State of New York
Court of Appeals

OPINION

No. 47
The People &c.,
Respondent,
v.
Sergey Aleynikov,
Appellant.

Kevin H. Marino, for appellant.
Elizabeth Roper, for respondent.

FAHEY, J.:

Ideas begin in the mind. By its very nature, an idea, be it a symphony or computer source code, begins as intangible property. However, the medium upon which an idea is stored is generally physical, whether it is represented on a computer hard drive, vinyl

record, or compact disc. The changes made to a hard drive or disc when information is copied onto it are physical in nature. The representation occupies space. Consequently, a statute that criminalizes the making of a tangible reproduction or representation of secret scientific material by electronically copying or recording applies to the acts of a defendant who uploads proprietary source code to a computer server.

Background

In May 2007, defendant Sergey Aleynikov began employment at Goldman Sachs (Goldman), the investment banking and financial services company, as a computer programmer working on the firm's high-frequency trading software. High-frequency trading – which uses sophisticated, electronic trading tools, proprietary strategies, and computer algorithms to perform market data calculations and trade securities at very rapid speeds – is highly competitive. At the time, larger, established institutions competed with nimbler start-up companies, which were developing their software from scratch. As a senior employee in Goldman's technology division explained at defendant's trial, the firm sought to "stay competitive by constantly investing in and updating [its] software to be as fast . . . as possible, to have the best connectivity and infrastructure as possible and [to] have the best algorithm[s] as possible."

The computer code for Goldman's high-frequency trading system is a key to successful trading for several reasons, as the senior employee would testify. First, one essential value of the code is "[c]onnectivity," which "allows [a] computer program to speak to various stock exchanges or to have market data about what's going on in the world," including the price of a stock at "any given second." Second is its "business logic"

component, the algorithms that permit Goldman employees "to make a decision about what trade to generate or price to advertise, which price [to] buy or sell a security at." A third key component of the computer code is the "infrastructure" or "all the other software . . . to make [the] system run robustly through the trading day." Goldman's high-frequency trading software is a constantly updated version of a system acquired by the firm when it purchased a pioneering algorithmic trading company in 1999 for some half a billion dollars.

Defendant's primary responsibilities at Goldman included "the infrastructure components" of the stock group and "upgrading one of the exchange connectivity components." Defendant had complete access to the high-frequency trading system's source code, i.e., computer instructions written in a human-readable programming language. The source code was contained in the firm's "software repository" or library. A software developer such as defendant "could check out the code . . . make changes to it and test it locally, merge it with the changes of other individuals, and then have those changes become the production software that runs every day."

Goldman employees, however, were not permitted to remove a copy of source code from the company's network. Every Goldman employee signed a confidentiality agreement acknowledging that any software the employee is creating is the property of the firm. The employee confidentiality agreement stated that "[c]onfidential and proprietary information and materials shall be used only as authorized and only for the purposes intended by Goldman Sachs." Moreover, access to the source code while an employee was away from the office was restricted, with the only authorized access to the source code repository from home or while traveling being "remote log-in access to [the employee's]

desktop," which gave an employee "a window onto" the employee's Goldman desktop computer, while "all of the files and contents" would "stay inside Goldman Sachs." Programmers were not permitted to email source code to themselves.

By late 2008, defendant's annual remuneration at Goldman was $400,000, but, in the spring of 2009, defendant accepted an offer of employment at Teza Technologies (Teza), a Chicago-based start-up company, where his annual compensation would be $1.2 million. Teza had no equipment, connectivity, or software for high-frequency trading at the time. Its founder planned to develop high-frequency trading infrastructure and software from scratch, and urged new employees to "execute relentlessly" because the start-up was "up against experienced and very wealthy competitors." Defendant was to be the "head of infrastructure" and "the system architect."

On June 5, 2009, his last day at Goldman, defendant uploaded a large quantity of Goldman's high-frequency trading source code, via a website, to a subversion repository, i.e., a remote server to which a user could transfer code. He used the same username, "saleyn," that he had chosen for his personal email account. The internet security systems at Goldman generally blocked employee access to such websites, but had overlooked this one, based in Germany.

Defendant wrote a computer script to compress data from Goldman's source code repository into files known as "tarballs." Defendant ran this program, encrypted the resulting tarballs, and uploaded the source code to the German server. In particular, defendant uploaded Goldman's "Order Book Builder" or OBB software, used to process

market data from stock exchanges. Defendant then erased the tarballs. He also "back dated the script" to make it appear that it had been created two years earlier.

