
CHAMBERS GLOBAL PRACTICE GUIDES

Trade Secrets 2023

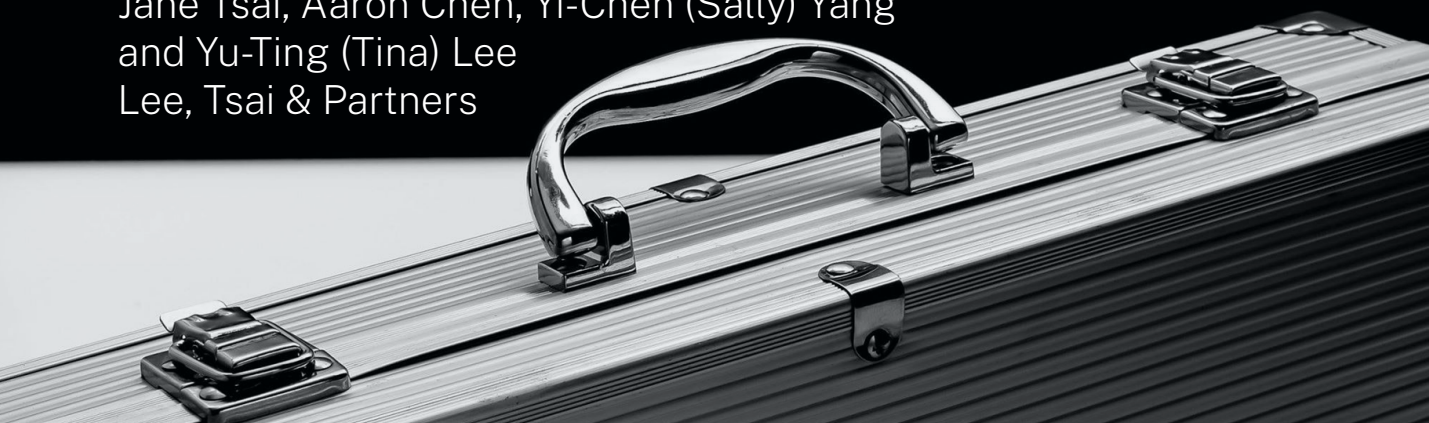
Definitive global law guides offering
comparative analysis from top-ranked lawyers

Taiwan: Law & Practice

Chung-Teh Lee, Sean Yu-Shao Liu, Jane Tsai and Pei-Ching Ji
Lee, Tsai & Partners

Taiwan: Trends & Developments

Jane Tsai, Aaron Chen, Yi-Chen (Sally) Yang
and Yu-Ting (Tina) Lee
Lee, Tsai & Partners



TAIWAN

Law and Practice

Contributed by:

Chung-Teh Lee, Sean Yu-Shao Liu, Jane Tsai and Pei-Ching Ji
Lee, Tsai & Partners



Contents

1. Legal Framework p.5

- 1.1 Sources of Legal Protection for Trade Secrets p.5
- 1.2 What Is Protectable as a Trade Secret p.6
- 1.3 Examples of Trade Secrets p.6
- 1.4 Elements of Trade Secret Protection p.6
- 1.5 Reasonable Measures p.6
- 1.6 Disclosure to Employees p.7
- 1.7 Independent Discovery p.7
- 1.8 Computer Software and Technology p.7
- 1.9 Duration of Protection for Trade Secrets p.7
- 1.10 Licensing p.8
- 1.11 What Differentiates Trade Secrets From Other IP Rights p.8
- 1.12 Overlapping IP Rights p.8
- 1.13 Other Legal Theories p.8
- 1.14 Criminal Liability p.8
- 1.15 Extraterritoriality p.9

2. Misappropriation of Trade Secrets p.9

- 2.1 The Definition of Misappropriation p.9
- 2.2 Employee Relationships p.9
- 2.3 Joint Ventures p.10
- 2.4 Industrial Espionage p.10

