected the outcome of Agrawal’s trial. See United States v. Marcus, 130 S. Ct. at 2164; cf. Neder v. United States, 527 U.S. 1, 16–17 (1999) (holding failure to charge or submit required element harmless error where proved by overwhelming evidence). For the same reason, the omission could not have seriously affected the fairness, integrity, or public reputation of the judicial proceedings. See United States v. Cotton, 535 U.S. at 632–33.

b. Failure To Differentiate Jurisdictional Elements of NSPA and EEA

In charging the jury as to the jurisdictional element of the NSPA, the district court instructed that the government was obliged to prove beyond a reasonable doubt “that the defendant, knowing the computer code was stolen, purposely transported it in interstate commerce.” Tr. 1315. Although Agrawal concedes that this is a correct statement of law, he submits that it was error for the district court not to emphasize the difference between this jurisdictional element and its EEA counterpart. Agrawal never sought any such further instruction in the district court.¹⁵

¹⁵ Insofar as Agrawal directs us to Eighth Circuit precedent emphasizing that, to convict under the NSPA, a jury must find that the property at issue was stolen or converted before it was transported in interstate commerce, see Loman v. United States, 243 F.2d 327, 329 (8th Cir. 1957); see also United States v. De La Barra, 447 F.2d 193, 195 (5th Cir. 1971), the charge in this case does not suggest otherwise, see Tr. 1315.

Agrawal's contention that a jury could conflate this instruction with the one given on the EEA's jurisdictional element is entirely speculative and at odds with the law's general assumption that juries follow the instructions they are given. See Weeks v. Angelone, 528 U.S. 225, 234 (2000) ("A jury is presumed to follow its instructions."); accord Britt v. Garcia, 457 F.3d 264, 272 (2d Cir. 2006). Indeed, such speculation appears particularly unwarranted here, where the district court charged the EEA and NSPA counts separately, reviewing all elements of the one crime before explaining any elements of the other. Moreover, unlike this court, which has used a common term, i.e., "jurisdictional element," to refer to the two statutes' required, but different, interstate commerce nexuses, the district court avoided any language suggesting that an element from one count might be related to an element from the other count. Thus, in charging the jury as to the EEA, Judge Rakoff made clear that the required jury finding pertained to the computer code. Did the government prove beyond a reasonable doubt "that the computer code was related to, or included in, a product that was, at least in part, produced for, or placed in, interstate or foreign commerce"? Tr. 1314. In connection with this burden, Judge Rakoff explained that "it is sufficient if the government proves that the purpose of the computer code was to effectuate securities trades, at least some of which were in interstate or foreign commerce." Id. at 1315. By contrast, in instructing the jury on the jurisdictional element of the NSPA, Judge Rakoff focused the jury's attention on the defendant's actions and state of mind. Did the government prove beyond a reasonable doubt "that the defendant, knowing the computer code was stolen, purposely transported it in interstate commerce?" Id.

These instructions were sufficiently clear and distinct that they present no reason to assume juror confusion or to warrant a departure from the general assumption that juries follow the instructions they are given. Accordingly, we identify no error, much less plain error, in this part of the district court's NSPA charge.¹⁶

c. Failure To Instruct on How To Assess Value

The district court instructed that to find Agrawal guilty of the NSPA charge, the jury had to find beyond a reasonable doubt that “the value of the [stolen] property was \$5,000 or more.” Tr. 1316. Agrawal submits that this was inadequate because it did not instruct the jury on how to determine the value of the stolen computer code. Agrawal not only failed to request such a charge in the district court, but also specifically declined the district court's invitation to comment on this part of the charge. After the prosecution secured a modification of the instruction to refer to the value of the “property” rather than the value of the “trade secret,” *id.* 896 (observing that NSPA conviction required government to prove only that stolen property had value of \$5,000 or more, regardless of whether property was trade secret), the district court asked if there was “[a]nything from the defense on this [instruction],” to which Agrawal's counsel replied, “No, your honor.” *Id.* This response was consistent with the defense's strategic decision to challenge nothing about the case except the government's ability to prove Agrawal's culpability at the precise time he copied and removed the computer code printouts. Such a strategic decision, evidenced not merely by

¹⁶ To the extent Agrawal relies on this alleged charging omission to support a claim of constructive amendment of the NSPA charge, we need not address that argument separately in light of our conclusion that there was no charging error.

silence but by a negative response on the record to a district court invitation to voice objection, does more than forfeit the unraised objection; it waives it. See United States v. Olano, 507 U.S. at 733 (distinguishing waiver from forfeiture); United States v. Quinones, 511 F.3d 289, 321 (2d Cir. 2007) (stating that true waiver can negate even plain-error review).

