Views on an evolving automotive industry

Using trade secrets to protect innovation

With the emergence of new technologies and innovation, such as connected autonomous vehicles and EVs, the use of trade secrets has grown in importance due to the immediacy of the protection trade secrets law offers offer and its ability to cover all types of information.

Where other intellectual property ("IP") rights require registration and lengthy application procedures, as long as the internal right policies are in place, trade secret protection can be invoked as and when needed and adapted as required. Trade secrets laws are therefore well suited to the protection of fast-paced innovation, and the information and data generated in this context. Indeed where other IP rights fail in enforcement terms, businesses can often fall back on trade secrets protection as a backstop.

It is now common for a small group of key employees to hold significant know-how extremely desirable to any competitor. Trade secrets provisions are also one of the main rights relied on to prevent dissemination of such know-how. Practical and technical restrictions should be put in place around how these sorts of employees can share key data and knowledge while in a business' employment, as well as restrictions around the use of such knowledge once the employee leaves the business.

In light of the increased prominence of trade secrets in the automotive industry, this article in our series "Views on an evolving automotive industry", provides an overview of key issues relating to the use of trade secrets to protect innovation, including setting out what constitutes a trade secret in the UK, Germany (EU), Australia and China, discussing employee risks, and advising on establishing a trade secrets protection strategy to reduce and police the risks of the loss of business critical know-how, and enforce rights in trade secrets.

What are "trade secrets"?

The reliance on trade secrets has in many cases arisen due to the difficulties in finding other IP rights that can protect business methods or AI-related innovations adequately in many jurisdictions.

Whilst it is generally the position that a trade secret is confidential information which arises in a commercial context, exactly what constitutes a 'trade secret' and the protection afforded to such varies across jurisdictions. This therefore means it is of utmost importance that automotive industry participants have an awareness of the differences across the jurisdictions in which they operate, rather than purely assuming a 'one size fits all' approach.

Click here for an overview of what a 'trade secret' is and the associated protection thereof in the UK, China, Australia, the US and Germany.

Trade secrets and employee risk

Against the backdrop of what a trade secret is in different jurisdictions and the protection afforded to such, the maintenance of confidentiality and ensuring that confidential information or trade secrets are not misused is critical.

Arguably, a key vulnerability in any IP strategy is the risk that a business's trade secrets are shared with and/or misused by others. Unfortunately such incidents are often instigated by employees.

The increased mobility of key employees with highly specialised knowledge and skills and their movement to a competitor has the potential to heighten this risk. Coupled with this, the increasing collaboration in the automotive industry is a recipe for the dissemination and potential unauthorised use of confidential information and trade secrets, unless strict controls are put in to place.

Although the automotive industry has a tradition of being non-litigious and one in which IP has been regularly cross-licensed, costly and time-consuming litigation over confidential information and trade secrets is ever increasing.

There are therefore practical steps organisations should take during the employee journey to mitigate against the risk of misuse of confidential information and trade secrets, or, in the worst case scenario, to put the organisation in the best position to take action in the event of misuse.

Recruitment and on-boarding

For new hires, employers should: (i) ensure appropriate provisions are in contracts of employment or contracts with freelancers or consultants (including considering whether there is a need for a separate confidentiality agreement); (ii) consider whether there is an appropriate definition of confidential information (albeit simply labelling information as "confidential" will not be sufficient to confer confidentiality, with how an organisation treats information in such documents being relevant to any later assessment of whether the information can properly be regarded as a trade secret or information); and (iii) provide training to new starters on, at a minimum, the type of information which the organisation considers is confidential and/or a trade secret and the restrictions on the access and use of such information.

In addition to steps to protect confidential information and trade secrets, when new hires arrive within any organisation, it is vital that they understand any restrictions upon them from using any information that they have acquired from previous roles with other businesses. They must be prevented from disclosing their previous organisation's trade secrets – otherwise the business which they join may find itself on the receiving end of an dispute. If a reasonable person in the position of such organisation ought to make enquiries but such organisation does not do so, then an obligation of confidentiality will likely arise (see, for example, the UK Court of Appeal decision in *Travel Counsellors v Trailfinders* [2021] EWCA Civ 38).