Subsequently, defendant downloaded the source code to his home computers. On June 9, 2009, Teza created an account on a website that allowed companies to share source code within a select group of users. Later that month, defendant placed high-frequency trading software in a source code repository on that website.

In late June 2009, Goldman employees responsible for the firm's information security discovered that unauthorized transfers of data from Goldman's repository had occurred in the early evening of June 5, 2009: over 13 megabytes of data in one transfer and over 4.5 megabytes of data in the other. The investigating team at Goldman identified the device from which the transfers had been conducted as defendant's work computer, and inspected its BASH history, which is a "record of commands issued by a given user to [a] computer."

The team retrieved the BASH history "from a snapshot directory" – saved on Goldman's computer network (rather than on defendant's computer itself) – showing recent past activity on defendant's computer. In this back-up BASH history, the investigators found "data transfer commands" related to the June 5 source code transfers. Moreover, the back-up BASH history revealed that defendant had entered a command to selectively remove, from the BASH history stored on his own computer, the copying of source code. Goldman contacted the Federal Bureau of Investigation.

Federal Action

FBI agents arrested defendant on July 3, 2009, after he returned from a trip to Teza's headquarters in Chicago. Defendant waived his Miranda rights and admitted that he had uploaded files from his work at Goldman to the German website and had subsequently downloaded the data to his home desktop computer. Defendant indicated that the data could also be found on his laptop computer, USB flash drive, and external hard drive. Defendant told an FBI agent that he had signed up for an account on the German website because Goldman had not "blocked" the site. Defendant suggested that he had kept the software because "he wanted to inspect the files much like a person in college would go back and read a paper." At first, defendant told the agent that he had uploaded and downloaded only files that contained open-source code, i.e., software developed by programmers in a collaborative manner and readily available to the public on the internet. However, after the agent began to ask questions revealing that the FBI knew the BASH history of defendant's computer, defendant suggested that he had transferred "more files than he intended to" from Goldman's high-frequency trading software library.

Defendant completed and signed a written statement, explaining the process whereby he had compressed, uploaded, and downloaded Goldman's high-frequency trading source code. Defendant again claimed that his initial purpose was "to collect open source work" from Goldman's repository that he "had previously worked on," which he "wanted to inspect . . . later," and he insisted that he had not shared Goldman's proprietary information with anyone.

In February 2010, a federal grand jury charged defendant with violation of the National Stolen Property Act, 18 USC § 2314, which makes it a crime to "transmit[], or transfer[] in interstate or foreign commerce any goods, . . . of the value of $5,000 or more, knowing the same to have been stolen," as well as violation of the Economic Espionage Act of 1996, 18 USC § 1832. Defendant proceeded to trial in the United States District Court for the Southern District of New York, and in December 2010 a jury found him guilty as charged. On appeal from the District Court's judgment of conviction and sentence, defendant argued that the source code was not a stolen "good" within the meaning of the National Stolen Property Act, and that the code was not "related to a product . . . used in or intended for use in interstate or foreign commerce" under the Economic Espionage Act.

In 2012, the United States Court of Appeals for the Second Circuit reversed, holding that the source code was "intangible property" and therefore not a "good" under the National Stolen Property Act (see United States v Aleynikov, 676 F3d 71, 76-79 [2d Cir 2012]). The Second Circuit ruled that "the theft and subsequent interstate transmission of purely intangible property is beyond the scope of the [National Stolen Property Act]" (id. at 77), which has, as its "basic element," a "taking of a physical thing" (id.). The federal court "decline[d] to stretch or update statutory words of plain and ordinary meaning in order to better accommodate the digital age" (id. at 79). The Second Circuit also held that defendant did not violate the Economic Espionage Act because the source code was not intended for use in interstate or foreign commerce (see id. at 82).

New York Action

In September 2012, defendant was charged in state court (see CPL 40.20 [2] [f]) with two counts of unlawful use of secret scientific material (Penal Law § 165.07) and one count of unlawful duplication of computer related material in the first degree (Penal Law § 156.30 [1]). Following pretrial motion practice and a suppression hearing and ruling not pertinent here, defendant proceeded to a jury trial in Supreme Court in April 2015.

The jury heard testimony from FBI agents and Goldman employees concerning the discoveries and admissions that had led to defendant's federal prosecution. In addition, the People called a number of witnesses who testified about the significance of the source code defendant had uploaded to the German server and then downloaded to his personal electronic devices.

