The Law in US, China and Europe

By Donal O'Connell

In this paper, Donal O'Connell, Managing Director of Chawton Innovation Services, discusses the changes in the law relating to trade secrets that have taken place in the United States, Europe and China.

USA:

The Defend Trade Secrets Act enacted on May 11, 2016 is a United States federal law that allows an owner of a trade secret to sue in federal court when its trade secrets have been misappropriated.

The act was signed into law by President Barack Obama and underscored Congress's desire to align closely with the Uniform Trade Secrets Act, which had been adopted in some form in almost every U.S. state. Technically, the DTSA extended the Economic Espionage Act of 1996, which criminalizes certain trade secret misappropriations. After the DTSA's passage by the Senate, Forbes magazine called the law the 'Biggest Development in Intellectual Property in Years'.

The recently passed Defend Trade Secret Act in the USA has a long reach, a reach so long that the new law should be as much of a concern to British, German, Chinese or Japanese companies as it is to US companies. The new law's reach has also been extended by tethering it with the US federal racketeering law.

One of the first DTSA litigations, for example, was brought against a researcher at Monsanto who was accused of stealing trade secrets to benefit his new employer in China (Monsanto vs Chen). German, British, Canadian, and Chinese companies have thus far appeared in US courts as either defendants or plaintiffs in DTSA cases. Other non-US companies have also likely been involved but tracking trade secret cases in the US federal court database is not straightforward.

How does a non-US company get snared? Well there are a number of ways in which a non-US company could get snared by the DTSA. In order to understand how, it is important to first understand that filing a DTSA complaint in a US federal court requires both "subject matter jurisdiction" and "personal jurisdiction". Then non-US companies need to understand the concept of "extraterritorial jurisdiction". Extraterritorial jurisdiction is the legal ability of a government to exercise authority beyond its normal boundaries.

And finally, non-US companies need to appreciate that the DTSA's reach has also been extended by tethering it with the US federal racketeering law. For subject matter jurisdiction, the civil provisions of the DTSA apply to the misappropriation of trade secrets if the "interstate commerce or foreign commerce" requirement of the law is satisfied.

The provision is spelled out in 18 U.S. Code § 1832 of the former Economic Espionage Act that served as the basis for the DTSA:

> a) Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—
>
> > 1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
> > 2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
> > 3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
> > 4) attempts to commit any offense described above; or
> > 5) conspires with one or more other persons to commit any offense described above, and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.
>
> b) Any organization that commits any offense described above shall be fined not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

The DTSA differs from its predecessor Economic Espionage Act in that the DTSA, among other things, provides for a civil cause of action for parties harmed by a trade secret theft.

Personal jurisdiction under the DTSA, for the most part, resembles personal jurisdiction under the bulk of US federal law. So, for example, personal jurisdiction against a non-US company might be established in these situations for example:

- The company sell products or services in the US and runs into a trade secret dispute there;
- The company has a business relationship with a US company (e.g., supplier, distributor, partner, subcontractor, customer, etc.), and the trade secret dispute involves the US company;
- The actual theft of the trade secret takes place in the US;
- An employee of the company leaves and goes to work for a US business, and takes the trade secret with them, or
- An employee of a US company leaves and goes to work for the non-US company and takes the trade secret with them.

Personal jurisdiction is often a litigated factual and legal matter as well as often requiring a constitutional analysis. So, cut and dried answers to personal jurisdiction can become complicated and require individual analysis by legal counsel.

The DTSA also retains the extraterritorial jurisdiction of its predecessor Economic Espionage Act where:

- The offender is a US citizen or permanent resident; or
- The offender is an organization organized under the laws of the United States or any State or political subdivision thereof; or
- An act in furtherance of the offense was committed in the United States

The DTSA also amended the RICO Act by adding theft of trade secrets under DTSA sections 1831 and 1832 as a racketeering activity, also known as a “predicate act.”

Racketeering, often associated with organised crime, is the act of offering of a dishonest service (a "racket") to solve a problem that wouldn't otherwise exist without the enterprise offering the service. The Racketeer Influenced and Corrupt Organizations (RICO) Act became US law in 1970, permitting law enforcement to charge individuals or groups with racketeering. Racketeering as defined by the RICO act in the USA includes a list of over 30 different crimes. If convicted of racketeering, a person could serve up a lengthy prison sentence and be fined a significant amount of money.

