Trade secrets have always been valuable, but the America Invents Act means they are now worth more than ever – potentially even more than patents. What is the best way to take advantage of this type of protection for your inventions – and what are the pitfalls?

By Bruce Story

Trade secret law, in its various versions around the world, has protected key business assets of companies for many years. One has only to think of the value of the Coca-Cola Company formula trade secret, which has been protected for many more years than patent protection would have allowed.

In the United States, trade secrets are protected by state law, with most states modelling their laws on the Uniform Trade Secret Act. This is distinct from patents, which are protected by federal law. However, the US government realised that trade secret theft benefiting foreign governments and companies should be treated as a federal crime. The US Economic Espionage Act of 1996 defines the term ‘economic espionage’ as the theft of a trade secret with the intent or knowledge that the offence will benefit a foreign government, foreign instrumentality or foreign agent. The act of receiving, purchasing or possessing a trade secret known to have been stolen or misappropriated, as well as any attempt or conspiracy to commit economic espionage, is punishable as a federal crime. Companies can bring such theft to the attention of the US Justice Department for help. Companies depend on the protection of trade secrets for some of their most valuable technology. Proprietary manufacturing processes, formulations and other technologies that are difficult to reverse engineer are typical subjects for trade secret protection. For the misappropriation of a trade secret to be enforceable, the company must derive economic value from it and take reasonable precautions to protect it. Many companies do treat trade secret theft seriously, as these recent cases demonstrate:

- A high-value case of trade secret theft has been playing out between DuPont and South Korean-based Kolon Industries. In September 2011 a court ruled that Kolon had stolen trade secrets for the production of Kevlar, DuPont’s aramid fibre. The verdict included an award of US$920 million. In August 2012 the district court ordered Kolon to return DuPont’s trade secrets and cease manufacturing and selling products made from them. In addition, in October 2012 it handed down a criminal indictment charging Kolon with theft of DuPont’s trade secrets, conspiracy and obstruction of justice. The indictment charges Kolon with engaging in a multi-year campaign to recruit DuPont employees to Kolon for the purpose of obtaining Kevlar-related trade secrets.

- In January 2012 a Sanofi chemist pleaded guilty to stealing trade secrets from the company on five developmental chemical compounds and offering them for sale. She had transferred the proprietary information to her home personal computer using her personal email address and a USB thumb drive. She was sentenced to 18 months in prison and to pay US$131,000 in restitution.

- In October 2010 a former chemist with DuPont was sentenced to 14 months in prison for stealing trade secrets from
DuPont concerning the manufacturing process for organic light-emitting diode displays. He had been planning to set up a factory for manufacturing these in China. DuPont’s quick action upon discovering the theft, and the involvement of federal officials, helped to prevent any significant loss to the company.

- In November 2010 a former engineer with Ford Motor Company pleaded guilty to federal charges of trade secret theft after taking design specifications for many automobile sub-systems. Most of the documents were downloaded to an external hard drive by the employee; many were subsequently found to have been loaded onto a laptop computer issued to him by a rival Chinese auto manufacturer. The stolen trade secrets were valued at up to US$100 million.

- In January 2012 a former Dow Chemical research scientist was sentenced to five years in prison for stealing manufacturing process trade secrets and selling them to Chinese companies. This manufacturing process was for making chlorinated polyethylene (CPE), which is used in the manufacture of vinyl siding, electrical cable jackets and industrial hoses. “Wen Chyu Liu, also known as David Liou, traveled extensively throughout China to market the stolen information, and evidence introduced at trial showed that he paid current and former Dow employees for Dow’s CPE-related material and information,” the US Justice Department said. Dow Chemical stated: “The technology that Mr Liou was convicted of stealing belonged to Dow. Because of his education and position within the company, Mr Liou knew of its immense value. This theft is a complete betrayal of the trust imparted to Mr Liou as a Dow employee.”

- In December 2011 a former Dow AgroSciences scientist was sentenced to several years in a federal prison after pleading guilty in two cases for stealing trade secrets from Dow and Cargill to benefit a Chinese university.

