Acosta, J.P., Richter, Mazzarelli, Kapnick, Gesmer, JJ.

1956 The People of the State of New York Ind. 4447/12
Appellant,

-against-

Sergey Aleynikov,
Defendant-Respondent.

_____

Cyrus R. Vance, Jr., District Attorney, New York, NY (Elizabeth Roper of counsel), for appellant.

Marino, Tortorella & Boyle, P.C., New York (John D. Tortorella and Kevin H. Marino of the bar of the State of New Jersey, admitted pro hac vice, of counsel), for respondent.

_____

Order, Supreme Court, New York County (Daniel P. Conviser, J.), entered on or about July 6, 2015, as amended July 7, 2015, reversed, on the law, the motion denied, the verdict reinstated, and the matter remanded for sentencing.

Opinion by Richter, J. All concur.

Order filed.

SUPREME COURT, APPELLATE DIVISION, FIRST DEPARTMENT,

Rolando T. Acosta, J.P.
Dianne T. Richter
Angela M. Mazzarelli
Barbara R. Kapnick
Ellen Gesmer, JJ.

1956
Ind. 4447/12

_____x

The People of the State of New York,
Appellant,

-against-

Sergey Aleynikov,
Defendant-Respondent.

_____x

The People appeal from the order of the Supreme Court, New York County (Daniel P. Conviser, J.), entered on or about July 6, 2015, as amended July 7, 2015, which, to the extent appealed from as limited by the briefs, granted defendant's motion for a trial order of dismissal to the extent of setting aside the jury's verdict convicting him of unlawful use of secret scientific material.

Cyrus R. Vance, Jr., District Attorney, New York, NY (Elizabeth Roper, Daniel Holmes and Jeremy Glickman of counsel), for appellant.

Marino, Tortorella & Boyle, P.C., New York (John D. Tortorella, Kevin H. Marino of the bar of the State of New Jersey, admitted pro hac vice, John Boyle and Erez Davy of counsel), for respondent.

RICHTER, J.

Defendant was formerly employed by Goldman Sachs as a computer programmer. Prior to leaving Goldman to work for a potential competitor, defendant made a digital copy of Goldman's proprietary computer source code by uploading and saving it to a hard drive of a server located outside the Goldman network. After surreptitiously uploading the source code, defendant transferred copies of it to several of his personal computing devices, and subsequently shared it with his new employer. As a result, defendant was charged with unlawful use of secret scientific material (Penal Law § 165.07). After a jury convicted defendant of this crime, the trial court set aside the verdict.

In this appeal, we are asked to decide whether defendant's actions constitute legally sufficient evidence to establish that he made a "tangible reproduction or representation" of the source code, and did so with the "intent to appropriate . . . [its] use," within the meaning of the unlawful use statute. We conclude that, viewed in the light most favorable to the People, the evidence was legally sufficient as to both of these elements. Accordingly, we reverse the trial court's decision, reinstate the jury's verdict and remand the matter for sentencing.

The evidence at trial, which is largely undisputed, established the following. In May 2007, Goldman hired defendant

as a computer programmer to write and maintain software for the company's high-frequency trading system. High-frequency trading entails the use of computers to make very rapid decisions concerning pricing of securities, and to quickly generate trades and orders. It is a competitive business that depends in large part on the speed with which information can be processed to seize fleeting market opportunities. High-frequency trading can be very lucrative, earning Goldman about $300 million in profits in 2009.

The infrastructure that supported Goldman's high-frequency trading business was based on a system the firm had purchased in 1999. Since that purchase, Goldman has regularly updated the system by incorporating new pieces of software into it. As a programmer at Goldman, defendant had access to the source code that ran the high-frequency trading system. Source code is a set of computer instructions written in a human-readable programming language. Defendant's programming duties included copying source code from Goldman's source code repository, modifying and testing it, and then integrating it into the existing software.

