New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
White-Collar CRIME
WWW.NYLJ.COM
TUESDAY, OCTOBER 9, 2012

Prosecutors Seek Guidance in Battle Against **Cyber Theft**

Second Circuit's 'Agrawal' decision could provide answers.

BY BENJAMIN GRUENSTEIN

After its release in April, the decision of the U.S. Court of Appeals for the Second Circuit in *United States v. Aleynikov*[1] was widely hailed as one that would likely weaken companies' ability to protect their most important computer trade secrets. At a time when prosecutors are sounding the alarm about the increasing risks of cyber crimes—going so far as to refer to cyber threats to American businesses and government as "the next Pearl Harbor; one of the greatest existential threats facing the United States"[2]—the Second Circuit appeared to limit the reach of two of the statutory tools available to combat the theft of computer trade secrets: the National Stolen Property Act (NSPA) and the Economic Espionage Act (EEA). However, much remains to be learned about whether, and to what extent, these statutes have in fact been narrowed, and a Second Circuit decision likely to be handed down in the coming months in the case of *United States v. Agrawal* will likely provide much needed guidance on these questions.

Second Circuit's 'Aleynikov' Decision

In 2009, the U.S. Attorney for the Southern District of New York charged Sergey Aleynikov, a former computer programmer at Goldman Sachs, with stealing the computer code for Goldman's proprietary high-frequency trading (HFT) system and unlawfully providing it to his new employer.[3] Aleynikov was alleged to have committed this crime by uploading sections of the HFT's source code to an Internet server in Germany and subsequently downloading the files to his personal computer and flash drive.[4] On Dec. 10, 2010, a jury in the Southern District convicted Aleynikov of violating both the NSPA—which criminalizes the interstate transportation of stolen property[5]—and the EEA—which criminalizes the theft of a trade secret "produced for or placed in interstate commerce."[6] Aleynikov was subsequently sentenced to 97 months in prison. On April 11, 2012, the Second Circuit reversed Aleynikov's convictions, holding that neither statute applied squarely to Aleynikov's actions.

The Second Circuit reversed Aleynikov's conviction under the NSPA, holding that the code stolen was intangible property and that intangible property does not constitute "goods" within the meaning of the NSPA.[7] Citing previous decisions of the First, Seventh, and Tenth circuits, the court held that "the theft and subsequent interstate transmission of purely *intangible* property is beyond the scope of the NSPA."[8]

The Second Circuit also reversed Aleynikov's conviction under the EEA. Although the EEA criminalizes stealing a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce,"[9] the court held that Goldman's HFT system

was not "produced for or placed in" interstate commerce.[10] In arriving at its decision, the court reasoned that Goldman's HFT system was not "produced for" interstate commerce, because:

> Goldman had no intention of selling its [trading] system or licensing it to anyone. It went to great lengths to maintain the secrecy of its system. The enormous profits the system yielded for Goldman depended on no one else having it.[11]

It did so despite evidence offered by the government at trial that, in 1999, Goldman had purchased a company, the crucial asset of which was its HFT system and that, as of the date of Aleynikov's theft, Goldman's HFT system incorporated many aspects of the HFT system that Goldman had purchased.[12]

On first blush, the *Aleynikov* decision appears to carry broad—and odd—implications. After *Aleynikov*, the theft of a thumb drive containing

BENJAMIN GRUENSTEIN *is a partner in the litigation department of Cravath, Swaine & Moore.*

source code would be illegal under the NSPA, but an electronic transfer of that same code—surely within the technical capabilities of computer thieves—would not. Similarly, after the Second Circuit's decision, the EEA appears to criminalize the theft of run-of-the-mill trading code on the theory that it could be bought or sold, but not the theft of highly valuable trading code, the owner of which would not dream of selling it in interstate commerce or otherwise.

'Aleynikov' Reexamined in 'Agrawal'

The Second Circuit's decision in *Aleynikov* is unlikely to be the court's last pronouncement on the topic. Shortly before the conviction in *Aleynikov*, another jury in the Southern District convicted another defendant for the theft of proprietary source code, also under the NSPA and the EEA. The defendant, Samarth Agrawal, worked in Société Générale's High Frequency Trading group in New York and, in the several months before resigning his position, copied modules of code to his personal network drive, created text documents containing the code and printed out the documents.[13] He subsequently provided a competitor and potential employer with information about the code, including detailed schematics of the structure of the code and mathematical formulae and algorithms contained in the code.[14] After the jury convicted him of violating both the NSPA and the EEA, the court sentenced Agrawal to 36 months in prison.[15] Agrawal, who has been detained since his April 2010 arrest, is due to be released from prison in the coming months.