Senior Goldman employees testified that having access to the firm's high-frequency trading source code would be useful to a competitor for a number of reasons. In addition to testimony about the value of access to Goldman's algorithmic "theoretical value library" of fair prices for stock, the jury heard that the infrastructure and connectivity aspects of the source code would be useful to a developer working at a start-up, because the developer "would have the answer in the back of the book from . . . tens or hundreds of people developing a system. If you are at a start-up and you are asked to undertake a task and you can refer to how that was done in a system that you know works, you will be much more productive, much more rapidly able to develop a system that works for the competitor."

The jury heard testimony regarding Goldman's OBB software. A former company vice-president who had supervised the firm's stock group testified as follows: "[y]ou

receive market data from exchanges. Effectively these are the orders that are . . . trying to trade in the market which then effectively makes up the price. But in addition to there being a price, . . . the exchange remembers all the orders that everybody has made on it and it communicates to everybody what this looks like . . . OBB is a way to organize all of these orders into what is called a book and present these books to the trading applications so they can understand the state of the market." Having an existing OBB program available to use as a reference would make it easier for a software developer to create a new high-frequency trading system and would improve a start-up's "time to market, meaning how long it would take a new trading venue . . . to start trading []effectively."

The computer engineer and algorithmic trader who had designed and developed Goldman's OBB, Navin Kumar, testified that he had spent a year and a half to two years on the project, and he explained that OBB was not dependent on other Goldman codes or libraries, and therefore would be easy to implement outside the firm. Most significantly, Kumar testified that the software that defendant placed in Teza's account at the source code repository website used "the same design as" Goldman's OBB software, including "[r]oughly a dozen" design decisions that the developer recalled making himself. Similarly, a cybercrime analyst at the District Attorney's Office testified that a comparison between what defendant uploaded to Teza's account at the repository website and corresponding material from Goldman revealed only minor modifications.

Kumar also gave testimony about the fundamental nature of source code, stating that "abstract source code," as intellectual property, does not have physical form, but that the "[r]epresentation of it" is "concrete." Kumar added that when computer files are stored

on a hard drive or compact disc, they are physically present on that drive or CD, and that data is visible "in aggregate" when stored on such a medium. For example, on "a burned CD, you'd be able to see . . . if anything is written." Similarly, an FBI agent testified that while source code itself is not something that can be touched and felt, code that is stored on a computer's hard drive "takes up physical space in a computer hard drive." In addition, the People called a German law enforcement officer who described how "physical drives," in the form of "two 400 gigabyte hard drives," had been removed from the subversion server.

At the close of the People's case, defendant moved for a trial order of dismissal, under CPL 290.10, arguing that the evidence was not sufficient to show that he had made "a tangible reproduction" of Goldman's source code, or to show his "intent to appropriate . . . the use of" the code. Defendant did not dispute that the source code constituted "secret scientific material" within the meaning of the pertinent definitional provision, Penal Law § 155.00 (6), or argue that he had copied only open source code. Supreme Court reserved decision on the motion.[1]

The jury found defendant guilty of unlawful use of secret scientific material committed on June 5, 2009, failed to reach a unanimous verdict on the other unlawful use count (related to an earlier date), and acquitted defendant of unlawful duplication.

[1] The principal defense witness was Teza's owner, who insisted that he had not hired defendant in the hope that he would copy source code from Goldman, but conceded that he had offered defendant by far the highest salary of the programmers he employed.

In July 2015, Supreme Court granted defendant's motion for a trial order of dismissal with respect to both unlawful use of secret scientific material counts and set aside the jury's verdict (49 Misc 3d 286 [Sup Ct, NY County 2015]). Observing that "[t]here was no evidence Aleynikov ever duplicated the source code he downloaded to a piece of paper, any medium where it could be touched or any medium outside a computer or thumb drive" (49 Misc 3d at 290), the trial court concluded that the source code was not a "tangible reproduction or representation" of the source code, within the meaning of Penal Law § 165.07. The court reasoned that although "[a]n electronic image can become tangible when it is printed on paper[,] . . . computer code does not become tangible merely because it is contained in a computer" (49 Misc 3d at 320).

