Court Examines Theft of Computer Code in 'Aleynikov'

by Steve Kramarsky

Technological advances, for all the good they bring to the world, often bring with them significant challenges for existing legal structures. As the pace of technological change accelerates, it can be difficult for the law to keep pace, and the jurisprudence of the printing press—or even the fax machine—may be a poor fit for the internet age. Nowhere are those challenges more apparent than in the realm of criminal law. Criminal statutes have life-changing consequences, and must be strictly interpreted. And in that context, courts have sometimes struggled to apply fit "pre-internet" statutes to conduct that occurs in the electronic realm.

For example, more than a decade ago New York courts faced the issue of whether the tort of conversion—the civil action for misappropriation of tangible property—should apply to files stored on a computer. The issue was unsettled in New York, and the U.S. Court of Appeals for the Second Circuit certified the question, which noted that the "'ancient doctrine' has gone through a great deal of evolution" since it appeared in the 15th century, see Thyroff v. Nationwide Mut. Ins., 8 N.Y.3d 283, 286 (N.Y. 2007) (internal citations omitted). With that in mind, the court held that, in the modern age, there was no good reason to limit the tort to tangible property. Because "it generally is not the physical nature of a document that determines its worth, it is the information memorialized in the document that has intrinsic value" and "the tort of conversion must keep pace with the contemporary realities of widespread computer use" the court held that theft of electronic records stored on a computer could be the basis for a civil claim of conversion.

But the criminal law—perhaps appropriately—moves more slowly. And courts continue to struggle with issues around criminal liability for theft of property stored in electronic form. Many criminal statutes proscribing theft were drafted with "physical" or "tangible" property in mind. They were drafted at a time when it was unimaginable that vast amounts of sensitive data—developed at great expense and having enormous commercial value—would be stored in something called the "cloud." Without delving into the metaphysical, it is not clear to what extent such information is within the scope of traditional criminal laws prohibiting the theft of "tangible" property. But a series of recent criminal cases against a single defendant, tried in both the Southern District of New York and New York Supreme Court, highlights the challenges presented by the theft of "intangible" property.

After substantial disagreement among the lower courts (and across the federal and state courts) the recent decision of the New York Court of Appeals provides some clarity and is worth a review.

'People v. Aleynikov'

On June 5, 2009, Sergey Aleynikov worked his last day at Goldman Sachs. Aleynikov had been employed as a computer programmer tasked with developing sophisticated electronic trading tools and computer algorithms to facilitate Goldman's high-frequency trading. During his two years of employment at the bank, Aleynikov was tasked with developing the "infrastructure" of Goldman's high-frequency trading platform. In layman's terms he was not responsible for developing the software algorithms that decided what stocks to trade or how to trade them; rather he had primary responsibility for developing the supporting software infrastructure to make the high-frequency trading "system run robustly through the trading day," in People v. Aleynikov, 2018 WL 2048707, 2018 N.Y. Slip Op. 03174, at *1 (N.Y. Ct. App. May 3, 2018).

Through his position, Aleynikov had access to the "source code" for the trading systems he worked on—the versions of the code written in human-readable programming language. After Aleynikov resigned from Goldman, he immediately joined a Chicago-based start-up company which had offered to triple his annual compensation, from $400,000 a year to $1.2 million a year. He was to be the "head of infrastructure" and "system architect" of a brand new high-frequency trading platform at his new job.

On his last day, Aleynikov uploaded portions of Goldman's source code to a remote server outside of Goldman's systems. Like most corporate employers, particularly in the financial industry, Goldman strictly prohibited such transfers but Aleynikov took a number of steps to evade Goldman's security systems—hiding the file transfer in an encrypted file, uploading it to a German system, and entering various commands to erase his tracks. Shortly after commencing employment at his new firm, Teza Technologies, Aleynikov transferred Goldman's source code to his personal computer and then to a source code repository maintained by Teza. It was not until the end of June 2009—almost a month after he resigned—that Goldman discovered Aleynikov had transferred the source code shortly before his resignation. Upon discovering the theft, Goldman contacted the FBI and Aleynikov was arrested. Aleynikov promptly admitted that he had uploaded the source code to a German server, which he knew would not be detected by Goldman's first layer of security, and then downloaded that code onto his personal computer, though he initially claimed he had taken only "open source" (publicly developed) code and that he had done so only for research purposes.