RICO provides civil plaintiffs with a separate cause of action related to trade secret misappropriation with different elements and damages. In some cases, a civil RICO claim could possibly bring higher damages than a trade misappropriation claim. Among other things, this change may allow non-US defendants to be hauled into US courts as co-conspirators in a RICO case as an alleged “criminal enterprise” based on a pattern of racketeering activity, e.g., a series of actions involving the theft of trade secrets.

For example, if a multinational company has the habit of stealing trade secrets from start-up companies whose products they find attractive, then the multinational might possibly find itself accused of being a criminal enterprise and facing extremely severe penalties in US federal court.

Civil RICO litigation typically depends upon whether the defendant’s predicate acts constitute a pattern. A “pattern” means that at least two predicate acts were committed, that the predicate acts were related to one another, and that the predicate acts amount to or pose a threat of continued criminal activity. The US Supreme Court in RJR Nabisco, Inc. vs. The European Community affirmed that the predicate acts may be committed outside the United States, although the plaintiff must still prove a domestic US injury in order to prevail on the RICO claim. While there is little case law yet, tying the DTSA to RICO may facilitate obtaining jurisdiction over non-US defendants who are not actually present in the US. Of course, non-US defendants with contacts in the US are likely already subject to personal jurisdiction in the US, as discussed above.

Europe:

On 8 June 2016, following a proposal from the European Commission, the European Parliament and the Council adopted a Directive that aims to standardise the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets. The EU Directive on Trade Secrets, which lays down common measures against the unlawful acquisition, use and disclosure of trade secrets, aims at ensuring the smooth functioning of the internal market.

It is also intended to have a deterrent effect against the illegal disclosure of trade secrets, without undermining fundamental rights and freedoms or the public interest, such as public safety, consumer protection, public health, environmental protection and mobility of workers. The EU Directive on Trade Secret defines a trade secret as information that:

- is secret
- has commercial value because it is secret
- has been subject to reasonable steps to keep it secret

What qualifies as a trade secret is very broad indeed. A trade secret can be a formula, practice, process, design, instrument, pattern, commercial method, or compilation of information which is not generally known or reasonably ascertainable by others, and by which a business can obtain an economic advantage over competitors or customers. The scope of trade secrets is virtually unlimited.

Nowadays there is great diversity of systems and definitions in EU member states as regards the treatment and the protection of trade secrets. The purpose of this new EU Directive on Trade Secrets is to bring legal clarity and a level playing field to all European companies. In accordance with the new legal framework, EU member states will have to provide for the measures, procedures and remedies necessary to ensure the availability of civil redress against the illegal acquisition, use and disclosure of trade secrets. These will have to be fair, effective and dissuasive. They must not be unnecessarily complicated or costly, nor may they entail unreasonable time limits or unwarranted delays. The limitation period for claims will not exceed six years.

Trade secret holders will be entitled to apply for remedies in case of damages following cases of illegal appropriation of documents, objects, materials, substances or electronic files containing a trade secret or from which a trade secret can be deduced. Where necessary, confidentiality of trade secrets will also be preserved during the course of and after the legal proceedings. After publication of the directive in the Official Journal of the EU and its entry into force, member states had a maximum of two years to incorporate the new provisions into domestic law.

EU countries were required to bring into force the laws and administrative provisions necessary to comply with the Directive by 9 June 2018. There is however no 'one size fits all' across the EU. It does not mean that we will have identical trade secret legislation across all EU member states as of June 2018. Firstly, as with any EU Directive, there will be differences in

interpretation from one member state to another as people draw upon their background and experiences to interpret information.

Secondly, the EU Directive on Trade Secrets merely sets a minimum standard for all EU member states to implement. There is nothing preventing any member state going beyond this minimum standard. A EU member state may for example cast an eye across the Atlantic to see what the US has enacted with their Defend Trade Secrets Act and determine to copy certain aspects of that powerful law.

Thirdly, this EU Directive only covers civil law, so it is therefore not excluded that member states will provide for additional sanctions to infringers in the field of criminal law. Some EU member states will definitely do so and provide such additional sanctions to infringers. What is 'reasonable' in terms of the reasonable steps to be taken to protect a trade secret may vary from one jurisdiction to another, at least in the short term as different courts go through a learning curve with respect to trade secrets cases.

As with any IP related legislation in the EU, the different levels of IP sophistication and maturity across EU member states should also be taken into account. One could also argue that the level of assistance and support from local white-collar crime fighting units when an organisation has had its trade secrets misappropriated will also differ from one EU member state to another. Organisations therefore need to appreciate that the EU Directive on Trade Secrets does not mean identical trade secret legislation across all EU member states.