Supreme Court also held that the evidence is legally insufficient that defendant intended "to appropriate . . . the use of" the source code under Penal Law §§ 165.07 and 155.00 (4). In particular, the trial court found no evidence that defendant "ever sold or attempted to sell the source code he transferred" (49 Misc 3d at 290), or that "Teza was motivated to hire [defendant] because of [his] unauthorized transfer of the code" or "earned any income from the source code [he] obtained" (id.).

The People appealed from Supreme Court's order to the extent it dismissed the unlawful use of secret scientific material count related to the June 5, 2009 transfer. (The People did not seek to reinstate the other unlawful use count.)

In 2017, the Appellate Division reversed Supreme Court's order, insofar as appealed from, denied defendant's motion and reinstated the verdict as to the challenged count, and remanded the matter for sentencing (148 AD3d 77 [1st Dept 2017]).

The Appellate Division held that defendant made a "tangible reproduction or representation" of the source code when he uploaded the code to the hard drive of the German server (see id. at 85). The Appellate Division pointed out that the issue was "not whether the source code itself was tangible, but whether defendant made a tangible reproduction of it" (id. [emphasis added]). The court held that defendant made a tangible reproduction of the code "when he copied it onto the server's 'physical' hard drive where it took up 'physical space' and was 'physically present'" (id.). The Appellate Division noted that "[t]he 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" (id.).

With respect to the question whether the unlawful use statute could have been intended to criminalize conduct involving 21st-century technology, the Appellate Division reasoned that "[t]he statute was drafted with broad generalized language that fits squarely into today's digital world" (148 AD3d at 86). The Appellate Division further observed that the statute "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'" (id., quoting Penal Law § 165.07).

The Appellate Division rejected Supreme Court's assumption "that the source code had to have been printed on paper in order to be tangible," explaining that

> "[t]he 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" (148 AD3d at 86).

The Appellate Division noted that

> "[t]he 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" (148 AD3d at 86-87).

The Appellate Division found support for its position that a "tangible reproduction or representation" of source code is created when the code is saved to a physical medium such as a hard drive in People v Kent (19 NY3d 290, 301-302 [2012]).

The Appellate Division wrote that the reasoning underlying the Second Circuit's decision did not call its conclusion into question.

> "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. 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" (148 AD3d at 88 [citation omitted]).

On the issue of intent, the Appellate Division held that "the evidence was legally sufficient to establish that defendant possessed the requisite mens rea" (id.). Supreme Court had "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" (id.).

> "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. . . . 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" (148 AD3d at 88-89).

A Judge of this Court granted defendant leave to appeal (29 NY3d 995 [2017]). We now affirm.

Analysis

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." Evidence is legally sufficient when "viewing the evidence in the light most favorable to the prosecution, 'there is a valid line of reasoning and permissible inferences from which a rational jury could have found the elements of the crime proved beyond a reasonable doubt'" (People v Reed, 22 NY3d 530, 534 [2014], quoting People v Danielson, 9 NY3d 342, 349 [2007]; see Jackson v Virginia, 443 US 307, 319 [1979]).

The crime of which defendant was found guilty is unlawful use of secret scientific material (Penal Law § 165.07), a class E felony. An individual is guilty of the crime "when, with intent to appropriate . . . the use of secret scientific material, and having no right to do so and no reasonable ground to believe that he [or she] has such right, [the individual] 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). The disputed elements in this appeal are "with intent to appropriate . . . the use of secret scientific material" and "tangible reproduction or representation of such secret scientific material." We discuss the "tangible reproduction" issue first.

I.

Defendant's initial contention is that there is legally insufficient evidence that the source code he uploaded and downloaded was tangible within the meaning of Penal Law § 165.07. Legislative history and case law guide our analysis of the issue.

Penal Law § 165.07, enacted in 1967 (see L 1967, ch 791), was intended to ensure that a defendant who makes a copy of secret scientific material, but does not take the original, is subject to criminal sanction even though the defendant has not committed larceny. The statute

> "works in tandem with the crime of larceny of secret scientific material [Penal Law § 155.30 (3)]. In the larceny, the defendant steals 'property' consisting of secret scientific material, for example, a document reciting a secret scientific formula. In the unlawful use, with the same larcenous intent with respect to the contents of the formula, the defendant, for example, photographs the document. 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'" (William C. Donnino, Practice Commentary, McKinney's Cons Laws of NY, Book 39, Penal Law § 165.07 at 200).