Employee risk in the automotive industry in China

In China many of the reported cases involving trade secret infringement in the automotive industry involve former employees who have, for instance, left big companies to become founders or key employees of EV manufacturers or auto driving tech companies (many of which are start-ups).

In a 2019 reported case, Geely commenced several law suits against WM Motor for trade secret infringements, claiming damages of around RMB 2.1 billion. WM Motor is a Shanghai-based EV start-up, and several of its senior officers previously held senior positions in Geely. Although Geely withdrew certain of the lawsuits, the dispute with WM Motor is reportedly still ongoing.

Similarly, in 2017, Baidu sued one of its former senior officers (who became a founder of an auto driving technology start-up, Jingchi) alleging trade secret infringement. Baidu ultimately withdrew the case without disclosing the reason.

During employment

It is critical that organisations put into place a trade secret policy and appropriate protocols to protect confidentiality. Just as important is implementing the policy and avoiding complacency in the workplace.

From a UK perspective under both the Trade Secret Regulations 2018 and common law confidential information and trade secrets are protected only as long as organisations take reasonable steps to keep the information confidential or secret. As a result, organisations should as best practice (i) mark documents with a confidentiality mark and ensure emails to which any such documents are attached are marked consistently; (ii) restrict circulation and/or access to confidential information and trade secrets (eg passwords); and (iii) consider whether confidential information and trade secrets can be isolated from other information.

Further, when considering any new substantial investment or collaboration with another business, appropriate contractual provisions must be put in place, particularly if there is likely to be cross-dissemination of information. Organisations should seek assurances that employees of the other business have been appropriately instructed that the information is considered confidential and/or a trade secret and must be treated appropriately to keep it secret.

Employee risk in the automotive industry in Germany

In Germany, with its high dependence on third parties as suppliers, the German automotive industry is particularly affected by the German Trade Secrets Act ("Trade Secrets Act"). Manufacturers often need to share their trade secrets with their suppliers and each trade secret is shared with a supplier the 'secret status' is put at risk dependent on the supplier's own trade secrets policy and standards of protection, no matter how strict the manufacturer's standards are.

In 2020, the Stuttgart Higher Regional Court (3 June 2020, OLG Stuttgart, Docket Number 2 U 575/19) denied protection pursuant to the Trade Secrets Act in a case where a company, a supplier to the automotive industry, allowed its employees to store confidential information on private data storages without password protection, stating that companies have to actively avoid third party access to information.

Departure of employees

When faced with the prospect of the departure of key employees, organisations should arrange for immediate IT access restrictions before employees exit the organisation. This is important not only for internal governance, but will be also of importance to investors or collaborators who view this as an important aspect of their decision to invest or collaborate.

Just as important is retrieving any confidential information or trade secrets in the possession of the employees. As such, when an employee departs, (i) organisations should have appropriate mechanisms to enable devices containing confidential information and trade secrets to be retrieved or wiped, even if employees are on garden leave or working remotely; (ii) any personal devices containing confidential information and trade secrets should be recovered, although care should be taken with personal information contained on the same device; (iii) departing employees should also be required pursuant to their employment contract to return any hard copy documents and provide necessary passwords for company IT equipment, and, ideally, warrant that all company property (including confidential information and trade secrets) is no longer in their possession; and (iv) some organisations may check whether any confidential information has been sent by the employee to their personal email just before they resigned or during their notice period, to identify any potential misuse of confidential information. Finally, organisations should remind departing employees of their obligations and any post-termination restrictions including regarding confidential information.

Employee risk in the automotive industry in Australia

In Australia, the courts have specifically recognised that former employees of automotive businesses who have obtained confidential information in the course of their employment - such as customer information, product development, financial performance, commonly-serviced vehicle models, and supply details - may be restrained from disclosing, misusing or benefitting from that information.

In *Freedom Motors Australia Pty Ltd v Vaupotic* ([2003] NSWSC 506) proceedings were bought against two former employees of a vehicle conversion business including in relation to alleged misuse of confidential information to set up a competing business. While the court refused to protect knowledge about vehicle conversion that it considered formed part of the ex-employees general stock of knowledge, it was satisfied that the use of customer information, product development, financial performance, commonly-serviced vehicle models and supply details, constituted use of information unknown to others in the trade which was confidential to Freedom Motors.

