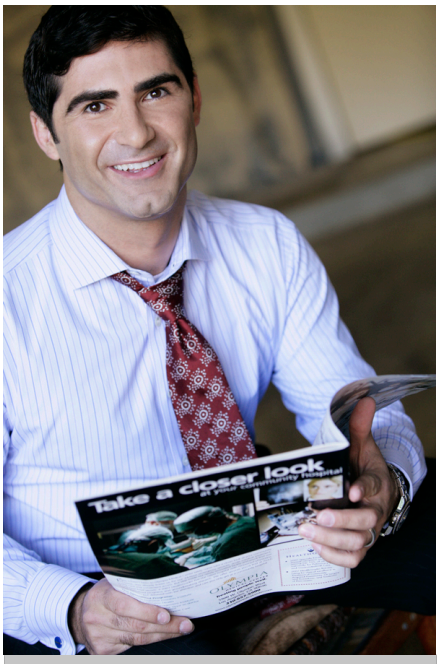
TSIRCOU | INTELLECTUAL PROPERTY LAW

The Drone Took My Secrets: Trade Secret Law in the Age of Drones



Trade Secret Law in the Age of Drones

- The standard required to protect information so it remains "secret" changes with drones
- Businesses must take possibility of drone surveillance into account when auditing security.

The concern over drone technology seems to be a ubiquitous worry in society these days. From near collisions with commercial aircraft at large international airports, or impeding fire-dropping aircraft from operating out of fear of collision, to simple privacy concerns over potential spying flying cameras, there is many issues that drones raise, and we are only in the infancy of the technology. However one overlooked area has been the interaction of drones with a little discussed area of intellectual property protection, trade secret law.

Trade secret law is a form of intellectual property protection without the use of trademarks, copyrights or patents. This term was brought into public discussion when in 2014 Elon Musk announced he was relying on this form of protection for his sensitive corporate information rather than patents (most of which he has given to the public domain). How trade secret law works is fairly simple: The Uniform Trade Secret Act (UTSA) says in order to be a "trade secret" information must not be publically available, and the business must make reasonable efforts to keep said information confidential. State laws define trade secrets similarly by using language like "reasonable security procedures and practices to protect the information from unauthorized access." In essence, if someone steals information that is not public, and you have taken efforts to keep it that way, that person is liable. However, once the information is not a secret anymore, the egg is already broken, it cannot become "secret" again, and anyone taking that information is not liable. This brings us to the strange convergence with drones.

WWW.TSIRCOULAW.COM
515 S. Flower Street, 36th Floor
Los Angeles, CA 90071

The required "reasonable steps" for keeping information "secret" is changing...

A case that helped outline the elements of trade secret law was *E.I. DuPont deNemours & Co. V. Christopher*. In this case, it was held DuPont did not voluntarily disclose confidential corporate information when a competitor of DuPont's flew an aerial surveillance airplane over a DuPont factory under construction, taking pictures through a hole in the roof. The information was not available to the public (by virtue of it being enclosed behind factory walls) and "reasonable steps" had been taken to keep said information secret (by construction of the factory walls). The fact there was a temporary hole open in the roof during construction did not make the information suddenly "available to the public". This case was decided in 1970 however, today it remains to be seen what efforts qualify as "reasonable" to protect your secrets.

In 1970 it was beyond the pale of imagination to say it was reasonable to have anyone other than extremely wealthy individuals or corporations to fly aerial surveillance cameras, however nowadays with $400 and zero experience, anyone can fly a high definition camera a few hundred feet vertically, and many thousands of feet horizontally. What were once reasonable measures to protect your business from unwanted disclosure of confidential information has now completely changed. In hand with this, the amount of "reasonable effort" necessary to keep confidential information protected under trade secret law has similarly changed. This begs the question, what is a business to do?

On the extreme end of the spectrum, no one is advocating to shoot unwanted drones out of the sky. While they may be seen as potentially prying into sensitive information, the drones themselves are property of someone's. This means the destruction, damage, or deprivation of a drone will give its owner legal recourse against you or your business. There are other less-aggressive aerial defense mechanisms being developed such as "geo-fencing", GPS signals not allowing drones to enter into certain designated areas, or signal jamming, impeding the drone's ability to communicate with its operator or send signals such as images. It must be remembered that places of business do not enjoy the same expectation of privacy as somewhere like your home, so laws like "Peeping Tom" laws making it illegal to look in one's window will not always apply in the situations discussed. The law is not necessarily going to protect you, so it is in the hands of businesses to be proactive. On the other hand the law may in fact hurt you if you decide to take too aggressive of vigilante measures into your own hands. While this is certainly an area ripe for case law, no such precedential guidance exists as of now.

So while the question remains, what is a business to do, it is now a fact that businesses must account for drones and their relationship to trade secret laws. When conducting an audit of "reasonable measures taken to keep information confidential", one must consider all the ways potentially prying eyes could "reveal" said information. Even flying cameras in the sky.