3. Preventing Trade Secret Misappropriation p.10

- 3.1 Best Practices for Safeguarding Trade Secrets p.10
- 3.2 Exit Interviews p.11

4. Safeguarding Against Allegations of Trade Secret Misappropriation p.11

- 4.1 Pre-existing Skills and Expertise p.11
- 4.2 New Employees p.12

5. Trade Secret Litigation p.12

- 5.1 Prerequisites to Filing a Lawsuit p.12
- 5.2 Limitations Period p.12
- 5.3 Initiating a Lawsuit p.12
- 5.4 Jurisdiction of the Courts p.12
- 5.5 Initial Pleading Standards p.12
- 5.6 Seizure Mechanisms p.12
- 5.7 Obtaining Information and Evidence p.13
- 5.8 Maintaining Secrecy While Litigating p.13
- 5.9 Defending Against Allegations of Misappropriation p.13
- 5.10 Dispositive Motions p.13
- 5.11 Cost of Litigation p.13

6. Trial p.14

- 6.1 Bench or Jury Trial p.14
- 6.2 Trial Process p.14
- 6.3 Use of Expert Witnesses p.14

7. Remedies p.14

- 7.1 Preliminary Injunctive Relief p.14
- 7.2 Measures of Damages p.15
- 7.3 Permanent Injunction p.15
- 7.4 Attorneys' Fees p.15
- 7.5 Costs p.15

8. Appeal p.16

- 8.1 Appellate Procedure p.16
- 8.2 Factual or Legal Review p.16

9. Criminal Offences p.16

- 9.1 Prosecution Process, Penalties and Defences p.16

10. Alternative Dispute Resolution (ADR) p.17

- 10.1 Dispute Resolution Mechanisms p.17

Lee, Tsai & Partners is a full-service boutique local firm servicing the Greater China region. The firm's headquarters are in Taipei, co-operating with a local partner law firm in Shanghai and a representative office of local IP consulting firm in Beijing. The firm's trade secrets law practice group includes former judges, a former prosecutor and experienced attorneys and is led by Dr Chung-Teh Lee. The firm has substantial experience representing companies in all instances of Taiwan courts and on landmark

cases. Lee, Tsai & Partners also regularly advises clients on the strategic planning and management of IP rights in relation to the high-tech industry, including obtaining patents and trademarks, IP licensing issues and litigation. The firm's client profile includes the largest online search engine providers, airlines, semiconductor manufacturers, telecommunications companies, pharmaceutical companies, infrastructure providers, banks, insurance companies, private equity funds and venture capitalists.

Authors



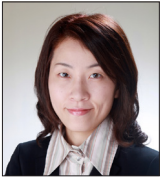
Chung-Teh Lee is a co-founder of Lee, Tsai & Partners, where he supervises the firm's trade secrets law practice. He specialises in dispute resolution, construction projects, cross-

border transactions and M&A. He is a former judge and was appointed by the Ministry of Transportation and Communication as a member of the Dispute Resolution Board for the Taiwan High-Speed Rail Project. He has acted as an arbitrator, legal representative and expert witness in a number of litigation matters.



Sean Yu-Shao Liu is a partner at Lee, Tsai & Partners and focuses his practice on trade secrets, fintech and commercial transactions. He has experience representing clients in

negotiations, settlements and disputes in both court and arbitration. With his in-depth knowledge of technology and business, Sean provides advice to major corporations on various legal matters including technology or commercial disputes, e-commerce, blockchain and digital assets, cyber and information security.



Jane Tsai is a partner at Lee, Tsai & Partners with over twenty years of experience. She specialises in intellectual property matters and is internationally recognised for her

expertise in trade marks, patents and trade secrets. She has a record of achieving success on behalf of her clients in complex intellectual property litigation in Taiwan. Ms Tsai further frequently assists her clients in intellectual property rights planning, including global trade mark strategic planning and internal trade secret protection mechanisms.