Other common risk areas for confidential information and trade secrets

- Contractors/freelancers
- Competitors
- Sharing/maintaining databases – data loss – GDPR compliance
- Cyber risk – hacking/data loss
- Disclosure of technology at trade/ industry events

Trade secret protection strategy

Considering the potential importance of trade secrets as a 'catch all' to protect innovation, particularly given the necessary acceleration in innovation and investment in R&D to realise the EV revolution and related EV targets, a sound trade secret protection strategy is vital. (For more on intellectual property strategies generally, see our previous briefing in our series: *Views on an evolving automotive industry: The importance of a clear IP strategy)*.

Not only will this strategy have to accommodate the cross section of legal regimes for trade secrets which will impact the relevant business, but the strategy will also have to have practical measures on the ground to ensure that the business and innovation qualify for protections from those legal regimes (eg that the relevant information is actually kept confidential).

A successful trade secret protection strategy can be broken down into five key areas below:

1. **Identify**: In order to fall within the scope of, and benefit from, the protection offered by the Trade Secrets Directive (as implemented in the UK and the EU) an organisation must identify information or data as a trade secret. In other jurisdictions the requirements vary but the principle of identification of valuable information and its treatment as confidential/secret is common to all systems.

   Trade secrets should be continuously identified with some form of (secure electronic) registry which has tight security controls, categorising information to identify and safeguard the business' most valuable information.

   The trade secret must be properly defined in any confidentiality agreement where contractual protection is sought.

2. **Protect and prevent**: A business should take 'reasonable steps' to protect its confidential information. It should have a process for ensuring that confidentiality agreements and policies are always in place with employees, contractors, suppliers and others. These processes should be in place at the outset and should limit disclosure of valuable trade secrets such that these are disclosed on a 'need to know' basis and within appropriate confidentiality arrangements.

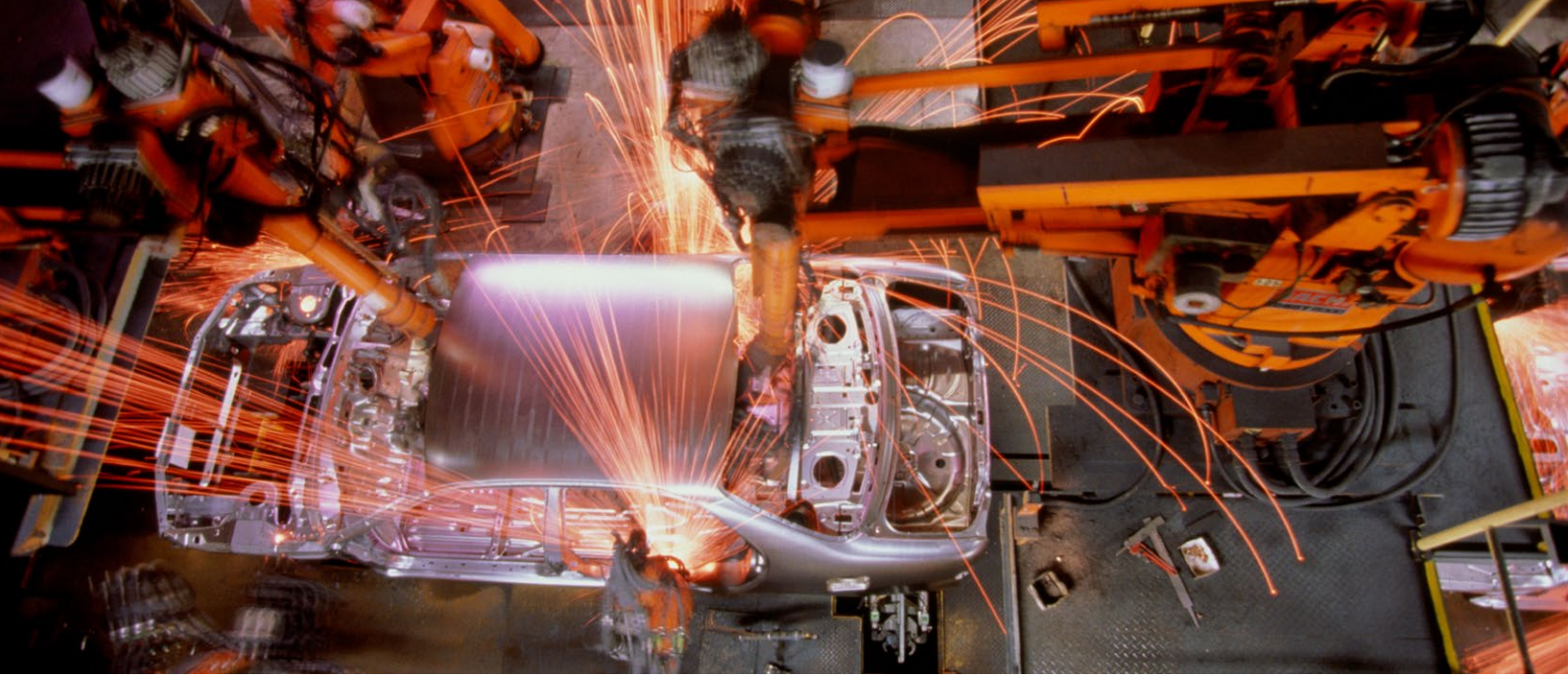
   Electronic controls include encryption and password controls, and physical controls such as document security are vital; labelling relevant information (in hard and soft copy) as confidential is a rudimentary and essential step. Employees (and any other party to whom disclosure is made) should be made aware of the trade secret status of particular information. The procedures put in place need to align with the level of perceived risk and value of the information concerned.

