Daily Journal

Intellectual Property, Corporate
Sep. 27, 2019

The scourge enveloping Silicon Valley: trade secret theft

As recent cases have exposed, trade secret theft from former employees and potential business partners have become a scourge in the high-tech world of Silicon Valley.

LAWRENCE M. HADLEY
Partner, Glaser Weil Fink Howard Avchen & Shapiro LLP

Email: lhadley@glaserweil.com

Lawrence is chair of the Intellectual Property Department and co-chair of the Crisis Management & Response Department.

See more...

CHRISTOPHER MCANDREW
Associate, Glaser Weil Fink Howard Avchen & Shapiro LLP

Email: cmcandrew@glaserweil.com

Christopher work in the firm's Intellectual Property Department.

See more...

Anthony Levandowski, a former autonomous vehicle engineer with Google and, later, Uber, leaves a courthouse in San Jose, Aug. 27, 2019.(New York Times News Service)

Silicon Valley was built to foster innovation. Technology giants and startups alike flocked to the California hotspot to produce some of world's most innovative products. At its inception and peak, Silicon Valley encouraged engineers to take the time (often years) to create something new and unimaginable. But as time went on, competition became fiercer in the Valley. Pressure to innovate quickly, fueled by competition for venture capital dollars, made speed combined with innovation a must.

Some companies, eager for venture capital dollars and faster times to market, seek a shortcut -- trade secret theft. And in the high-tech world, many companies' most highly valuable trade secrets are vulnerable to theft, particularly from departing employees looking for a shortcut in their next venture. As recent cases have exposed, trade secret theft from former employees and potential business partners have become a scourge in the high-tech world of Silicon Valley.

Trade secrets are the livelihood of innovative, high-tech companies looking for the next technology breakthrough. Under the common definition, trade secrets can be any information used in business that provides a company an economic advantage over competitors who do not know or use the information. Trade secrets may be found in computer source code, development timelines, trial and error analyses, business plans, pricing models, customer targets, and, not least significant, strategies for raising venture capital. Often the result of years of sweat and millions of dollars in research and development, a company's proprietary and trade secret information are the "crown jewels" -- often irreplaceable once disclosed and potentially fatal in the hands of a competitor seeking traction in the same target markets.

The landscape surrounding trade secret protection has not always been the same. In Silicon Valley's early days, trade secret protection, while necessary and important, was not considered a technology company's most valuable intellectual property. Rather, the focus of intellectual property protection

revolved around a strong patent portfolio -- often a prerequisite for securing the venture capital funding needed to enter the market.

But protecting innovation though patenting ideas takes an approach much different from trade secret protection. For example, Coca Cola's formula is still protected as a trade secret, instead of as a publicly disclosed formula in a patent that would have expired decades ago. Instead of keeping innovations secret, the patent system relies on a government-granted protection. In exchange for publishing an innovation in a patent, the government grants the owner 20 years of exclusive rights in the invention. Yet over the last 20 years, companies have found that enforcing granted patent rights against alleged infringers is not only and exorbitantly expensive and a years-long process, shifts in patent law, including availability of injunctions, limitations on damages, claim construction uncertainty, and new procedures to challenge validity, have made protecting innovation through patents sometimes illusory. While Silicon Valley high-tech companies still patent certain inventions, many have turned to simply keeping their most innovative ideas and work -- with some shunning the patent system altogether. Now many venture capitalist are more interested in what a company has kept secret as opposed what it has disclosed in patents.

But protecting innovation as trade secrets requires, as the name implies, secrecy. In the era of free and frequent employee mobility, keeping innovation secret among competitors is not as easy as it sounds. The documentary "The Secrets of Silicon Valley" explores big high tech's surveillance of the American population and manipulation of consumer behavior. Yet for years, a not very well-kept secret in Silicon Valley has been that not much is secret between competitors. California has a well-known legal policy favoring employee mobility. And once an engineer or business executive knows a companies' secrets, those secrets cannot be unlearned when the employee departs for a job with the new competitor across the Valley who offers more money and stock bonuses. The same is true when a group of engineers and executives, believing their employer is missing a market opportunity, decide to depart and form their own startup.