The Federal Proceedings

In February 2010, Aleynikov was charged by a federal grand jury with violation of the National Stolen Property Act "which makes it a crime to 'transmit, or transfer in interstate or foreign commerce any goods" over a certain value as well as the Economic Espionage Act.

A jury found Aleynikov guilty on both counts, but Aleynikov appealed, "arguing that the source code was not a stolen 'good' within the meaning of the National Stolen Property Act" nor "related to a product … used in or intended for use in interstate of foreign commerce" under the Economic Espionage Act.

In 2012, the Second Circuit reversed the conviction, holding that the source code was "intangible property" and thus not a "good" under the definition of the National Stole Property Act. The Second Circuit acknowledged that the source code was "highly valuable" and acknowledged that "the value of the intangible code … vastly exceeds the value of any physical item on which it might be stored." Nonetheless, because "federal crimes 'are solely a creature of statute'" the Second Circuit reversed the trial court, declining "to stretch or update statutory words of plain and ordinary meaning in order to better accommodate the digital age," in United States v. Aleynikov, 676 F.3d 71, 76-79 (2d Cir. 2012).

The New York Action

In September 2012, while the federal proceedings were pending, Aleynikov was charged in New York state court with two counts of unlawful use of secret scientific material (Penal Law Section 165.07), which generally prohibits making an unauthorized "tangible reproduction or representation" of secret scientific material, and one count of unlawful duplication of computer-related materials in the first degree (Penal Law Section 156.30[1]). After a trial, the jury found Aleynikov guilty of unlawful use of secret scientific material. In July 2015, the Supreme Court granted Aleynikov's motion for a trial order of dismissal, setting aside the jury's verdict. The Supreme Court held that "there 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." In essence, the Supreme Court held that the copying the source code to an external repository was not a "tangible reproduction"—the Supreme Court was, in some sense, agreeing with the Second Circuit.

In 2017, the Appellate Division reversed, reinstating the verdict, following which Aleynikov appealed to the Court of Appeals. The Court of Appeals affirmed the Appellate Division's decision. The Court of Appeals began its analysis with an examination of the purpose of Penal Law Section 165.07—to ensure that a defendant who makes a copy of secret scientific material, but does not take the original, is subject to criminal sanction." The law was introduced to fill a potential gap in the criminal law, made apparent by the rise of photocopying and other reproduction technology, and "thus sought to criminalize misappropriations of intellectual property that were not traditional takings, but resulted in tangible reproductions of the protected material." As in the federal proceedings, the Court of Appeals' decision thus depended on a definition of the word "tangible."

The Court of Appeals defined "tangible" as "material" or "having physical form." Relying on testimony that the source code "takes up physical space in a computer hard drive," the court held that Aleynikov made a "tangible reproduction" of that source code when he copied it to an external source. The court wrote, somewhat poetically: "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 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."

A Tangible Inconsistency?

At first blush, it appears that two appellate courts reached inconsistent conclusions as to whether electronically stored information is "tangible" for purposes of criminal statutes. However, upon closer inspection, as explained by the Court of Appeals, the decisions are not inconsistent because they posed fundamentally different questions. In United States v. Aleynikov, the Second Circuit determined that the source code itself was intangible because that was the focus of the federal criminal statute at issue. The Court of Appeals, on the other hand, focused on the reproduction of the source code—its physical manifestation on an external hard drive—because that was the focus of the New York statute. That reproduction was tangible: it "took up space" on the hard drive of the German server, for example. Whether that's accurate or not is a metaphysical question (a 1 takes up the same amount of physical space as a 0) but it is certainly true that the hard drive itself is a tangible object on which the copy exists. In any case, the Court of Appeals noted that "a copy of source code may be tangible even if the source code itself is not."

And it is unclear, for purposes of New York criminal law, whether that distinction even matters. The Court of Appeals did not take a position as to whether the source code itself was tangible property. Under its reasoning—that storage of the source code occupied physical space on a hard drive—it stands to reason that the Court of Appeals might similarly hold that computer code is tangible property. After all, does the code have an existence separate from the medium in which it is stored?

For now, the Court of Appeals has managed to stay ahead of the technological curve—finding a 1967 law malleable enough to apply to millennial misconduct. However, technology marches on and one suspects that the next shift in storage technology, or the next clever hacker, may raise further difficult questions as to the "tangibility" of stolen data.

This article first appeared in the *New York Law Journal* on May 21, 2018. John Millson, an associate at the firm, assisted with the preparation of this article.