3. **Detect**: Being able to detect unauthorised use of trade secrets is vital and time is of the essence. In practice where trade secrets are important, businesses should be able to detect when sensitive information is copied or downloaded. This is not only key so that the business can limit onward disclosure of trade secrets but also from a reputational and liability point of view. Data loss protection software can be used to detect information loss as well as monitoring employee activity. Competitor activity can also be an indication of trade secret loss, especially when paired with employee movements.

4. **Assess & Contain**: Businesses need to assess any information "leak" and attempt to contain it. There is a need to balance the risks of trade secret loss against reputational damage that could ensue from taking enforcement action, however, swift and decisive action is mandatory if a business wants to consider applying for an interim injunction for example.

5. **Enforce**: The misuse of confidential information or a trade secret can be prevented by court proceedings.

   In the UK, for example, if you can demonstrate that: (i) the information had trade secret status; (ii) the access, use or disclosure of trade secrets was without consent, or via conduct contrary to honest commercial practices; and (iii) the information was acquired unlawfully or where the acquirer knew or ought to have known under the circumstances, this can lead to enforcement of trade secrets by the courts, usually in the form of an injunction but also in relation to any goods that significantly benefit from the trade secret's misappropriation.



Recent automotive industry dispute relating to trade secrets

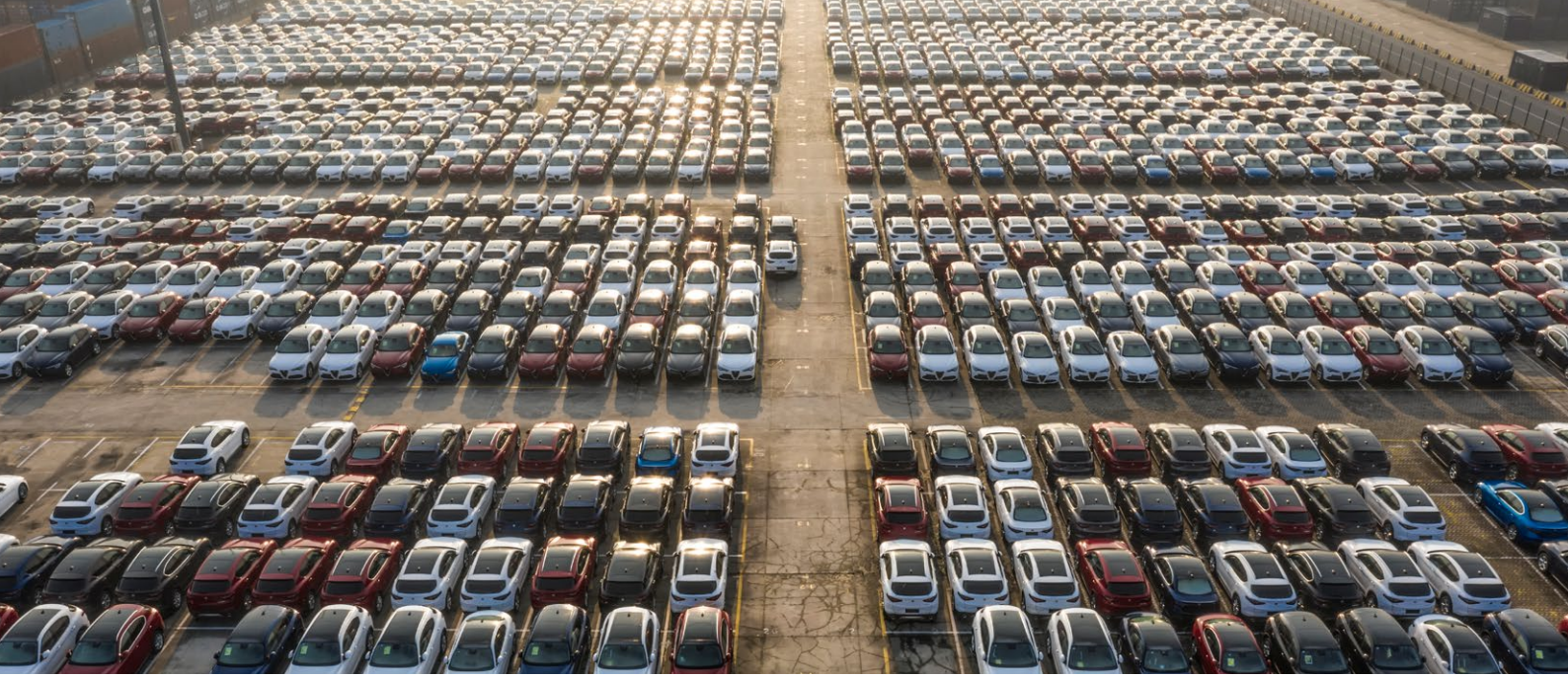
LG Chem ("LGC") complained to the US International Trade Commission ("ITC") that rival SK Innovation ("SKI") had misappropriated trade secrets from LGC related to EV battery technology. LGC claimed that SKI allegedly poached LGC employees to gain access to its rival's trade secrets for the development and production of batteries.