- An organic chemist who worked for Frontier Scientific was charged with stealing the manufacturing process for certain chemical compounds. He was accused of emailing the process to his brother-in-law, who was setting up a competing firm in India. Frontier’s CEO said that he thought his firm had sufficient security measures in place to safeguard its intellectual property from theft.

- In 2012 a former DuPont researcher pleaded guilty to conspiracy to commit economic espionage with regard to DuPont’s proprietary manufacturing process for titanium dioxide. Other former DuPont employees were allegedly involved. DuPont’s general counsel said that the firm was “disappointed that former DuPont employees working together with certain companies allegedly stole our proprietary technology”.

**Why trade secret theft?**

As can be seen from this list of thefts, most prosecuted cases are caused by an employee sending confidential information to outsiders so that they can build competing businesses or employees themselves leaving a company to set up a competing business. But who knows how much theft occurring through hacking into a company’s confidential files via the internet remains undiscovered?

The US Federal Bureau of Investigation (FBI) assistant director, counterintelligence division, testifying before Congress on 28th June 2012, said that the threat from company insiders is nothing new, but it is becoming more prevalent for various reasons, including:

- Widespread employee financial hardships during economic difficulties.
- The global economic crisis facing foreign nations, making it even more attractive, cost effective and worth the risk to steal technology rather than invest in R&D.
- The ease of stealing anything stored electronically, especially when one has legitimate access to it.
- The increasing exposure to foreign intelligence services presented by the
Secret strategies

show of bipartisan support in both houses of Congress is indicative of the widely perceived threat that trade secret theft poses to the United States’ economic future.

On 14th January 2013 President Obama signed the Foreign and Economic Espionage Penalty Enhancement Act of 2012. This raises the maximum fine for an individual found guilty of stealing trade secrets from US$500,000 to US$5 million. The maximum fine for a company increases from US$10 million to either US$10 million or three times the value of the stolen trade secret. This value includes the cost of R&D and other expenses that the defendant avoided through economic espionage. Also, the new act directs the US Sentencing Commission to review and increase the penalties “relating to the transmission or attempted transmission of a stolen trade secret outside of the United States” in order to “reflect the seriousness of these offenses, account for the potential and actual harm caused by these offenses, and provide adequate deterrence against such offenses.” House of Representatives Judiciary Chairman Lamar Smith stated: “The economic and national security of our country depends on the security of our information. Reports show that our economy loses billions of dollars every year because foreign spies steal our intellectual property and trade secrets.”

Trade secret protection begins with employees

Employees are usually the weakest link in trade secret protection. How can that link be strengthened? Best practices in industry focus on these basics:

• Good hiring procedures to weed out security risks consistent with the country, culture and local law.

• Employee contracts that clearly articulate the employee’s confidentiality responsibilities.

• Employee training on what is proprietary, confidential and a trade secret, instructions on how to protect this and the consequences to the company and the employee if misappropriated.

• Physical security — locked offices, fences, badge access, cameras, controlled access by the public.

• Computer security — controlled access to confidential information, need-to-know basis, passwords, monitoring employees access to confidential information and controlled documents, enterprise digital rights management, limited downloading capabilities of reality of global business, joint ventures and the growing international footprint of US firms.

Most of these recent cases demonstrate that the confidential information is stolen when an employee sends email with confidential attachments or downloads such information onto a laptop computer or thumb drive. One ex-employee was found to have thousands of confidential research reports downloaded onto his laptop when it was seized by police. Indeed, data indicates that 76% of all defendants charged under the Economic Espionage Act are insiders, 17% are outsiders and 7% have an unknown relationship with the trade secret owner.

Even with all the reported theft, federal law enforcement officials state that many US companies do too little to protect their interests, failing to monitor employees and rarely bringing problems to federal agents for fear of bad publicity. There must be many more instances of trade secret theft that are not reported to the authorities.

Increasing federal penalties for theft

The US Congress has noted that the penalty for trade secret theft that benefits foreign entities has been perceived as being too low and there are questions over whether it serves as a sufficient deterrent (see Figure 1). Because of the proliferation of such theft to the detriment of domestic businesses, the House of Representatives passed the Foreign and Economic Espionage Penalty Enhancement Act on 1st August 2012 by voice vote and the Senate passed it unanimously, with one amendment. The house agreed to the Senate’s amendment on 1st January 2013 and sent it to the president on 3rd January. This unusual
confidential information.