Because the high-frequency source code was so valuable, Goldman took a variety of steps to safeguard its secrecy. These measures included physical security of the corporate building, a limit on the number of people who had access to the software, and

the creation of an information security group responsible for ensuring that Goldman's systems were not vulnerable to attack. Further, every Goldman employee signed confidentiality and nondisclosure agreements wherein they acknowledged that they could not use Goldman's confidential information for their own purposes. Goldman programmers were forbidden from copying Goldman's source code outside of Goldman's network. Although employees were allowed to work from home, they had to use remote access or a firm laptop to ensure that all the source code stayed within the Goldman network.

In the spring of 2009, defendant was hired by Teza Technologies, a startup high-frequency trading firm. At that time, Teza had no software, connectivity or equipment for high-frequency trading activities, but hoped to build a system from scratch and be operational by the end of 2009. Teza hired defendant as a systems architect for its new trading platform. His annual salary was $1.2 million, about three times his salary at Goldman. At the end of May 2009, Teza's principal sent defendant an email emphasizing that the company had less than six months to launch the new system, and that the group developing the system had to "move fast."

Defendant ended his employment with Goldman on June 5, 2009. Later that month, Goldman's information security department

noticed unusual activity while reviewing a report generated by Goldman's computer monitoring systems. Specifically, the monitoring report showed that on June 1, 2009 and June 5, 2009, large amounts of data had been uploaded from the Goldman network to a Germany-based "subversion website," which is a website designed to allow a user to move, copy and store source code. Although Goldman's security system normally would block access to such websites, it somehow missed this one.

The monitoring report indicated that the transfers were made from defendant's work computer. Examination of defendant's computer showed that on his last day of work, he executed a program he had written to copy thousands of proprietary files from Goldman's source code repository. The files transferred that day included components of Goldman's high-frequency trading platform that would be highly valuable to any competitor. The files were compressed into smaller files called "tarballs," encrypted, and then uploaded onto the German subversion website.

Goldman's investigation revealed that the program defendant used to transfer the files had been backdated to make it seem two years older than it really was. The investigation also revealed that after running the program, defendant deleted it from his work computer, along with his "bash history," which is a list of the most recent commands a user has typed into his computer.

According to testimony at trial, deleting a bash history is not common, and there is no reason why a user would do so.[1] Police in Germany located the server of the subversion website, removed the hard drives and made forensic copies of them. A search of the information on those drives revealed that an individual with the username "saleyn" had uploaded information onto the server and then later retrieved it. Defendant had used this same username — which consists of his first initial and the first five letters of his last name — as his personal email address. The investigation further showed that by the end of June 2009, defendant had placed some source code into a "repository" account that Teza had created on a third-party website. A review of that code revealed that it was based upon the Goldman high-frequency trading programs that defendant had copied to the German server.

On July 3, 2009, defendant was arrested by the Federal Bureau of Investigation (FBI); Teza immediately terminated his employment. A search of two personal computers and a digital storage device found in defendant's home revealed that all three contained data from Goldman. When questioned by the FBI,

[1] Because Goldman's systems periodically created a copy of each user's bash history, investigators were able to uncover defendant's conduct that day, as well as his attempts to cover it up.

defendant at first denied transferring any proprietary information from Goldman. Upon further inquiry, however, defendant made a series of incriminating statements. In particular, defendant admitted that (i) he uploaded material from Goldman to the German server; (ii) he specifically chose that server because it was not blocked by Goldman's security system; (iii) he subsequently downloaded the material from the German server to his home computer and other storage devices; and (iv) he purposely erased the encryption software, the tarballs and his bash history because he knew his actions had violated Goldman's security policies.

In February 2010, defendant was charged in a federal indictment with transferring the Goldman source code in violation of, inter alia, the National Stolen Property Act (18 USC § 2314). On December 10, 2010, defendant was convicted following a jury trial in the District Court for the Southern District of New York. Defendant subsequently appealed his conviction to the Court of Appeals for the Second Circuit. On April 11, 2012, the Second Circuit reversed the conviction, concluding that defendant's actions did not violate the federal statute (*see United States v Aleynikov*, 676 F3d 71 [2d Cir 2012]).