In early 2021, the ITC ruled for LGC determining that the appropriate remedy was a limited 10-year exclusion order prohibiting imports of SKI's lithium batteries into the US, although also holding that some components of the batteries may still be imported by SKI and that SKI was also allowed to replace batteries in certain vehicles sold to US customers; as well as cease and desist orders.

It was reported the decision could have been overturned by President Biden (who has publically supported the EV industry); however, on 11 April 2021 the parties announced a settlement of the matter, with SKI agreeing to pay 2 trillion won (c. $1.8 billion) for the alleged theft of IP. As a result, the ITC decision and the import restrictions on SKI in the USA were set aside. Both companies agreed to withdraw all pending legal disputes in the US and Korea and to refrain from suing each other for the next ten years.

In China, when pursuing an infringement case in the courts, you need to show that (i) the trade secret satisfies the statutory conditions; (ii) the counterparty possesses information that is the same or substantially the same as the trade secret; and (iii) the counterparty has used improper means to obtain the trade secret. If preliminary evidence is presented in the court proceedings to prove that confidential measures have been taken to protect the trade secret and that the trade secret has been infringed, the burden of proof shifts to the counterparty to show that its information is not the trade secret. If preliminary evidence can reasonably demonstrate that the trade secret has been infringed and one of the following exists, the onus will be on the counterparty to show that it has not infringed the trade secret: (i) the counterparty has channels or the opportunity to obtain the trade secret and the information it uses is essentially the same as the trade secret; (ii) there is evidence to show that the trade secret has been disclosed or used by the counterparty, or there is a risk of being disclosed or used; or (iii) there is other evidence of infringement of the trade secret by the counterparty.