When this happens, the temptation to not only use what the former employee has learned in the prior job, but to actually take some of the innovations and business ideas that the employee helped develop with the prior employers, proves too much to resist. And for creative engineers and executives, taking trade secrets from one startup to a new employer, whether a new startup, an established tech giant, or anything in between, can be much too easy despite contractual prohibitions and even the best security available. Tiny electronic storage devices can hold as much data as a main-frame computer did 25 years ago. Most high-tech employees own laptop computers and mobile computing devices. Phones have high quality digital cameras. Startup operating on limited venture capital investments simply cannot devote the time and energy needed to bring a product to market and still maintain security like the NSA -- and even the NSA, as we know from Edward Snowden, has soft spots in its security. China may cost U.S. industry billions in trade secret theft, but within Silicon Valley alone, the cost of just former employees helping themselves to trade secrets when departing for a new employer may have just as large of an impactful on the U.S. economy. Even worse, if left unsolved, trade secret theft

in Silicon Valley will adversely affect the venture capital dollars needed to create new innovation in the first place.

Recent statistics provide solid evidence of the Silicon Valleys' trade secret theft epidemic. Lex Machina, a LexisNexis company, released a report showing a substantial increase in in the number of trade secret case filings -- skyrocketing by more than 30% in 2017. That same report estimated losses from trade secret misappropriation exceeding hundreds of millions of dollars.

Both high-profile federal indictments and trade secret litigation further demonstrate the extent of trade secret theft in Silicon Valley. Just recently, the U.S. attorney in Silicon Valley returned a 33-count indictment charging Anthony Levandowski, the former Google engineer and at the center of a trade secrets lawsuit between Uber and Waymo, with federal trade secret theft relating to self-driving vehicle technology. Levandowski was charged after allegedly downloading more than 14,000 files before leaving Waymo and forming his own competing business, before folding his new business into Uber. If found guilty, Levandowski could face up to 10 years in prison.

In another criminal matter, federal prosecutors have charged six former and current Fitbit employees in an indictment for misappropriating stolen trade secrets involving wearable technology from Jawbone -- their former employer and Jawbone competitor. In the underlying litigation between the companies, Jawbone offered evidence that the six indicted former employees pilfered over 300,000 confidential files that they took to Fitbit. Even though Jawbone was forced to cease business, the parties settled the outstanding litigation.

On the civil litigation side, for example, real estate data-analytics startup, HouseCanary, was subjected to a concerted and aggressive effort to illicitly and fraudulently misappropriation its core analytical technology by a massive competitor, Title Source (now known as Amrock), which sought a shortcut in its effort to become a real estate technology company. Following an extended jury trial, HouseCanary, obtained a jury verdict exceeding $706 million against Title Source/Amrock trade secret misappropriation and fraud. The verdict was the largest for intellectual property matters in the U.S. in 2018. In a less publicized ongoing case between AI software rivals, Quid, Inc. accused its former CTO (Sean Gourley) as well as two former data scientists (Emmanuel Yera and Amy Heineike) of taking numerous computer devices, including laptops, hard drives, and removable storage devices, containing over 100,000 files of source code and other data, to Dr. Gourley's new AI startup, Primer Technologies.

What can be done? Several solutions can be put in place so that Silicon Valley, while remaining competitive, can continue to innovate with less risk of theft and continued investment of venture capital dollars.

First, federal prosecutors have taken a critical initial step in returning high-profile indictments against former employees accused of taking trade secrets to new employers. This alone should have a significant chilling effect on employees who might otherwise be tempted to help themselves to their former employers' trade secrets. Continued efforts in this area, in cases both big and small, is

essential.

Second, California law should be revised so that noncompete provisions in employment contracts to protect their trade secrets, within appropriate limitations, are more easily enforceable. While court have reached different results, noncompete provisions in California employment contracts are often found to be unenforceable. The California Legislature should allow such provisions, subject to reasonable limitations as to time period, scope and position.

Third, California trade secret law should be modified to eliminate draconian provisions that place needless barriers in trade secret misappropriation actions against former employees. Under California Code of Civil Procedure Section 2019.210, a plaintiff in a trade secret action must disclose with reasonable particularity the trade secrets allegedly misappropriated before any discovery will commence. These required disclosures often result in satellite litigation over the adequacy of the disclosures -- thereby delaying resolution and increasing costs. No other states impose such requirements. Nor does the federal Defense of Trade Secrets Act impose such a requirement. While the trade secret disclosure might make sense in a case where Coca Cola accuses a competitor of stealing its secret formula to Coca Cola, it can create an impossible burden when a company discovers that a former engineer walked out the door with a 12-terabyte disk drive full of company documents and data.

In sum, Silicon Valley tech companies must be vigilant when it comes to protecting its trade secrets. But the scourge of trade secret theft, particularly by departing employees, is not a problem that will be easily solved with increased security. Better enforcement in both the criminal and civil justice system is needed to reduce the temptation to take a former employers' trade secrets so that fair competition and innovation can continue to attract investment dollars.