In September 2012, defendant was charged in a New York County indictment with two counts of unlawful use of secret

scientific material (Penal Law § 165.07) (one count based on defendant's transfer of data on June 1, 2009, and the other based on his June 5, 2009 transfer), and one count of unlawful duplication of computer related material in the first degree (Penal Law § 156.30[1]). These state charges were based on the same conduct that led to his federal prosecution.[2] On April 8, 2015, defendant proceeded to a trial before a jury. At the close of the People's case, defendant moved, pursuant to CPL 290.10, for a trial order of dismissal as to all counts of the indictment; the court reserved decision on the motion.[3]

The jury returned a verdict of guilty on the count of the indictment charging unlawful use of secret scientific material arising from the June 5, 2009 transfer. The jury could not reach a unanimous verdict on the unlawful use count based on the June 1, 2009 transfer, and acquitted defendant of unlawful duplication of computer related material in the first degree.[4] In a decision entered on or about July 6, 2015, as amended July 7, 2015, the trial court granted defendant's motion for a trial order of

---

[2] In a pretrial decision, the trial court concluded that the state prosecution was not barred by double jeopardy.

[3] Defendant periodically renewed his motion during jury deliberations.

[4] Those two counts are not at issue in this appeal.

dismissal as to the two counts of unlawful use. The court concluded that the evidence was insufficient to show that: (i) defendant made a "tangible reproduction or representation" of the source code; and (ii) he acted with the "intent to appropriate . . . the use of" the source code. The People appeal from the court's order to the extent it dismissed the unlawful use count related to the June 5, 2009 transfer. We now reverse.

Under CPL 290.10(1)(a), a court may grant a motion for a trial order of dismissal when the "trial evidence is not legally sufficient to establish the offense charged." "Legally sufficient evidence" is defined as "competent evidence which, if accepted as true, would establish every element of an offense charged and the defendant's commission thereof" (CPL 70.10[1]). In reviewing the legal sufficiency of the evidence, "all questions as to the quality or weight of the evidence must be deferred, the inquiry being whether the competent evidence, if accepted as true, establishes every element of the offense charged" (*People v Carrion*, 165 AD2d 671, 672 [1st Dept 1990]). In deciding the motion, the court must view all of the evidence in the light most favorable to the People (*People v Simon*, 157 AD2d 508, 512 [1st Dept 1990]).

Applying these principles, we conclude that the evidence at trial was legally sufficient to establish defendant's guilt of

unlawful use of secret scientific material. That statute, which became part of the Penal Law in 1967, provides:

> "A person is guilty of unlawful use of secret scientific material when, *with intent to appropriate to himself or another the use of secret scientific material*, and having no right to do so and no reasonable ground to believe that he has such right, he makes a *tangible reproduction or representation of such secret scientific material* by means of writing, photographing, drawing, mechanically or *electronically reproducing or recording* such secret scientific material"

(Penal Law § 165.07 [emphasis added]). In his motion for a trial order of dismissal, defendant did not challenge the People's proof that he electronically reproduced the source code. Nor did he claim that the source code did not constitute "secret scientific material," as that term is defined in Penal Law § 155.00(6). Rather, as relevant here, he argued that he did not make a tangible reproduction of the source code and that he lacked the requisite intent.

Although there is a dearth of case law interpreting this provision, the legislative history reveals why it was added to the Penal Law. The Temporary Commission on Revision of the Penal Law and Criminal Code explained that prior to the statute's enactment, "a person who [stole] the blueprints of a secret process, commit[ted] larceny[, but] one who surreptitiously [made] a photographic copy of such blueprint, leaving the

original in its proper place, [did] not commit larceny because he [was] not stealing 'property'" (1967 NY Legis Ann at 21; *see* William C. Donnino, Practice Commentary, McKinney's Cons Laws of NY, Book 39, Penal Law § 165.07 at 200 ["In the absence of the unlawful use crime, the photographing [of a document containing a secret scientific formula] would not be a crime since it does not represent a traditional taking of the 'property'"]).