In the US, the most significant recent development in the enforcement of trade secrets is the enactment of the Defend Trade Secrets Act of 2016 ("DTSA"). Among the many changes and expansions it contains, it provides Federal jurisdiction for theft of trade secrets, such that an owner of a misappropriated trade secret may initiate a private civil action in Federal court if the trade secret relates to a product or service used in, or intended for use in, interstate or foreign commerce.



The remedies available to the court in a civil action brought under the DTSA include if appropriate: (i) granting an injunction (including ex parte) to prevent any actual or threatened misappropriation and requiring affirmative steps be taken to protect the trade secret; and (ii) awarding damages for actual loss from the misappropriation and damages for unjust enrichment caused by the misappropriation (to extent) not factored in calculating damages for actual loss; or in lieu of damages measured by other methods, damages calculated by imposing liability for a reasonable royalty for the misappropriator's unauthorised disclosure or use of the trade secret. If the trade secret is wilfully and maliciously misappropriated, exemplary damages can be awarded.

The DTSA also amended 18 U.S. Code § 1832 to increase the maximum criminal penalty for an organisation for a violation of that section from $5,000,000 to "not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret to the organisation, including expenses for research and design and other costs of reproducing the trade secret that the organisation has thereby avoided . . . ."

The future for trade secrets

Trade secrets are increasingly being recognised by multiple major jurisdictions as an area where legislation needs tightening to protect both innovation and the reasonable and legitimate use of ideas and knowledge.

In introducing the DTSA the US has taken a landmark step forward in trade secret legislation, updating, strengthening, and broadening the law on behalf of trade secret owners.

The EU's approach, harmonising protection across its member states, has improved protection and in some instances introduced it, for trade secrets in an attempt to encourage inter-state R&D projects and the free flow of ideas across the trading block. By ensuring that trade secrets could be protected in court (which was not the case in each member state previously) this has also done a great deal to help businesses enforce their rights without losing confidentiality at the same time.

Traditionally, given the possibility of 'reverse engineering' traditional vehicle hardware, trade secrets have been seen as having had more limited effectiveness in relation to product design than the more traditional IP rights (such as patents and registered design rights) and have more often been used to protect manufacturing processes. Trade secrets now, however, look to be coming to the fore as a means of protecting fast moving innovations (including algorithms) and securing the know-how carried by specialist employees.

Another key aspect of the current pace (and cost) of innovation in the automotive industry is the necessity of collaborating with third parties in next generation design areas such as BEV platform architecture and EV batteries. This inevitably involves a sharing of existing know-how/trade secrets by both parties and the creation of new trade secrets (including data) and other IP rights as a result of the collaboration. The arrangements for the long term use and ownership of such rights need to be in place before the commercial relationship commences. It is this aspect that our next IP-focussed briefing, in our *Views on an emerging automotive industry* series will discuss.

If you have any questions, or would like to know how this might affect your business, please get in touch with any one of the following individuals.

London

Roddy Martin
Global Head of Automotive, Partner
T +44 20 7466 2255
roddy.martin@hsf.com

Jonathan Turnbull
Partner
T +44 20 7466 2174
jonathan.turnbull@hsf.com

Christine Young
Partner
T +44 20 7466 2845
christine.young@hsf.com

Rachel Montagnon
Consultant
T +44 20 7466 2217
rachel.montagnon@hsf.com

Jessica Welborn
Senior Associate
T +44 20 7466 2243
jessica.welborn@hsf.com

Sian McKinley
Senior Associate
T +44 20 7466 2996
sian.mcKinley@hsf.com

Germany

Ina vom Feld
Partner
T +49 211 975 59091
ina.vomfeld@hsf.com

Kevin Nebel
Associate
T +49 211 975 59142
kevin.nebel@hsf.com

China

Nanda Lau
Partner
T +86 21 23222117
nanda.lau@hsf.com

Peng Lei
Partner
T +86 21 2322 2113
peng.lei@hsf.com

Alizee Zheng
Senior Associate
T +86 21 23222117
alizee.zheng@hsf.com

Australia

Rebekah Gay
Partner and Joint Global Head of Intellectual Property
T +61 2 9225 5242
rebekah.gay@hsf.com

Emma Iles
Partner
T +61 3 9288 1625
emma.iles@hsf.com

New York

Lawrence Savell
Professional Support Lawyer
T +1 917 542 7816
lawrence.savell@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**