Even were this argument merely forfeited, however, Agrawal could not demonstrate plain error. The trial evidence showed that Tower was willing to pay Agrawal several hundred thousand dollars based on his professed ability to duplicate SocGen's confidential HFT system. That system earned SocGen tens of millions of dollars of profits a year. Agrawal's ability to clone SocGen's system derived from his possession of a printed copy of the computer code that made up the system. On this record, a reasonable jury could certainly have found the computer code to have a value of at least \$5,000, and we cannot conclude that allowing the jury to make such a finding in the absence of a valuation instruction never sought by the defense affected Agrawal's substantial rights, see United States v. Marcus, 130 S. Ct. at 2164, or seriously affected the fairness, integrity, or public reputation of the judicial proceeding, see United States v. Cotton, 535 U.S. at 632–33.

In sum, we identify no charging error warranting vacatur with respect to either count of conviction.

D. Constructive Amendment of EEA Count

Agrawal argues that the EEA charge was constructively amended in violation of the

Fifth Amendment's Grand Jury Clause, insofar as his conviction rests on facts outside the "to wit" clause of the EEA count, which alleges only his unauthorized copying, printing, and removal of SocGen's confidential computer code. We review a constructive amendment challenge de novo. See United States v. Banki, 685 F.3d 99, 118 (2d Cir. 2012). To prevail on such a claim, "a defendant must demonstrate that either the proof at trial or the trial court's jury instructions so altered an essential element of the charge that, upon review, it is uncertain whether the defendant was convicted of conduct that was the subject of the grand jury's indictment." United States v. Frank, 156 F.3d 332, 337 (2d Cir. 1998); accord United States v. Rigas, 490 F.3d 208, 226 (2d Cir. 2007); United States v. Salmonese, 352 F.3d 608, 620 (2d Cir. 2003). Although constructive amendment is viewed as a per se violation of the Grand Jury Clause, sufficient to secure relief without any showing of prejudice, this court has proceeded cautiously in identifying such error, "consistently permitt[ing] significant flexibility in proof, provided that the defendant was given notice of the core of criminality to be proven at trial." United States v. D'Amelio, 683 F.3d 412, 417 (2d Cir. 2012) (emphasis in original; internal quotation marks omitted).

By contrast to constructive amendment, "variance," of which Agrawal also complains, occurs when the charging terms of an indictment are unaltered, but the trial evidence proves facts materially different from those alleged in the indictment. See United States v. D'Amelio, 683 F.3d at 417; United States v. Salmonese, 352 F.3d at 621. A variance raises constitutional concerns only if it deprives a defendant of the notice and double jeopardy protections of an indictment, see United States v. D'Amelio, 683 F.3d at 417, which

prejudice the defendant must establish to secure relief on appeal, see United States v. Salmonese, 352 F.3d at 621–22.

In D’Amelio, our most recent discussion of these concepts, the crime charged was attempted enticement of a minor for purposes of sexual activity in violation of 18 U.S.C. § 2422(b). An essential element of that crime was the use of a “facility or means of interstate commerce,” id. § 2422(b), which was specifically identified in the indictment’s “to wit” clause as the Internet, see United States v. D’Amelio, 683 F.3d at 414. The defendant argued that where the indictment thus cabined an element of the crime, it was a constructive amendment, or at least a prejudicial variance, for the prosecution to argue, and for the district court to instruct, that the jurisdictional element could be satisfied by evidence of other, uncharged means—specifically, the use of a telephone. See id. at 413–414.

Rejecting this argument, D’Amelio explained that the “core of criminality” is “the essence of a crime, in general terms; the particulars of how a defendant effected the crime falls outside that purview.” Id. While constructive amendment is evident if a jury convicts “based on a complex of facts distinctly different from that which the grand jury set forth in the indictment,” no such concern arises where the indictment charges “a single set of discrete facts from which the government’s proof was at most a non-prejudicial variance.” Id. at 419 (internal quotation marks omitted). In concluding that D’Amelio fell into the second category, this court observed that the core of criminality for the charged crime was the attempted enticement over a period of time of a particular person (believed to be a minor) into sexual activity. All of the communications relied on by the government to demonstrate

that enticement, whether e-mails or telephone calls, took place in furtherance of the same core criminality. See id. Further, the defendant in D’Amelio did not—and apparently could not—argue that he was surprised by the government’s reliance on telephone communications, having been given notice of such evidence 18 months before trial. See id. at 414, 420.

In this case, the core of criminality proscribed by the EEA is the theft of trade secrets. To be sure, only the title of the statutory section uses the common law term “theft.” Nevertheless, in numbered subsections, the statutory text so exhaustively details the means by which theft can be committed that one can only conclude that Congress intended the means provisions of the EEA to reach as broadly as human ingenuity could conceive to accomplish theft—subject of course to the EEA’s jurisdictional and mens rea requirements. See generally Florida Dep’t of Revenue v. Piccadilly Cafeterias, Inc., 554 U.S. 33 (2008) (“[S]tatutory titles and section headings are tools available for the resolution of a doubt about the meaning of a statute.” (internal quotation marks omitted)); cf. Collazos v. United States, 368 F.3d 190, 196 (2d Cir. 2004) (cautioning that common-law meaning of word found only in statutory title cannot limit plain meaning of unambiguous text).