With this context in place, we turn to the arguments advanced by the People on this appeal. First, the People contend that, contrary to the trial court's conclusion, the evidence was sufficient to establish that defendant made a "tangible reproduction or representation" of the source code. The Penal Law does not define "tangible." In construing the meaning of this term, we are guided by well-settled principles of statutory construction. "[C]ourts are obliged to interpret a statute to effectuate the intent of the Legislature" (*People v Williams*, 19 NY3d 100, 103 [2012]). "'As the clearest indicator of legislative intent is the statutory text, the starting point in any case of interpretation must always be the language itself, giving effect to the plain meaning thereof'" (*People v Golo*, 26 NY3d 358, 361 [2015], quoting *Majewski v Broadalbin-Perth Cent. School Dist.*, 91 NY2d 577, 583 [1998]).

We must "presum[e] that lawmakers have used words as they

are commonly or ordinarily employed, unless there is something in the context or purpose of the [statute] which shows a contrary intention" (*People v Finley*, 10 NY3d 647, 654 [2008] [internal quotation marks omitted]). Further, Penal Law provisions "must be construed according to the fair import of their terms to promote justice and effect the objects of the law" (Penal Law § 5.00), and courts should "dispense with hypertechnical or strained interpretations" of penal provisions (*People v Versaggi*, 83 NY2d 123, 131 [1994] [internal quotation marks omitted]).

Where, as here, a word is not defined by statute, dictionary definitions serve as "useful guideposts" in determining the word's meaning (*People v Ocasio*, __NY3d__, 2016 NY Slip Op 07105 [2016] [internal quotation marks omitted]). Black's Law Dictionary defines "tangible" as "[h]aving or possessing physical form; CORPOREAL[;] [c]apable of being touched and seen; perceptible to the touch; capable of being possessed or realized" (Black's Law Dictionary [9th ed 2009]).[5] The People and defendant are in essential agreement that the term "tangible" means something having "physical form and characteristics" (*see e.g. People v Barden*, 117 AD3d 216, 231 n 5 [1st Dept 2014]

[5] Although Black's Law Dictionary also defines "tangible" as "[c]apable of being understood by the mind," the People, on appeal, do not argue that this definition should be used to determine the legal sufficiency of the trial evidence.

[defining "tangible property"], *reversed on other grounds* 27 NY3d 550 [2016]). The heart of their dispute is whether defendant made a "tangible reproduction or representation" of Goldman's source code when he copied and saved the code onto the hard drive of the German server. We conclude that he did.

The testimony of the People's witnesses at trial established that defendant created a copy of the source code that physically resided on the server's hard drive, a physical medium. Mirko Manske, a German law enforcement officer, described how police removed "physical" hard drives from the German server. Other witnesses testified that computer data can be physically present on various storage media, including hard drives. FBI Agent Michael McSwain explained that source code that is stored on a computer's hard drive "takes up physical space" on the hard drive. Navin Kumar, a computer engineer at Goldman, testified that when computer files are stored on a hard drive or compact disk, they are "physically present on that hard drive or [compact disk]." In fact, Kumar stated that data can be "visible" in the "aggregate" when stored on a medium such as a compact disk. Kumar explained that although source code in its abstract sense as intellectual property does not have physical form, a "representation" of the source code is "concrete."

Despite this testimony, defendant argues that he did not

make a "tangible reproduction or representation" of Goldman's source code because the source code remained in an intangible state even when defendant saved it onto the server's hard drive. The relevant question, however, is not whether the source code itself was tangible, but whether defendant made a tangible *reproduction* of it, which he unquestionably did when he copied it onto the server's "physical" hard drive where it took up "physical space" and was "physically present" (*see People v Barden*, 117 AD3d at 231 n 5 [although a credit card number is intangible, it can be reduced to a tangible medium in the form of an imprinted plastic credit card]; *United States v Zhang*, 995 F Supp 2d 340, 349 [ED Pa 2014] ["information stored in computer hardware has a physical manifestation"]; *see also* Penal Law §§ 156.00[2], [3] [both a "(c)omputer program" and "(c)omputer data" can exist "in any form, including magnetic storage media, punched cards, *or stored internally in the memory of the computer*" [emphasis added]).