Pei-Ching Ji is a seasoned litigator with 15 years of experience representing clients in complex disputes at all levels of courts, government dispute resolution proceedings, and

international and domestic arbitrations. She is experienced in defending clients in criminal allegations. Ms Ji has obtained decisions to not prosecute for her clients on numerous occasions, including defending a representative of a domestic video game company in an insider trading case, and defending representatives of a domestic systems technology company in a criminal violation of the Government Procurement Act action and a breach of trust criminal action.

Lee, Tsai & Partners

9F, 218 Tun Hwa S. Road
Sec. 2, Taipei
106033
Taiwan

Tel: +886 2 23785780
Fax: +886 2 23785781
Email: lawtec@leetsai.com
Web: www.leetsai.com



A GREATER CHINA LOCAL FIRM

1. Legal Framework

1.1 Sources of Legal Protection for Trade Secrets

The Trade Secrets Act (TSA) is the primary legal framework for protecting trade secrets in Taiwan. It offers civil remedies to trade secret owners to safeguard their trade secrets and seek damages, as well as criminal penalties for anyone who illegally exploits others' trade secrets for their own gain.

Under the TSA, the court need not consider tort liabilities under the Civil Code if the information constitutes a trade secret. Additionally, Article 317 of the Penal Code penalises those who disclose industrial or commercial secrets and violate their legal or contractual obligations, with less stringent requirements on reasonable measures. Therefore, if proprietary information does not meet the criteria for a trade secret under the TSA, it may still qualify as "industrial or commercial secrets" under the Penal Code.

Apart from the TSA and the Penal Code, the Intellectual Property Case Adjudication Act (the “IPCAA”) provides procedural guidance on litigating disputes involving trade secrets and other intellectual property. It takes precedence over general procedures.

1.2 What Is Protectable as a Trade Secret

The TSA is quite comprehensive in terms of the types of information that may be recognised as trade secrets. It includes any method, technique, process, formula, program, design, or any other information that may be used during production, sale or operation, provided it meets the requirements of secrecy, economic value and reasonable measures.

1.3 Examples of Trade Secrets

As stated above, trade secrets set out in the TSA include any method, technique, process, formula, program, design, or any other information that may be used during production, sale or operation. Examples of trade secrets recognised by court precedents include, but are not limited to, food formulas, equipment designs, customer databases, experiment data, circuit diagrams and price quotes.

1.4 Elements of Trade Secret Protection

The following are the details of the elements required for trade secret protection under the TSA.

- **Secrecy** – the information must not be generally known to those who deal with similar information. Unlike the “novelty” requirement under patent law, secrecy under the TSA only requires minimal novelty and need not be of utility. Additionally, combinations of different prior arts cannot be used to deny secrecy.

- **Economic value** – the information must have substantial or potential economic value, and that value is due to its secrecy.
- **Reasonable measures** – the owner must have taken reasonable measures to maintain the information’s secrecy. Please refer to **1.5 Reasonable Measures** for more information.

1.5 Reasonable Measures

Under the TSA, one of the requirements for claiming trade secret protection is that the owner must have taken reasonable measures to keep the information confidential. The owner must strike a balance between protection and efficiency as trade secrets are used to generate economic value.

The TSA does not require the measure to be perfect or bulletproof. It would be considered “reasonable” if the measure can generally prevent unnecessary access to the information and demonstrate the owner’s intention to protect it.

The determination of whether the measures taken were reasonable is based on the specific circumstances of each case. Some factors that courts may consider include:

- owner’s manpower and financial capability;
- currently available techniques;
- access control on a need-to-know basis;
- non-disclosure agreements (NDAs) with employees and contractors;
- company policy for protecting confidential information; and
- physical or digital restrictions for protecting confidential information.