More to the point, the indictment here signals that the grand jury availed itself of the breadth of the EEA’s means provisions, intending that Agrawal be prosecuted for every means he employed in the theft of SocGen’s trade secrets, a crime alleged to have begun on a single day but to have been maintained over a ten-month period from June 12, 2009, to April 2010. Thus, the indictment referenced no fewer than 17 statutory means in charging

Agrawal with the theft of SocGen’s confidential HFT code. See Indictment ¶ 19 (charging that Agrawal “copied, duplicated, sketched, drew, photographed, downloaded, uploaded, altered, destroyed, photocopied, replicated, transmitted, delivered, sent, mailed, communicated, and conveyed a trade secret,” see 18 U.S.C. § 1832(a)(2)). In the “to wit” clause that followed, the indictment repeated one of these 17 means and added two more. See Indictment ¶ 19 (charging that Agrawal “copied, printed and removed” proprietary computer code from SocGen’s offices; see 18 U.S.C. § 1832(a)(1)–(2)).¹⁷ Moreover, in the indictment’s 18 preceding paragraphs, the grand jury detailed how these means, as well as another—Agrawal’s continued possession of the trade secrets in his home even after he had resigned from SocGen, see 18 U.S.C. § 1832(a)(3)—were all part of the thievery that was the core of criminality charged. See Indictment ¶¶ 1–19.

When the indictment is thus considered as a whole, the “to wit” clause is properly understood to be illustrative rather than definitional of the core of criminality charged by the grand jury. Indeed, that conclusion is stronger here than in D’Amelio. There, the court ruled that no constructive amendment was effected by the use of an unpleaded means, *i.e.*, a telephone, to prove the jurisdictional element of a crime whose core of criminality remained unchanged. The conclusion applies with more force here, where as part of a detailed and unaltered scheme, the indictment served notice of every means of theft referenced by the prosecution in urging conviction.

¹⁷ Although the statutory references at the end of the EEA count of the indictment cite only to paragraph (2) of § 1832, the “removal” charged in the “to wit” clause is proscribed by paragraph (1) (“steals, or without authorization appropriates, takes, [or] carries away”).

Indeed, in complaining that Judge Rakoff’s intent instruction constructively amended the EEA count of the indictment by referencing continued unauthorized possession, Agrawal never asserted that the indictment failed to afford him notice that he was alleged to have retained unauthorized possession of SocGen’s computer code even after he removed it from his employer’s office. Rather, he argued that the government should not be allowed to rely on any proscribed means of theft referenced in the indictment other than those expressly stated in the “to wit” clause. The Grand Jury Clause defeats, rather than supports, such an effort to construe a crime by reference to only part of the indictment returned by the grand jury.

Because Agrawal fails to show either constructive amendment of the indictment or a prejudicial variance in proof, this challenge to his EEA conviction fails on the merits.

III. Conclusion

To summarize, we conclude as follows:

1. On plain-error review of Agrawal’s defaulted legal insufficiency challenge to his EEA conviction, defendant fails to show that purported error in the pleading of the law’s jurisdictional element affected his substantial rights or the fairness, integrity, or public reputation of judicial proceedings, because:

- (a) although the trade secret at issue in this case, computer code, was included in a confidential trading system that could not itself be the product “produced for or placed in” interstate commerce necessary to satisfy the jurisdictional element of the EEA, see United States v. Aleynikov, 676 F.3d at 81–82, this product requirement as well as the

statute's "related to" requirement were nonetheless satisfied by the securities which the code was designed and used to trade on national markets;

(b) neither the indictment nor the prosecution's arguments or the court's charge ever identified the trading system as the only product relied on to establish jurisdiction; rather, the indictment, arguments, and charge all signaled that securities were the product placed in interstate commerce; and

(c) even if there could have been any confusion on this point, for the jury to have found the trading system to be a product in interstate commerce, it necessarily had to find that the securities traded using that system were products in interstate commerce.

2. On plain-error review of Agrawal's defaulted legal insufficiency challenge to his NSPA conviction, defendant fails to show that the theft of SocGen's computer code did not satisfy the law's "goods, wares, [or] merchandise" requirement because, although the code itself was intangible intellectual property, Agrawal stole it in the tangible form of thousands of sheets of paper.

3. On plain-error review of Agrawal's defaulted jury charge challenge, defendant fails to carry his burden at one or more of the four steps of analysis on his claims of (a) legal error in the instruction on the requisite EEA intent, (b) the omission of an instruction on the requisite EEA knowledge, (c) the failure to have the jury find whether the stolen code was a good, ware, or merchandise for purposes of the NSPA, (d) the failure to emphasize

differences in the jurisdictional elements of the NSPA and EEA, and (e) omission of an instruction as to how to assess the requisite NSPA value.

4. Agrawal's preserved claims of constructive amendment and prejudicial variance fail on the merits.

Accordingly, the judgment of conviction entered by the district court is hereby AFFIRMED.