There is no merit to defendant's argument that the unlawful use statute could not have been intended to criminalize his conduct because it was enacted in 1967, long before the advent of the technology used by defendant to copy Goldman's proprietary information. Whether the legislature envisioned the specific type of technology that exists today is not dispositive of this

appeal. The statute was drafted with broad generalized language that fits squarely into today's digital world (*see People v Russo*, 131 Misc 2d 677, 681, 683 [Suffolk County Court 1986] [concluding that in drafting the unlawful use statute, the legislature provided an "an elastic . . . definition" for "secret scientific material" so as to include a "computer program" within its ambit]). It proscribes making tangible reproductions or representations of secret scientific material not only by means of "writing, photographing [and] drawing," but also by "mechanically or *electronically reproducing or recording* [the] material" (Penal Law § 165.07 [emphasis added]). There is no dispute that defendant's copying of the source code here was accomplished by "electronically reproducing" the code.

The trial court's apparent belief that the source code had to have been printed on paper in order to be tangible is at odds with the language of the statute. The statute merely requires a "tangible reproduction or representation" of the secret material, and is silent as to the medium upon which the reproduction or representation will reside. Thus, the fact that defendant made the reproduction onto a physical hard drive, rather than onto a piece of paper, is of no consequence. Both are tangible within the meaning of the unlawful use statute. It would be incongruous to allow defendant to escape criminal liability merely because he

made a digital copy of the misappropriated source code instead of printing it onto a piece of paper (*see Thyroff v Nationwide Mut. Ins. Co.*, 8 NY3d 283, 292 [2007], quoting *Kremen v Cohen*, 337 F3d 1024, 1034 [9th Cir 2003] ["'It would be a curious jurisprudence that turned on the existence of a paper document rather than an electronic one'"]).

The natural extension of the trial court's position is that even if defendant had copied the source code onto a compact disk or a thumb drive, and walked out of Goldman's premises with that device, he still would not have violated the unlawful use statute because no paper was involved. Such a result makes little sense because a compact disk and a thumb drive are both unquestionably tangible. The trial court's position also ignores the trial evidence that a hard drive can be taken out of the server, and thus has a physical presence independent of the computer in which it was housed.

Although no reported decision has addressed the meaning of the term "tangible" within the meaning of Penal Law § 165.07, the Court of Appeals' decision in *People v Kent* (19 NY3d 290 [2012]) is instructive. In *Kent*, the defendant was charged with procuring and possessing child pornography on his computer. The evidence showed that some of the images and videos had been downloaded onto the defendant's computer. The Court upheld the

defendant's conviction relating to these items because "[the] defendant downloaded and/or saved the video and the images, thereby committing them to the allocated space of his computer" (*id.* at 304). The Court also observed that a "hard drive" is "tangible" (*id.* at 301), and described the "tangibility of [a computer] image" as "its permanent placement on [a] hard drive and [the] ability to access it later" (*id.* at 302). Thus, *Kent* supports our conclusion that a "tangible reproduction or representation" of source code is made when it is saved to a physical medium, such as a hard drive.

Defendant's reliance on *Thyroff v Nationwide Mut. Ins. Co.* (8 NY3d 283 [2007], *supra*) is misplaced. In *Thyroff*, the Court concluded that the common-law tort of conversion can apply to electronic data stored on a computer, which the Court described as "intangible property" (*id.* at 292-293). First, it does not appear that the parties in *Thyroff* actually litigated the question of whether electronic data is tangible or not. In any event, the fact that the Court described electronic data as "intangible" does not undermine our conclusion here. Regardless of whether the source code itself is intangible, defendant unquestionably made a tangible reproduction of it, within the meaning of the unlawful use statute.

