PULLMAN &COMLEY LLC
ATTORNEYS

Cyber Law TRACKER
Developments in Cybersecurity

A publication of Pullman & Comley, LLC

April 30, 2012

# The Second Circuit Reverses Conviction of Computer Programmer and Holds that Theft of Intellectual Property Is Not Necessarily Criminal

*By T. Scott Cowperthwait*
*April 27, 2012*

Earlier this month, the U.S. Court of Appeals for the Second Circuit seemingly stripped federal prosecutors of the use of two statutes used to combat the theft of intellectual property, critical technologies and other proprietary and sensitive business information, when it reversed the conviction of Sergey Aleynikov. See *United States v. Aleynikov*, --- F.3d ---, 2012 WL 1193611 (2d Cir. 2012). As discussed below, the Aleynikov opinion has far-reaching implications for companies seeking to protect their intellectual property and other proprietary products and information. It further serves as a lesson that now is the time for companies to review internal policies and processes relating to identifying and protecting intellectual property, computer use and removable media and information sharing between human resources, management, information technology and security.

In February 2010, a grand jury sitting in the U.S. District Court for the Southern District of New York returned an indictment charging Mr. Aleynikov, a computer programmer formerly employed by Goldman Sachs & Co. who helped to write the source code for Goldman's proprietary high-frequency trading (HFT) system, with (1) theft of trade secrets in violation of the Economic Espionage Act of 1996, 18 U.S.C. § 1832 (the "EEA"), (2) transportation of stolen property in interstate and foreign commerce, in violation of the National Stolen Property Act, 18 U.S.C. § 2314 (the "NSPA"), and (3) unauthorized computer access, in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA").

Goldman kept this source code and the other components of the HFT system highly confidential. Goldman did not license its proprietary system to third parties, and prohibited employees, like Mr. Aleynikov, from taking it or using it when their employment ended.

In April 2009, Mr. Aleynikov accepted an employment offer with Teza Technologies LLC, a startup company based in Chicago that sought to develop its own HFT system. On his last day of employment at Goldman, Mr. Aleynikov uploaded, compressed and encrypted approximately 500,000 lines of source code and proprietary data stored on Goldman's servers, and transferred this data to an external server located in Germany. Mr. Aleynikov then deleted the encryption program and history of computer commands from his Goldman computer. He subsequently downloaded the source code from the server in Germany to his home computer and copied some of the files to other computer devices. Approximately one month later, Mr. Aleynikov traveled to Chicago to attend meetings at Teza and brought with him a flash drive and a laptop computer containing portions of the source code.

Prior to trial, the U.S. District Court for the Southern District of New York dismissed the CFAA count against Mr. Aleynikov because the district court concluded that he was authorized to access the Goldman computer, did not exceed the scope of his authorization, and that authorized use of a computer in a manner that misappropriates information is not an offense under the CFAA. On December 10, 2010, a jury convicted Mr. Aleynikov of violating the EEA and NSPA. On appeal, Mr. Aleynikov challenged his conviction, arguing that (1) the source code is "a purely intangible product" and therefore not a "good" that was "stolen" within the meaning of NSPA, and (2) the source code is not "related to or included in a product that is produced for or placed in interstate or foreign commerce" within the meaning of the EEA.

In considering the applicability of the NSPA to the theft of intellectual property, the Second Circuit explained that "[t]he decisive question is whether the source code that Aleynikov uploaded to a server in Germany, then downloaded to his computer devices in New Jersey, and later transferred to Illinois, constituted stolen 'goods,' 'wares,' or 'merchandise' within the meaning of the NSPA." The Second Circuit examined historical appellate precedent from other circuit courts before concluding that that the theft of "purely intangible property," such as the HFT system's source code, even if such "intangible property" is later transferred to "a tangible medium," does not constitute a crime under the NSPA.

With respect to the EEA conviction, the Second Circuit noted that Mr. Aleynikov's conviction under the EEA, which contains two operative provisions -- one focused on foreign espionage and the other on domestic theft -- was limited to the domestic provision. The Second Circuit noted that the domestic provision of the EEA applies only to those trade secrets that are "related to or included in a product that is produced for or placed in interstate or foreign commerce." In reviewing the district court's decision and the applicability of the EEA's domestic provision, the Second Circuit concluded that "[b]ecause the HFT system was not designed to enter or pass into commerce, or to make something that does, Aleynikov's theft of source code relating to that system was not an offense under the EEA." In reaching this conclusion, the Second Circuit focused on Goldman's strict confidentiality policies designed to keep in "strict confidence" Goldman's proprietary information, including its HFT system and source code, and noted that Goldman that did not sell or license its HFT system.

The Aleynikov opinion significantly limits potential criminal liability under the NSPA and EEA in matters of economic and industrial espionage involving the theft of intellectual property, critical technologies and other proprietary and sensitive business information. In short, the opinion is troubling in that it seems to penalize companies which go to great lengths to protect their in-house intellectual property from entering the competitive marketplace and public domain. The Aleynikov matter reiterates the need for companies to develop effective cybersecurity and counterintelligence policies and programs designed to limit vulnerability issues, identify internal sources of information theft, and develop effective lines of communication between a resigning or terminated employee's manager, human resources, information technology and security. By increasing internal awareness and understanding of the current threat from intellectual property theft, companies may be able to reduce the risk, exposure and impact of intellectual property theft.

A copy of the Second Circuit's opinion in *United States v. Aleynikov*, --- F.3d ---, 2012 WL 1193611 (2d Cir. 2012) can be accessed here.