The Temporary Commission on Revision of the Penal Law and Criminal Code, which prepared the bill, explained that prior to its 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 [or she] [was] not stealing 'property'" (1967 NY Legis Ann at 21). Penal Law § 165.07 was intended "[t]o make this . . . type of conduct subject to criminal sanction" (id.).

The stimulus for the legislation (see id. at 20-21) was a federal case, United States v Bottone, in which defendants took, photocopied (at home), and then returned secret scientific documents – instructions for the manufacture of antibiotics and a steroid – from a drug manufacturing company, but did not take the documents permanently (see United States v Bottone, 365 F2d 389, 391 [2d Cir 1966]). The issue in Bottone was whether the documents had been "stolen" and "transport[ed]" within the meaning of the federal statute under which the defendants (and much later Aleynikov) were prosecuted, the National Stolen Property Act, 18 USC § 2314. Although the Second Circuit ruled that 18 USC § 2314 did apply, our legislature acted to ensure that there was no possible gap in the Revised Penal Law of 1967. The legislature thus sought to criminalize misappropriations of intellectual property that were not traditional takings, but resulted in tangible reproductions of the protected material.

The term "tangible" is not defined in the Penal Law. When a word used in a statute is not defined in the statute, dictionary definitions serve as "useful guideposts" in determining the word's "'ordinary' and 'commonly understood' meaning" (People v Ocasio, 28 NY3d 178, 181 [2016]). This follows from the principle that, generally, unless a contrary intent is clear, lawmakers employ "words as they are commonly or ordinarily employed" (People v Finley, 10 NY3d 647, 654 [2008], quoting McKinney's Cons Laws of NY, Book 1, Statutes § 232, Comment).

Dictionaries give two meanings of the word "tangible" that are pertinent for our purposes. One is a narrower definition that conforms closely to the word's etymology: "[c]apable of being touched; affecting the sense of touch; touchable" (Oxford English Dictionary, http://www.oed.com [last accessed April 19, 2018]). This definition – "[c]apable of being touched" – was one of the meanings of the term listed in the edition of Black's Law Dictionary that was current in 1967 (see Black's Law Dictionary 1627 [4th ed 1951]). Another meaning of "tangible," a derivative meaning, but equally valid, is "[m]aterial, externally real, objective" (Oxford English Dictionary, http://www.oed.com [last accessed April 19, 2018]), "[h]aving or possessing physical form; corporeal" (Black's Law Dictionary [10th ed 2014]), or "substantially real: material" (Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/tangible [last accessed April 19, 2018]). This definition – "real; substantial" – was also one of the meanings of the word

listed in the edition of Black's Law Dictionary current in 1967 (see Black's Law Dictionary 1627 [4th ed 1951]).[2]

Defendant invites us to accept only the more restrictive meaning, "touchable," and then to conclude that the source code he uploaded was intangible because, he maintains, code cannot be touched. Defendant's argument fails for two fundamental reasons. First, we decline defendant's invitation to focus on the narrow meaning of "tangible" ("touchable"). Interpreted in this manner, the term does not apply to ink printed on paper any more readily than to source code, and provides no workable criterion. Instead, we accept the dictionaries' lesson that "tangible" can also denote "material" or "having physical form." Second, the statutory language is unambiguous that the crime occurs when an individual "makes a tangible reproduction or representation of . . . 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]). What must be tangible is not the secret scientific material – here, the source code – but the reproduction or representation thereof. The question for the Court, then, is not whether source code is tangible, but whether defendant made a tangible copy or copies of source code when he uploaded source code to a server and downloaded it to his electronic devices.

[2] A third meaning, "[c]apable of being understood by the mind" (Black's Law Dictionary [10th ed 2014]), is figurative, and the People do not argue on appeal that the term "tangible" in the statute means "capable of being understood by the mind."

Once this distinction is made, it becomes clear that the Second Circuit's conclusion, that Goldman's source code was "purely intangible property . . . at the time of the theft" (Aleynikov, 676 F3d at 78), i.e., prior to being stored on the German server, has no direct bearing on the question before us today, namely whether the "reproduction or representation" that defendant made of the source code is tangible. A copy of source code may be tangible even if the source code itself is not.

