Brandon Buchanan
Internet and Computer Law
March 27, 2013

Trade secrecy is an important topic that deals with the secret information that companies create and protect for their financial well-being and in which keeping the information private provides its economic benefit. When individuals or organizations attempt to steal this information for their own financial gain, an act of espionage is committed. However, ~~given circumstances of~~ in real life situations, the grounds for what constitutes espionage can be tricky.

In ~~An~~ important judicial decision made in December 2010, ~~involving a case in which~~ the defendant, Sergey Aleynikov was convicted of espionage and sentenced to eight years in prison after downloading around 32 megabytes of software code of a high frequency trading platform from his employer, Goldman Sachs, but a federal appeals court reversed the decision in April 2011 after he had spent nearly a year in jail. Aleynikov was prosecuted under the Economic Espionage Act, as well as the Computer Fraud and Abuse Act and the Interstate Transportation of Stolen Property Act, but the defendant's second lawyer argued to the appeals court that since Goldman Sachs gave permission for Aleynikov to access the code, no computer fraud laws were broken, and more importantly, since the secretive software was never intended to be licensed or sold, the defendant had not performed an act of espionage. In recent news, the state of New York is attempting to prosecute Aleynikov under its state laws, but this may be an issue because it would place the defendant in double jeopardy.

In December 2012, Yihao "Ben" Pu, faced a lengthy jail sentence due to his copying of confidential source code from his former employer and plaintiff Citadel. The source code was of a trading program that executes trades on a frequent basis based on its predictions of market fluctuations, similar to the circumstances of *Goldman Sachs v. Aleynikov*. Pu was prosecuted under the Economic Espionage Act, which addresses trade secrets and its theft, without regards as to how Pu was to use the information that he copied. The defendant's lawyers argued the same premise as Aleynikov lawyer's – that the software protected by Citadel was never intended to be sold or licensed, therefore exempting Pu from being prosecuted under the Economic Espionage Act. The case is still pending.

These judicial decisions are important from protecting employees from overprotective and overbearing companies as related to their internal information. Aleynikov alleges that most of the code that was copied from Goldman Sachs included open source code that was already freely available to the public. Under most open source licensing rights, any project that incorporates open source code shall also release its source code, though as a multi-billion dollar company, Goldman Sachs is not likely to give up any portion of its source code for its trading platforms, and would argue that its source code disclosure is not necessary despite its use of open source code. It does not seem fair that Goldman Sachs would be excluded from releasing ~~their~~ its source code if it contains open source code, while Aleynikov would have spent eight years in prison for copying parts of the code that were already publicly known, including that the percentage of code that Aleynikov "stole" was around 3.2%, not likely to cause severe detriment to his former employer. This precedent in favor of the defendant helps to level the playing field so that large corporations cannot improperly accused former employees of espionage for stealing trade secrets when the secrets in questions are never meant to be sold in the first place.

watch agreement

- Sources??
- Interesting cases! Citations?

93