

500,000 Lines of Source Code: The New “Intangible Property”

Editorial Board

Posted on July 17, 2015



Sergey Aleynikov’s six-year trade secret odyssey through all possible configurations of litigation, civil and criminal, federal and state, may at long last have come to an end after the New York Supreme Court recently overturned his only surviving criminal conviction for unlawful use of secret scientific material. We here at *Trade Secrets Watch* have closely tracked Aleynikov’s journey, recently reporting on his [newest victory](#), and previously covering his convoluted trials and tribulations. In particular, prior to the recent New York Supreme Court decision, the Second Circuit overturned Aleynikov’s convictions under the Economic Espionage Act (EEA) and the National Stolen Property Act (NSPA), which also led to a change in the [EEA legislation](#).

Importantly, Manhattan Supreme Court Justice Daniel Conviser’s 72-page opinion underscores the severe difficulty of obtaining state court trade secret theft convictions in an era where rampant technological development outpaces decades-old legislation. Justice Conviser’s opinion hinges on the word “tangible” in an archaic law in finding that the electronic transmission of source code from one computer to another does not constitute a “tangible” reproduction of the allegedly misappropriated code. This holding, which follows the federal court’s 2012 holding overturning an [earlier conviction](#), places valuable trade secrets at a tremendous risk as society becomes increasingly electronic and cloud accessible.

Justice Conviser’s recent opinion—echoing the federal court before him—ruled that New York’s outmoded criminal trade secret statute, which has not been amended since its enactment in 1967, did not apply to Aleynikov because transferring source code electronically from point A to point B does not constitute “tangible reproduction” of the code. New York’s unlawful use of secret scientific material [statute](#) requires a “tangible reproduction or representation of such scientific material.”

“Tangible” is nowhere defined in the statute nor in (the scarce) supporting case law. Instead, Justice Conviser analyzed dictionary definitions, including the infamous Black’s Law Dictionary, to conclude that the term “tangible” means “the manifestation of a thing in the physical world.” In other words, tangible requires having a physical form. The Court held the prosecution did not submit evidence proving the source code “could be touched” or had any physical characteristics, even though the source code existed on servers in New York, Germany, *and* later on Aleynikov’s computer in New Jersey. According to the Court, “computer code does not become tangible merely because it is contained in a computer.”

Both *Aleynikov* cases raise challenging issues for intellectual property owners and government prosecutors prosecuting trade secret theft, especially in the modern technological world we live in. Indeed, Justice Conviser is acutely aware of this risk as he stated, “in today’s world, an electronic transmission may be much more potentially damaging to the holder of valuable intellectual property than a paper record.”

At this point, trade secrets owners and prosecutors are hanging their heads in defeat at the seemingly dim prospect of ever obtaining justice when there isn’t a tangible misappropriation of the trade secret. However, a patent law principle—the *Beauregard* claim—may provide a sliver of hope to utilizing some existing criminal trade secret laws, and perhaps create new ones, to mitigate the increased risk of electronic transmission of proprietary information.

A *Beauregard* claim is a computer readable medium (“CRM”) claim that protects intellectual property, such as source code for performing steps of a process, embodied within computerized systems or devices. A CRM claim is not one of the statutory defined categories of patentable inventions, 35 U.S.C. § 101 (“process, machine, manufacture or composition of matter”). Instead, a CRM claim is a judicial creation, established to comport with the statutory language in response to technological evolution, and consistent with the policy underlying the Patent Act. With a CRM claim, a patent holder can pursue infringement claims under *Beauregard* to protect source code—the very thing Judge Conviser said was intangible.

In fact, a plaintiff can pursue the claim without actually proving that the infringer used the source code, provided that the source code could perform the subject matter recited in the CRM claim. For example, in *Finjan, Inc. v. Secure Computing Corp.*, the Federal Circuit affirmed a finding of infringement for the sale of software that was capable of infringing, even though the infringing features were disabled. It did not matter if the defendant was actually using the infringing feature. Rather, the deciding question was whether the software embodying the infringing feature is *simply capable* of infringing patent holder’s protectable software code. The fact that the features were disabled, the *Finjan* court said, “does not detract from or somehow nullify the existence” of a finding of infringement because “to infringe a claim that recites capability and not actual operation, an accused device *need only be capable of operating* in the described mode.”

Finjan is particularly instructive in the trade secret context because information transferred electronically can still embody highly valuable info—and in Aleynikov’s case, massive quantities of proprietary source code information—even if the information is not transcribed in a physical medium. Transferring data electronically from point A to point B, in the words of *Finjan*, should not “detract from or somehow nullify the existence” of trade secret theft. Yet, by distinguishing between “tangible” and “intangible,” and finding that source code only has value when it exists in a physical medium, current criminal trade secret statutes may be too narrowly construed and/or are failing to adequately protect critical corporate secrets, and could actually increase the risk of employees transmitting data electronically. In a world monopolized by electronic data, criminal trade secret statutes would provide for more protection if the statutes focused on substance and not form in protecting a company’s secret recipe.

This entry was posted in [Criminal](#), [Cybersecurity](#), [Economic Espionage](#), [Employee Misappropriation](#), [Patents](#), [Policy](#), [Practical Tips](#), [Trade Secrets](#), [Trial](#), [Verdicts](#). Bookmark the [permalink](#).

[← Hacking Your Rivals – Corporate Espionage in Major League Baseball](#)

[Fifth Circuit Revisits Copyright Preemption of Trade Secret Law →](#)

 Print Page


Search ...

Search

Awards and Achievements



Recent Tweets

 **Orrick** 23 hours ago


Orrick’s Alyssa Caridis will discuss recent court cases on attorney misconduct at the annual Berkeley-Stanford Advanced Patent Law Institute, being held Dec. 12-13 in Palo Alto. The conference will cover the full range of [#patentlaw](#) issues. bit.ly/2DLVLCz

Retweeted by Trade Secrets Watch

 **Trade Secrets Watch** 1 week ago

Eight months after MillerCoors filed a lawsuit against AB for [#falseadvertising](#) and [#trademark](#) dilution, AB filed a motion to add a counterclaim for [#tradesecrets](#) misappropriation against MillerCoors. blogs.orrick.com/trade-secrets-...

From Corn-Gate to You-Stole-My-Trade-Secrets-Gate (Maybe): Defendant Beer Maker Moves to Add a Counterclaim for Trade Secrets Misappropriation in False Advertisement Litigation

 **Trade Secrets Watch** 1 month ago

The Workforce Mobility Act has been reintroduced in the Senate and, if passed, would restrict the use of [#noncompetes](#) more thoroughly than any recent state legislation. Our blog explains. blogs.orrick.com/trade-secrets-...

Congress Aims to Restrict Use of Non-Competes Nationwide

 **Trade Secrets Watch** 1 month ago

Our blog explains why an order issued by a federal judge in Chicago may encourage more aggressive prosecution of attempted [#tradesecret](#) theft, particularly as the government continues to focus on China’s potential acquisition of U.S. IP. blogs.orrick.com/trade-secrets-...

Court Upholds One Year in Prison for Theft of non-Trade Secrets

 **Orrick** 1 month ago

What’s new in [#corpgov](#) and [#securities](#) law? Our team analyzes recent rulings and other trends and offers key takeaways. Retweeted by Trade Secrets Watchbit.ly/32lu7RE

Trade Secrets Watch Weekly Update

[Subscribe here](#)

Events

No Events

Categories

Select Category ▼

Posts Archives by Month

Select Month ▼