For example, if a company stores its trade secrets in a password-protected folder that only employees with related duties have access to, then it is more likely that the company has taken

reasonable measures. In contrast, if anyone in the organisation can access the folder, then it would be hard to argue that the owner intends to protect the information and has taken reasonable measures.

Overall, while it is not necessary to mark each trade secret as confidential, the owner must have related measures in place to convey their intention to protect the information. This can include a restricted scope of the folder, management of access rights, company policy, non-disclosure agreements and more.

1.6 Disclosure to Employees

Disclosure of a trade secret to employees does not necessarily compromise its protection, as long as certain conditions are satisfied, and appropriate measures are in place to maintain the information's confidentiality. When disclosing trade secrets to employees, it is crucial to ensure the following:

- share the trade secret only when it is essential for employees to perform their job duties;
- employees who receive the trade secret should be subject to the company's policies and procedures that safeguard the information's secrecy;
- require employees to sign confidentiality agreements or non-disclosure agreements;
- educate employees on the importance of trade secret protection; and
- label documents, files or other materials containing trade secrets as "confidential" or "proprietary".

1.7 Independent Discovery

Independent discovery or reverse engineering does not necessarily exclude trade secret protection. A 2021 judgment by the Supreme Court explicitly stated that reverse engineering is not

inherently an "illegitimate method of acquiring trade secrets", and that information resulting from reverse engineering may be protected as a trade secret if no illegal activity is involved.

On the other hand, if reverse engineering includes stealing a competitor's prototype or any other illegal activity, the information obtained would not qualify as a trade secret and the individual who participates in such illegal activity may infringe on someone else's trade secrets.

Although the judgment is not binding on other courts, it is highly persuasive and could impact the positions of lower courts on this issue.

1.8 Computer Software and Technology

In Taiwan, if a trade secret is designated as a "National Core Key Technology", violating it can result in a more severe penalty under the recently revised National Security Act. Please see **2.4 Industrial Espionage**.

1.9 Duration of Protection for Trade Secrets

The legal protection of trade secrets can endure indefinitely, provided that the conditions of secrecy, economic value and reasonable measures are met. However, accidental disclosure can lead to a trade secret losing its protection if it fails to meet the legal requirements.

Nonetheless, controlled disclosure in fulfilling employment duties or business co-operation operations will likely satisfy the legal requirements if reasonable measures are implemented. Reasonable measures may include having recipients sign a non-disclosure agreement, classifying and marking information as confidential and implementing access control through information systems, among others.

1.10 Licensing

The owner of a trade secret is entitled to license it to others and the licensing scope, such as territory, period, content and method, can be agreed upon in a contract. As licensing may introduce the risk of disclosing or misusing the trade secret, trade secret owners should take the following precautions when granting licences:

- include confidentiality clauses that bind the licensee to protect the trade secret;
- grant the licence on a need-to-know basis, allowing access only to individuals who require the information for licensed use;
- the licensee must maintain appropriate security measures; and
- the trade secret owner has the right to monitor the licensee's use of the trade secret and conduct periodic audits to ensure compliance.

1.11 What Differentiates Trade Secrets From Other IP Rights

Trade secret protection differs from other types of intellectual property protection in several ways.

- Trade secrets can be protected by law even without registration with the authorities, unlike patents and trademarks.
- The protection is granted as long as the trade secret satisfies the criteria of secrecy, economic value and reasonable measures. This differs from patents, which have a limited term of protection.
- Copyrights, on the other hand, differ from trade secrets in that they only protect specific expressions, not ideas or methods. Furthermore, if an idea is already known to individuals within the same field, a different expression of that idea is not protected under trade secret law.

- The enforcement of trade secrets and copyright usually involves criminal prosecution, while the protection of patents is generally pursued through civil litigation.

1.12 Overlapping IP Rights

The law in Taiwan allows trade secret owners to assert their rights in conjunction with other types of intellectual property rights. For instance, if an offender steals and reproduces a formula that is protected as a trade secret and also expressed in an original document, the owner can assert their rights under both the Trade Secret Act and the Copyright Act.

