Law360

Another Decision In Goldman Code Theft Case

By **Jonathan Waisnor** (July 11, 2018)

Jonathan Waisnor

On May 3, 2018, the New York Court of Appeals unanimously affirmed the conviction of Sergei Aleynikov for unlawfully using secret scientific material.[1] The Court of Appeals held that a person who uploads a copy or reproduction of a former employer's proprietary source code to a server or other electronic storage device without authorization may be subject to criminal liability. The Court of Appeals further held that a person could act with intent to misappropriate source code even where the act of copying or reproducing the source code would not deprive the former employer of the ability to use or control the original source code.

Background

The Aleynikov case involved a long and complicated prosecution that has been described as a "legal odyssey."[2] Aleynikov, a computer programmer, began work at Goldman Sachs in May 2007, developing high-frequency trading software, and signed a confidentiality agreement acknowledging that any confidential or proprietary software was property of the firm and could not be used in an unauthorized manner. In 2009, Aleynikov was hired by a startup, Teza Technologies, to develop Teza's high frequency trading software from scratch. In violation of his confidentiality agreement with Goldman, Aleynikov uploaded a large quantity of Goldman's high-frequency trading source code to his own repository and the repository used by Teza. This code could be used to create new high frequency trading software.

In 2010, Aleynikov was charged in federal court and convicted of violations of two federal statutes, the National Stolen Property Act, 18 USC § 2314, and the Economic Espionage Act of 1996, 18 USC § 1832. The United States Court of Appeals for the Second Circuit reversed his conviction, holding that the proprietary source code was not a "physical thing" under the statute and that "purely intangible property" was beyond the scope of the National Stolen Property Act, and that Aleynikov's activities did not violate the Economic Espionage Act because they were not sufficiently related to a product produced for or placed in interstate commerce.[3]

Aleynikov's State Court Proceedings

Aleynikov was then charged in New York state court with violations of Penal Law 165.07, New York's statute criminalizing the unlawful misappropriation or reproduction of secret scientific material. Penal Law 165.07 makes it unlawful for a person "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 ... 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." Secret scientific material is defined as "a sample, culture, micro-organism, specimen, record, recording, document, drawing or any other article, material, device or substance which constitutes, represents, evidences, reflects, or records a scientific or technical process, invention or formula or any part or phase thereof" that is not available to unauthorized users, and that would give a user an advantage over competitors or other persons.[4] [5]

Aleynikov was convicted of one violation of Penal Law 165.07. His conviction was vacated by the trial court, and reversed by the Appellate Division.[6] On appeal to the New York Court of Appeals, Aleynikov's primary argument was similar to the one upon which the Second Circuit reversed his federal convictions; that the statute required "tangible reproduction or representation," which implied that the reproduction must have physical form, and computer code did not have a physical form.

However, the Court of Appeals interpreted tangible to mean "physical in nature." It then held that, while the source code itself may not be tangible, the focus of the statute was on whether the reproduction or representation was "tangible." Under this reasoning, the prosecution's evidence that code on a hard drive or CD physically takes up space and alters the hard drive or the CD was sufficient evidence for a jury to find that source code was tangible. The Court of Appeals observed that by enacting Penal Law 165.07 in 1967, the Legislature hoped to ensure that a defendant who copied secret scientific material, but did not physically take or remove it, would be subject to criminal sanction, giving the example of a person who made copies of blueprints without taking the blueprints themselves.

The Court of Appeals also held that there was sufficient evidence to show that Aleynikov acted with intent to appropriate the secret scientific material, even though Aleynikov's reproduction of the source code would not deprive Goldman from using the original. The Court of Appeals found that Penal Law 165.07 required only that Aleynikov exercise an intent to control the use of his copy of the source code, and that the statute contemplated the simultaneous exercise of control by the rightful possessor of the scientific material and by the wrongful user. The Court of Appeals thus affirmed Aleynikov's convictions.

Conclusion

The Aleynikov case demonstrates that employees who attempt to use the proprietary source code of their former employers without authorization may face not only the risk of civil liability, but also prosecution under New York's unlawful use statute. Furthermore, in response to the Second Circuit's decision in Aleynikov, Congress expanded the scope of the Economic Espionage Act, meaning that employees may also face liability under federal criminal laws to the extent that the source code they misappropriated relates to a product or service intended for interstate commerce.

The Aleynikov case began with a complaint from Goldman Sachs to federal law enforcement authorities. The success of the prosecution demonstrates that employers who learn that an employee is copying their proprietary source code for an unauthorized purpose may not only pursue civil claims against the employees, but may also refer the matter to local authorities for criminal prosecution. While the decision to investigate and prosecute will always lie within the scope of the prosecution's discretion, the "odyssey" that was the Aleynikov case demonstrates the seriousness with which law enforcement authorities will pursue crimes based on the unlawful use of source code.

Employers who are considering hiring employees who had access to their former employer's source code should be aware of the possibility that these employees may attempt to unlawfully use their former employer's source code and that this may expose them to criminal liability. Furthermore, because Penal Law 165.07 is a Class E felony, employers who aid in an employee's unlawful use of source code might also face prosecution for aiding and abetting a felony under New York laws prohibiting criminal facilitation, criminal solicitation, or conspiracy to commit a felony. Employers, especially those in technology-related industries, should keep this in mind when recruiting potential employees that are likely to have had access to valuable proprietary source code of their current or former employers.

It remains to be seen whether any employers would be prosecuted for aiding and abetting the conduct of their employees who unlawfully use source code of a former employer, or what facts might be sufficient to trigger such prosecution. In light of the Aleynikov decision and Congress' amendment of the Economic Espionage Act, employers may want to take more aggressive steps to guard against the suggestion that they influenced or endorsed an employee's unlawful use of source code from a former employer. Employers should consider having the prospective employee represent that he or she is not, and does not plan to be, in violation of any noncompetition or confidentiality agreement and will not use any source code or other proprietary computer data from his or her former employer. Employers should also be wary of suspicious bulk transfers of source code to their own repositories or systems. It may be advisable for employers to institute training programs to educate employees regarding the laws surrounding the unlawful use of source code.

Finally, a robust compliance or internal audit program would serve to both ensure that new employees remain in compliance with federal and state laws regarding unlawful use of source code, and to rebut any suggestion that the employer encouraged or facilitated such activity.

Jonathan D. Waisnor is an associate at Willkie Farr & Gallagher LLP.

[1] People v. Aleynikov, No. 47, 2018 WL 2048707 (N.Y. May 3, 2018)

[2] https://www.bloomberg.com/news/articles/2017-01-24/aleynikov-s-conviction-is-reinstated-by-state-appeals-court; https://www.nytimes.com/2017/01/30/business/dealbook/a-former-goldman-employees-long-strange-legal-odyssey.html.

[3] United States v Aleynikov, 676 F3d 71, 76-79 (2d Cir 2012).

[4] Penal Law 155.00(6).

[5] Aleynikov did not raise, and the Court of Appeals declined to reach, the issue of whether source code is within the definition of secret scientific material.

[6] People v. Aleynikov, 148 A.D.3d 77 (1st Dep't 2017).