Without leaving the confines of the trial evidence before us, we conclude that viewing the facts in the light most favorable to the People, a rational jury could have found that the "reproduction or representation" that defendant made of Goldman's source code, when he uploaded it to the German server, was tangible in the sense of "material" or "having physical form." The jury heard testimony that the representation of source code has physical form. Kumar, the computer engineer, testified that while source code, as abstract intellectual property, does not have physical form, the "[r]epresentation of it" is material. He explained that when computer files are stored on a hard drive or CD, they are physically present on that hard drive or disc, and further stated that data is visible "in aggregate" when stored on such a medium. The jury also heard testimony that source code that is stored on a computer "takes up physical space in a computer hard drive." Given that a reproduction of computer code takes up space on a drive, it is clear that it is physical in nature. In short, the changes that are made to the hard drive or disc, when code or other information is stored, are physical.

Defendant contends that if "tangible" means "having physical form," then the statutory term "tangible reproduction" would involve a redundancy because all computer

data is stored in some physical medium. We disagree. Someone with a photographic memory who memorized a piece of source code would not be making a tangible reproduction of the code (see generally Bottone, 365 F2d at 393 [referring to a hypothetical "case where a carefully guarded secret formula was memorized, carried away in the recesses of a thievish mind and placed in writing only after a boundary had been crossed"]). It is true that copying secret scientific material solely by memorizing it would not fall under the statute for a separate reason, i.e., that it would not be "writing, photographing, drawing, mechanically or electronically reproducing or recording such secret scientific material" (Penal Law § 165.07). Nevertheless, the word "tangible," as we interpret it, does not introduce redundancy; it adds a modest element to "reproduction," serving to emphasize that the crime consists in making a physical, not a mental, copy of secret scientific material.

Defendant also insists that the legislature did not use broad, open-ended language that could accommodate new forms of technology unforeseen in the 1960s. However, the language of Penal Law § 165.07 is broad, including all "mechanically or electronically reproducing or recording" of material. That the statutory language could have been made even broader does not imply that it is narrow to begin with. Moreover, the inclusion in the statutory language of material copied electronically supports the conclusion that the intent was not to limit the law to reproductions that are tangible in the sense of being able to be manually touched. Indeed, it would be absurd to suppose that the statute criminalizes photographs stored on film but not ones stored on a hard drive.

Further, defendant contends that when the Legislature enacted Penal Law § 156.30 (unlawful duplication of computer related material in the first degree), the first statutory

scheme in New York for prosecuting computer crime specifically, in 1986 (see L 1986, ch 514, § 1), the legislators apparently believed that the existing statutes did not address computer crimes and for that reason enacted laws criminalizing the reproduction in certain circumstances of computer data or computer programs. The argument is that the 1986 statute would not have been necessary if taking of computer data were included in the 1967 statute.

There is some support in the legislative history for defendant's contention. In 1986, the Division of Probation and Correctional Alternatives expressed the view that "modern technology in the area of computers has resulted in attempts or commissions of acts for improper purposes and/or inappropriate monetary gain. Unfortunately, law enforcement and prosecutors have been hindered by existing penal statutes which do not address these improper acts" (Letter from Linda J. Valenti, General Counsel, Division of Probation and Correctional Alternatives to Evan A. Davis, Counsel to the Governor, and Lawrence T. Kurlander, Director of Criminal Justice, dated July 1, 1986, in Bill Jacket, L 1986, ch 514, at 15). However, a closer inspection of the Bill Jacket suggests that the 1986 legislation was designed to "eliminate any doubt" that the taking of computer data can be subject to the Penal Law (Amended Memorandum of Attorney General Robert Abrams in Bill Jacket, L 1986, ch 514, at 35 [emphasis added]), rather than to fill an indisputably empty gap.

In any case, the focus of Penal Law § 156.30 is illegal use of computers generally, while Penal Law § 165.07 targets mechanical or electronic reproduction of scientific secrets. The two statutes criminalize different types of conduct. Of course, a defendant might be guilty under both statutory schemes if the defendant steals scientific secrets by

means of a computer, but the existence of the 1986 statute does not prevent the earlier statute from applying to computer crimes.

We conclude that there is legally sufficient evidence that defendant created a tangible copy of the source code on the German server in violation of Penal Law § 165.07.

II.

Our case law is not to the contrary. In Thyroff v Nationwide Mut. Ins. Co. (8 NY3d 283 [2007]), which defendant relies on, the question before the Court was whether information stored in the form of electronic records on a computer, rather than as printed documents, is subject to a claim of the tort of conversion in New York. The plaintiff was an insurance agent of the defendant, which leased the plaintiff computer hardware and software, to facilitate the collection and transfer of customer information to the defendant. The plaintiff used the computer system for data storage pertaining to his customers. After the defendant cancelled the plaintiff's contract, it repossessed the computer system and denied the plaintiff access to the electronic records and data.