It should also be noted that there are a number of important safeguards built into the EU Directive on Trade Secrets. Journalists will remain free to investigate and publish news on companies' practices and business affairs, as they are today. The EU Directive on Trade Secrets only deals with unlawful conduct by which someone acquires or discloses, without authorization and through illicit means, information with commercial value that companies treat as confidential in order to keep a competitive advantage over their competitors.

The EU Directive on Trade Secrets does not alter the current legal obligations on companies to divulge information for such public policy objectives. The public interest prevails over private interest in such matters. Companies are subject to legal obligations to disclose information of public interest, for example, in the chemical and pharmaceutical sectors. Such regulations, which ensure a high level of transparency, will not be affected. The EU Directive on Trade Secrets does not provide any grounds for companies to hide information that they are obliged to submit to regulatory authorities or to the public at large.

Moreover, the EU Directive on Trade Secrets does not alter and does not have any impact on the regulations that foresee the right of citizens to access documents in the possession of public authorities, including documents submitted by third parties such as companies and business organisations.

In addition, the EU Directive on Trade Secrets expressly safeguards those who, acting in the public interest, disclose a trade secret for the purpose of revealing a misconduct, wrongdoing

or illegal activity. This safeguard is operative if the trade secret was acquired or passed to the whistle-blower through the use of illicit means such as the breach of law or contract.

China:

China strengthened its trade secret laws with a revision of the Anti-Unfair Competition Law on 1 Jan 2018.

The key changes to the Chinese Law are as follows:

- The definition of a trade secret has been simplified to now be 'commercial secrets of sufficient commercial value' (and more in line with the definition of trade secrets in the US and in Europe)
- The fines have been increased from CNY 200,000 to CNY 3,000,000.
- The law has been expanded in that 3rd parties with actual or constructive knowledge of the theft of a trade secret could also now violate the law.

This revision of the Chinese Law is effective from 1 Jan 2018.

It should be noted that China's rules defining and regulating trade secrets are scattered among a series of laws and regulations. The most important of these however is the Anti-Unfair Competition Law.

Conclusions

In just over 24 months from mid-2016 to mid-2018, trade secrets laws have been strengthened considerably in three key jurisdictions - the USA, Europe and China. Trade secrets have been until recently the neglected step-child of IP. Trade secrets have tended to get overlooked in most IP training sessions. Some in-house IP managers have claimed that trade secret asset management were not part of their job spec. Many so called full service IP Firms have failed to even list trade secrets in their 'areas of expertise'. Some IP professionals have even claimed that trade secret were not 'real' IP because they are not a registered form of IP.

Those days are over. It is time to take trade secret asset management seriously.

Companies need to start taking action now so that they are much better prepared. I suggest that the following steps should at least be taken:

- A trade secret policy should be created.
- A top-level trade secret process should be defined
- A trade secret asset management system should be taken into use as technology can greatly help underpin the process.
- A trade secret educational program should be deployed within the organisation.
- An exercise should be conducted to attempt to gather information on the various trade secrets existing within the organisation

- A similar exercise should be conducted to identify any trade secrets belonging to 3rd parties but entrusted into the care of the company.
- A governance structure should be put in place.

This list is not exhaustive and other steps may also be required to be taken.
Are you ready? Is your company ready for this change? Let's conduct a simple test. Does this below describe your company and its approach to trade secrets and trade secret asset management?

- The company is not properly managing its trade secrets with no clear ownership of the trade secret management process or the secrets themselves.
- Documentation about the trade secrets is poor.
- Access to and access control around its trade secrets is very ad hoc.
- Protection mechanism deployed to safe guard its trade secrets is poor or non-existent.
- There is a lack of any classification of the trade secrets by the company.
- Details on whether trade secrets had already been shared with 3rd parties is often missing
- Information of any trade secrets belonging to 3rd parties but entrusted to the company is scarce.
- There is no audit trail.

If this describes your company, then perhaps some action is needed now.

Almost every organisation possesses trade secrets or rather information would could qualify as trade secrets. Trade secrets are among some of the most valuable assets an organisation possesses, so they need proper and professional management. Admittedly, trade secrets have been the neglected step-child of IP but that is changing.

Most organisations are still very poor at managing their trade secrets. Various reputable surveys, benchmark exercises and research projects have shown this to be the case.
Trade secret metadata is key. You can have data without information but you can't have information without data. At the very basic level, organisations need to have education about trade secrets; a policy and procedures about trade secrets; and some governance of their trade secrets.