- Exit interviews with departing employees reminding them of their responsibilities to protect company confidential information.

Sometimes, companies will write a letter to the ex-employee’s new company to alert them to the employee’s access to certain trade secrets and other confidential information so that they will not put the employee in a compromising situation meantime, what changes in trade secret management might it require? What is certain is that good records will need to be made of the trade secret and when it was first commercially used, or at least when it can be proven to have been used commercially. Companies will need to record more details than a brief description if they hope to overcome future patent claims. For example, if the trade secret is a particular manufacturing process step, the ranges of process temperatures, pressures, dimensions and flows, among other details, will all need to be recorded. This record may need to be updated periodically as the process evolves or improvements are made.

Many companies have put off making inventories of their trade secrets for various reasons, including security, but the America Invents Act makes taking this seriously much more important when businesses and product lines are at risk. Proper consideration will need to be given to protecting these inventories of trade secrets from theft (e.g., enterprise digital rights management technology may help to protect inventories from easy downloading by unscrupulous employees or external hacking).

One caveat: in Congress’s wisdom, the prior user right is not available as defence to infringement of university patents. The ‘university exception’ states that “a person… may not assert a defense under this section if the claimed invention with respect to which the defense is asserted, was… owned or subject to an obligation of assignment to… a technology transfer organization whose primary purpose is to facilitate the commercialization of technologies developed by one or more such institutions of higher education”. This exception increases the value of patents owned or originally assigned

Trade secrets value inflated by the America Invents Act

In the past, US companies had the potential business risk, if operating under trade secret protection, that an independent inventor might invent and subsequently patent the subject of their trade secret. If the new patentee discovered that the first company was operating under a trade secret that was covered under the claims of their issued patent, the patentee could seek to enforce its patent. This caught a number of companies unawares.

There has been a popular misconception that the United States had a prior user right. However, the only earlier prior user defence allowed had been for business method patents, as authorised by the 1999 American Inventors Protection Act. Since the earliest days of US patent law, Congress has incentivised the fully enabled disclosure of inventions by awarding a limited-time monopoly on the patentable claims of the invention. However, the claims had to be fully described so that they could be used by the public after the patent expired. With the America Invents Act — which was signed into law by President Obama in September 2011 — Congress has incentivised keeping inventions secret through the new prior user rights defence (see Figure 2). This is a major change and reduces the business risk that a business operating under trade secret protection could be shut down or face paying a royalty for doing what it has been doing for years.

Overturning an infringement charge using a prior user rights defence is far from straightforward. The defendant must prove by “clear and convincing” evidence that he or she was commercially using the invention as detailed in the claims being enforced more than one year before the effective filing date of the patent; whereas the plaintiff need only show by a “preponderance” of the evidence that an infringement has occurred.

Only time and court decisions will tell how effective this defence can be. In the

Figure 3. Relative value increase for university patents

<table>
<thead>
<tr>
<th>Corporate patents</th>
<th>Individual patents</th>
<th>University patents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relative value before America Invents Act</td>
<td>Relative value after America Invents Act</td>
<td></td>
</tr>
</tbody>
</table>
Inventor training – include trade secret

Trade secrets include:

- A change in IP strategy to focus more on key management processes affected by manufacturing organisations and documenting their commercial use.
- IP review committee – educate the IP value metrics for your company’s trade secrets so you do for the patents protecting your products and manufacturing. This can demonstrate the value of the trade secrets to management and provide a rationale for improving the protection of trade secrets within the company.
- IP strategy process – for each new product development, create an IP strategy that considers the appropriate mix of trade secrets, patents and publications to support the business strategy.

Patent filing strategy – consider filing a provisional patent application on the trade secret, if it is perceived to be patentable. This gives you 12 months to sort out the competitive and business situations before either choosing to continue with patenting or keeping it as a trade secret.

Impact under the first inventor to file law

As Congress set about trying to reform and harmonise US patent law with the rest of the world, there was enough of a domestic lobby to keep the one-year grace period for publication by the inventor before the effective filing date. This enhances the potential risk of the invention becoming known to others who may file the patent application first. The America Invent Act makes it clear that the patent should go to the “first inventor to file”.