The property that the defendant in Thyroff allegedly exerted control over and interfered with was plaintiff's "customer information and other personal information . . . stored on . . . computers" (id. at 285). The Court wrote that "the tort of conversion must keep pace with the contemporary realities of widespread computer use" and held "that the type of data that [the defendant] allegedly took possession of – electronic records that were stored on a computer and were indistinguishable from printed documents – is subject to a claim of conversion in New York" (id. at 292-293).

Defendant points to language in Thyroff implying that the electronic records in question constituted "intangible property" (id.). Thyroff is best read, however, as treating the allegedly converted information as intangible property, rather than as holding or implying that any electronic reproduction of the information stored on a computer was intangible. The Court had no need to analyze the nature, whether physical or intangible, of electronic reproduction, because it was the information itself that gave rise to the allegations of dominion or control over property amounting to conversion. To the limited extent that the Thyroff Court may have suggested that "the information was stored" in an intangible format on computers (see id. at 292), such suggestions amounted to dicta. Indeed, the point of Thyroff was that information "stored on a computer hard drive has the same value as a paper document kept in a file cabinet" (id.).

We came closer to addressing the issues of the present appeal in People v Kent (19 NY3d 290 [2012]), where, as relevant here, this Court rejected the defendant's contention that child pornography images he had downloaded to his computer were intangible and that he could not be convicted of possessing a sexual performance by a child.[3]

The defendant in Kent pointed out that the Penal Law defines "possess" as meaning "to have physical possession or otherwise to exercise dominion or control over tangible property" (Penal Law § 10.00 [8] [emphasis added]) and insisted that neither an image

[3] The Court also held a defendant may not be convicted of promoting a sexual performance by a child or possessing a sexual performance by a child solely on the basis of evidence of a web cache showing that the defendant accessed, and viewed on the computer screen, a child pornography image from a website, when the defendant did not download, save, print or otherwise manipulate or control the image (see Kent, 19 NY3d at 303-304).

appearing on a computer screen nor the computer representation that underlies it is tangible. This Court disagreed, embracing the perspective of federal courts "that for digital images to constitute evidence of knowing possession of child pornography, such images must be connected to something tangible (e.g., the hard drive) . . . and that the defendant must be aware of that connection" (Kent, 19 NY3d at 301, citing United States v Romm, 455 F3d 990, 1000 [9th Cir 2006]; United States v Tucker, 305 F3d 1193, 1205 [10th Cir 2002]). We summarized the federal courts' interpretation of the tangible quality of a computer image by referring to the image's "permanent placement on the defendant's hard drive and his ability to access it later" (Kent, 19 NY3d at 302).

Defendant interprets this language from Kent as contrasting intangible computer or internet images with tangible hard drives, and he would have us hold that the information he uploaded and downloaded is intangible in nature. The majority opinion in Kent, however, is entirely consistent with the principle that a representation of information stored on a hard drive is tangible. The contrast Kent sets out is the distinction between intangible information and physical storage. Just as in Kent we held that a defendant may be convicted of possessing a sexual performance by a child if the defendant knows that the images are stored on some tangible material in his possession, so we now hold that a defendant may be convicted of unlawful use of secret scientific material if the defendant makes a copy in the form of tangible material on a server. The Appellate Division properly interpreted Kent to support the conclusion that a defendant creates "a 'tangible

reproduction or representation' of source code . . . when it is saved to a physical medium, such as a hard drive" (148 AD3d at 87).[4]

III.

The last issue we must decide is whether there is legally sufficient evidence that Aleynikov had the necessary mens rea of "intent to appropriate . . . the use of secret scientific material" (Penal Law § 165.07). Defendant insists that he cannot have had that intent because he did not intend to deprive Goldman of the source code. Goldman could and did carry on using the source code after defendant copied it, and there was no evidence that he intended otherwise.