The Second Circuit's reversal of defendant's federal

conviction under the National Stolen Property Act (18 USC § 2314) does not change the result. That federal statute makes it a crime, as relevant here, to "transmit[], or transfer[] in . . . foreign commerce any goods, . . . knowing the same to have been stolen." The Second Circuit did not address the precise question presented here — whether defendant made a "tangible reproduction or representation" of the source code. Thus, the Second Circuit's interpretation of the federal statue, which has different elements from the unlawful use statute here, has no bearing on whether the trial evidence was sufficient to sustain the jury's verdict (*see Hartnett v New York City Tr. Auth.*, 200 AD2d 27, 32 [2d Dept 1994] ["A federal decision contrary in principle is not binding upon a State court in respect of a State statute"] [internal quotation marks omitted], *affd* 86 NY2d 438 [1995]).

Nor does the reasoning underlying the Second Circuit's decision call into question our conclusion here. In finding that defendant's conduct did not violate the National Stolen Property Act, the Second Circuit concluded that the source code transferred by defendant was "intangible property," and therefore was not a "stolen" "good" within the meaning of the federal statute (*see United States v Aleynikov*, 676 F3d at 78). As discussed earlier, the relevant inquiry under the unlawful use

statute is not whether the source code itself was tangible, but whether defendant made a tangible reproduction of it, which the evidence shows that he did.

We reject defendant's alternative argument that the trial evidence did not establish that he uploaded Goldman's source code to the hard drives of the German server. Although no Goldman source code was found on the hard drives at the time they were examined, there was ample proof that defendant had in fact uploaded the source code to them. First, defendant made statements admitting that he had done so. Next, transmission logs showed that the source code was uploaded to the German server, and subsequently downloaded to defendant's home computer. Finally, when defendant's home devices were examined, Goldman's source code was found on them.

Contrary to the trial court's conclusion, the evidence was legally sufficient to establish that defendant possessed the requisite mens rea. To sustain a conviction under the unlawful use statute, defendant must have acted with the "intent to appropriate to himself or another the use of" Goldman's source code (Penal Law § 165.07). Under Penal Law § 155.00[4], a person "appropriate[s]" property by exercising control over the property either (i) "permanently" or (ii) "for so extended a period or under such circumstances as to acquire the major portion of its

economic value or benefit" (*see People v Jennings*, 69 NY2d 103, 118 [1983] [the concept of "appropriate" connotes a purpose to exert permanent or virtually permanent control]).

In finding the People's proof lacking, the trial court focused only on the second prong of the definition of "appropriate," and failed to appreciate the first prong, which refers to the intent to "permanently" exercise control. Here, the People's proof at trial permits a rational inference that defendant intended to exercise permanent control over the use of Goldman's source code, as opposed to a short-term borrowing. The People presented evidence that defendant surreptitiously uploaded the source code to the German server, downloaded it onto several personal computing devices, and then shared it with his new employer, a potential competitor of Goldman. The evidence further showed that defendant took multiple measures to cover up his illicit transfer of the data. Further, the record contains no evidence that defendant ever tried to return the misappropriated source code to Goldman, or to delete it from his or his new employer's devices.

Because the evidence was sufficient to show defendant's intent to exercise permanent control, the People correctly argue that they were not required to prove the second prong of the definition of "appropriate," i.e., that defendant intended to

acquire the major portion of the economic value or benefit of the source code. Nor was it necessary for the People to prove that defendant intended to deprive Goldman of the use of the source code. The unlawful use statute only requires the intent to "appropriate" the use of the secret scientific material and does not require any intent to "deprive." Further, the statute does not require that defendant intend to appropriate the source code itself, but only the *use* of the code.

We have considered defendant's remaining arguments and find them unavailing.

Accordingly, the order of the Supreme Court, New York County (Daniel P. Conviser, J.), entered on or about July 6, 2015, as amended July 7, 2015, which, to the extent appealed from as limited by the briefs, granted defendant's motion for a trial order of dismissal to the extent of setting aside the jury's verdict convicting him of unlawful use of secret scientific

material, should be reversed, on the law, the motion denied, the verdict reinstated, and the matter remanded for sentencing.

All concur.

THIS CONSTITUTES THE DECISION AND ORDER
OF THE SUPREME COURT, APPELLATE DIVISION, FIRST DEPARTMENT.

ENTERED: JANUARY 24, 2017

CLERK