A new procedure has been created to correct inventorship if a person deriving the invention (substantially the same) from the true inventor files first. However, until this is tested in court, no one knows how well this will protect an inventor’s ownership of his invention after the fact. A burning question is what “substantially the same” actually means. If a third party can modify the invention slightly after becoming aware of the non-filed invention, will the derived procedure still protect the original inventor?

Courts will have to interpret this phrase in their judgments.

This potential risk of losing ownership of patentable claims necessitates a careful consideration of keeping the invention secret before filing the patent application. Inventions can be lost if:
- Company employees publish or speak publicly on the grace period and someone else files the patent application first.
- Company employees are overheard describing the invention in public (e.g. in a restaurant, elevator or aircraft).
- A co-inventor leaves the company and files first.
- Co-workers send information on the invention to others who may file first in other countries.
- The company fails to use or follow up on non-disclosure agreements when discussing the invention with third parties.
- The company is unaware of newly published patent applications (the America Invent Act allows up to one year following a patent application publication to bring a petition for a derived proceeding).

The following will all help to protect an invention:
- File the patent application quickly.
- Protect the invention as a trade secret before filing.
- Carefully decide whether publishing or speaking about the invention before filing is worth the risk.
- Invent around your invention and file as many improvements or variations as possible to pre-empt others.
- Utilise non-disclosure agreements before allowing third parties access to your invention.
- Document every access by third parties to your invention (record of transmittal of confidential information) – for instance, what, when and to whom.
- Use a current awareness patent application publication service to track related subject-matter patent applications.

Changes in best mode considerations

Before the America Invent Act, the best mode of enablement for the invention was required for patentability and any deficiency in this could be grounds for an inequitable conduct charge in litigation. The America Invent Act still requires the best mode for patentability, but releases this as a ground for inequitable conduct. Some applicants may use this new law as the basis to enable the invention minimally.

Key management processes affected by a change in IP strategy to focus more on trade secrets include:

- Inventor rewards and recognition – consider including inventors of trade secrets in your rewards and recognition programme, just as you would inventors of patents. This will encourage the documentation of technology that should be subject to the protection offered by trade secrets.
- Inventor training – include trade secret protection, strategy and documentation in inventor training programmes.
- Extraction and inventorying trade secrets – if you do not have a trade secret inventory, consider extracting the trade secrets from each relevant part of the company’s technology and manufacturing organisations and documenting their commercial use.
- IP review committee – educate the IP review committee on the increased value of trade secret protection and what the decision criteria should be.
Secret strategies

just enough for patentability, but keep the best mode as a trade secret. If you can spot this and invent on top of it, you may be able to force a cross-licence or other consideration from the patent owner. In the larger context, this demonstrates that the ultimate protection for an invention may include a mix of patents, trade secrets and judicious publication.

What is the impact on IP strategy?
Considering the new America Invents Act incentive for trade secrets and the enhanced penalties for theft, what will be the impact on IP strategy?

After moving away from the use of trade secrets and towards patenting after the establishment of the Court of Appeals for the Federal Circuit in 1983, IP strategists are recommending greater use of trade secrets, if applicable. This recommendation takes advantage of the longer protection trade secrets afford, if managed well, and the reduced business risk due to the new prior user rights defence from the America Invents Act. Although very recent, the new Foreign and Economic Espionage Enhanced Penalty Act of 2012 provides a greater deterrent for trade secret theft. The value of keeping your key technology secret from your competitors is great – they cannot invent around or on top of, or improve, what you have invented if they do not know about it.

When considering whether to file an invention as a patent application, one should always ask: “Can this invention be reverse engineered or otherwise revealed by an analysis of the product or service sold to the public?” If it cannot, then trade secret protection should be considered seriously. Another positive aspect to the use of trade secret protection is that it costs considerably less than filing a patent. In addition, if you instead opt to file a patent application and it is published, but not allowed, then your invention is left completely unprotected and your competition knows what you are doing.

Bruce Story is a senior adviser at ipCapital Group