The Penal Law defines the term "to appropriate" in disjunctive terms. "To 'appropriate' property of another to oneself or a third person means (a) to exercise control over it, or to aid a third person to exercise control over it, permanently or for so extended a period or under such circumstances as to acquire the major portion of its economic value or benefit, or (b) to dispose of the property for the benefit of oneself or a third person" (Penal Law § 155.00 [4] [emphasis added]). Penal Law § 155.00 (4) (a) is implicated here. We read the clause "as to acquire the major portion of its economic value or benefit" as grammatically dependent on "for so extended a period or under such circumstances" and not on "permanently." Under Penal Law § 155.00 (4) (a), then, a person "appropriate[s]"

[4] Defendant cites other cases that, like Thyroff and Kent are concerned primarily with the question whether software or other computer data, as information, are intangible (see e.g. Am. Online, Inc. v St. Paul Mercury Ins. Co., 207 F Supp 2d 459, 468 [ED Va 2002], affd 347 F3d 89 [4th Cir 2003]; Lucent Tech., Inc. v Bd. of Equalization, 241 Cal App 4th 19, 42 [2015]), as opposed to whether a reproduction of software or code can be tangible.

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."

It follows that exercising permanent control over another's property is sufficient, without more, for appropriation within the meaning of the Penal Law. Contrary to the trial court's reasoning, determination of whether a defendant acquired the major part of the property's economic value or benefit is not necessary if the control (or, here, intended control) is permanent. The interpretation of appropriation then hinges on whether there was sufficient evidence that defendant intended to exercise control over the source code (or aid Teza to do so) permanently. If there was such intent, there is no need to engage in an analysis of the "major portion of its economic value or benefit" element.

Here, defendant concedes that he intended to exercise control over the source code permanently, alluding in his brief to the fact "that Aleynikov intended to permanently retain (i.e., did not intend to return) the copy he made of Goldman's source code." Instead, defendant insists that he cannot be guilty under Penal Law § 165.07 for merely copying the code, while leaving the original on the Goldman network, because appropriation is the "taking from another to one's self . . . to the exclusion of others" (People v Lammerts, 164 NY 137, 144 [1900]).

Defendant's argument fails. Appropriation does not imply depriving another of property. In fact, larceny in general is defined as involving either intent to appropriate or intent to deprive, with the clear implication that the two terms refer to separate concepts. Indeed, Penal Law § 155.00 defines "deprive" and "appropriate" separately, in § 155.00

(3) and (4) respectively. "A person steals property and commits larceny when, with intent to deprive another of property or to appropriate the same . . ., he [or she] wrongfully takes, obtains or withholds such property from an owner thereof" (Penal Law § 155.05 [1]; accord People v Jennings, 69 NY2d 103, 118 [1986] [stating that "the concepts of 'deprive' and 'appropriate' . . . connote a purpose . . . to exert permanent or virtually permanent control over the property taken, or to cause permanent or virtually permanent loss to the owner of the possession and use thereof"]).

Defendant's contention also reads the words "the use of" out of the statute, which refers to "intent to appropriate . . . the use of secret scientific material" (Penal Law § 165.07 [emphasis added]). In focusing on the appropriation of the use of scientific material, rather than appropriation of the material itself, the statute necessarily contemplates the simultaneous exercise of control by the rightful possessor of the scientific material.

Defendant relies on Almeida v Holder (588 F3d 778 [2d Cir 2009]), which analyzed a corresponding Connecticut statute. The Second Circuit wrote that "Connecticut defines 'deprive' for purposes of its larceny statute by reference to an owner's loss of his right to actual possession of his property," and "defines 'appropriate' to reach further, making larcenous actions that deny an owner constructive possession of his property, i.e., his ability 'to exercise control over it'" (Almeida, 588 F3d at 787-788). The federal court noted that Connecticut's "statutory scheme, in using 'intent to deprive' and 'intent to appropriate' to focus on different property rights, ultimately establishes a broad generic requirement of an intent to deprive another person . . . of some rights or benefits of property ownership" (Almeida, 588 F3d at 788). Defendant suggests that the Second Circuit held that one

cannot intend to "appropriate" the property of another without also intending to deprive the owner of that property, but there is no basis for that interpretation of Almeida. Instead, we interpret Almeida to mean that appropriation may involve depriving another of rights or benefits of property ownership that do not rise to the level of actual physical possession. Almeida is consistent with the principle that defendant may have intended to "appropriate" the source code without intending to deprive Goldman of all possession or use.

Defendant's remaining contentions lack merit.

Accordingly, the order of the Appellate Division should be affirmed.

* * * * * * * * * * * * * * * * *

Order affirmed. Opinion by Judge Fahey. Chief Judge DiFiore and Judges Rivera, Stein, Garcia, Wilson and Feinman concur.

Decided May 3, 2018