The appeal in *Aleynikov* was decided before the briefing in *Agrawal* was completed. Thus, on appeal, the government sought to distinguish the facts in *Agrawal* from those in *Aleynikov*, noting that, unlike Aleynikov, Agrawal did not digitally transmit the code but rather printed it out, thus stealing a tangible good (the paper on which the code had been printed). This, the government argued, was dispositive of the NSPA count, as earlier cases make clear that the theft of "tangible goods" is within the scope of the statute.[16] And, in *Aleynikov* itself, Chief Judge Dennis Jacobs recognized that:

> [t]here was no allegation that [the defendant] physically seized anything tangible…such as a compact disc or thumb drive containing source code, so we need not decide whether that would suffice as a physical theft.[17]

Because Agrawal did "assume physical control" over a tangible object—the printouts of the text files he created—he, unlike Aleynikov, did deprive his employer of their use to some degree, and did violate the NSPA.

The government also sought to distinguish *Agrawal* from *Aleynikov* on the basis that it had argued to the jury in *Agrawal*, but not in *Aleynikov*, that the stolen code was not only included in the HFT system, but also "related" to the securities traded by the HFT system.[18] Relying on the plain text and legislative history of the EEA, the government argued on appeal "that a trade secret may relate to, but need not be included in, the product that is placed in or produced for interstate commerce."[19] Given that the government in *Agrawal* had argued to the jury that the product at issue was the traded securities, and not the HFT program itself, the EEA conviction should stand, the government argued, because the computer code "related to" the traded securities and those securities "products" that were "produced for or placed in interstate commerce."

Conclusion

The impact of *Aleynikov* after *Agrawal* remains to be seen. With respect to the NSPA, the court in *Agrawal* will have the opportunity to clarify a point that the *Aleynikov* court stated it need not decide: that had Aleynikov stolen a *tangible* item containing source code, such as a compact disc or thumb drive, that theft of code could be prosecuted under the NSPA.[20] Ultimately, however, even if the Second Circuit goes on to make this point explicit, the practical import of such a ruling will be unclear, given that any code thief capable of stealing code via a physical medium could likely also do so by transporting the code across state lines through some "intangible" means.

With respect to the EEA, however, the court in *Agrawal* could significantly negate the import of *Aleynikov*, limiting it to cases where the government had taken the position that the nexus to interstate commerce was the computer program itself in which the code was contained and not the securities that were traded using this program. If the court in *Agrawal* adopts the government's position, and finds that the interstate commerce nexus was satisfied by virtue of the traded securities, then the Second Circuit will have restored the EEA as a reliable means to prosecute theft of code cases, even when the code is part of an invaluable program that its owner would never place in the stream of commerce. *Aleynikov* would no longer stand in the way of prosecutors' ability to bring charges under the EEA in such a case, as commentators had feared, but would rather simply inform the theory under which they charge those cases and ultimately argue them to juries.

1. 676 F.3d 71 (2d Cir. 2012).

2. Preet Bharara, "Asleep at the Laptop," The New York Times, June 4, 2012, at A25.

3. 676 F.3d at 73-74 (2d Cir. 2012).

4. Id. at 74.

5. 18 U.S.C. §2314.

6. Id. §1832.

7. 676 F.3d at 78.

8. Id. (emphasis added) (citations omitted).

9. 18 U.S.C. §1832.

10. 676 F.3d at 82.

11. Id. (internal citation omitted).

12. Brief for Appellee at 43, United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012) (No. 11-1126).

13. Brief for Appellant at 4-5, United States v. Agrawal, No. 11-1074 (2d Cir. Dec. 30, 2011).

14. Id. at 6.

15. Judgment, United States v. Agrawal, No. 1:10-cr-00417-JSR.

16. United States v. Bottone, 365 F.2d 389, 393 (2d Cir. 1966).

17. 676 F.3d at 78.

18. Supplemental Brief for Appellee at 5, United States v. Agrawal, No. 11-1074 (2d Cir. May 14, 2012).

19. Id. at 11.

20. Aleynikov, 676 F.3d at 78 (declining to answer the question, though recognizing the First Circuit's holding that the NSPA "does apply when there has been some tangible item taken, however insignificant or valueless it may be, absent the intangible component" (quoting United States v. Martin, 228 F.3d 1, 14-15 (1st Cir. 2000)) (emphasis in original)).