1.13 Other Legal Theories

Claims under the TSA, contract and tort within the Civil Code can be pursued concurrently. This approach is particularly prevalent in cases where employees misappropriate their employer's trade secrets.

However, the TSA often provides superior protection for trade secret owners, as it allows them to seek damages based on the offender's income or profit derived from the misappropriation. This advantage eliminates the need to prove the owner's actual damages. Consequently, unless the information in dispute does not qualify as a trade secret, plaintiffs are more likely to prioritise the TSA when initiating legal action.

1.14 Criminal Liability

Criminal penalties will be imposed on the offenders if they intend to obtain illegal benefits for themselves or third parties or to impair the trade secret owner's interest and conduct one of the following acts:

- acquiring a trade secret by theft, embezzlement, fraud, threat, unauthorised reproduc-

- tion, or other wrongful means, or using or disclosing a trade secret so acquired;
- unauthorised reproduction, usage or disclosure of a trade secret that the offender has known or possessed;
- failing to delete or destroy a trade secret that the offender has possessed as the trade secret holder so orders, or disguising it instead; or
- acquiring, using, or disclosing a trade secret that the offender knows is known or possessed by a third party due to any of the above-mentioned violations.

Simultaneous pursuit of criminal and civil claims is allowed for trade secret owners in Taiwan, and both claims do not interfere with each other. However, it is common for civil claims to be filed after the offender has been prosecuted, as it can help save litigation fees by filing the civil claim with the criminal court.

1.15 Extraterritoriality

Criminal liability

In the case of acts violating trade secrets, the place of the act or the place where the consequences occur must be within Taiwan for the TSA to apply. Notably, if an offender misappropriates trade secrets with the intention to use the same in a foreign country, the complaint of the owner is not required for criminal prosecution and the penalties will be more severe.

Civil liability

Where the misappropriation happens in a foreign country, the owner of trade secrets may still bring a civil lawsuit in Taiwan, provided that the offender is Taiwanese or has a residence in Taiwan. Nonetheless, if the offender is a foreigner with no residence in Taiwan, the Taiwan court would not have jurisdiction over the dispute outside of Taiwan. That being said, whether the mis-

appropriation happens in Taiwan may be interpreted broadly. For example, if a hacker outside of Taiwan remotely hacks into a server located in Taiwan, the misappropriation will most likely be deemed as happening in Taiwan.

In any case, obtaining testimonies from witnesses and gathering evidence in a foreign country may present additional challenges due to the international context.

2. Misappropriation of Trade Secrets

2.1 The Definition of Misappropriation

The trade secret owner does not always need to demonstrate that the defendant actually used the trade secret. Providing evidence that the defendant obtained unauthorized access or acquired the trade secret without permission could be enough to constitute a violation of the TSA. Nonetheless, showing that the trade secret was indeed used may bolster the owner's claim and potentially increase the damages awarded. For details, please refer to **1.14 Criminal Liability**.

A provision in the IPCAA recognises that misappropriation of trade secrets is often done covertly, and it can be challenging for victims to prove. In order to help ease this burden, the provision states that the burden of proof can shift to the defendant if the trade secret owner presents prima facie evidence indicating that the trade secret has been misappropriated.

2.2 Employee Relationships

In cases where an employee engages in trade secret misappropriation, the employer may likely pursue claims under the TSA, the employment

agreement and the Civil Code, potentially resulting in a stronger case against the employee.

Typically, employment agreements include a confidentiality clause obligating the employee to protect “confidential information”. The scope of this information is often broader than the definition of “trade secret” under the TSA. Additionally, if present, the non-compete and punitive damages clauses within the employment agreement can offer the employer further advantages and play a crucial role in litigation.

2.3 Joint Ventures

Trade secret misappropriation disputes have often arisen in the context of joint ventures, collaborations between companies, OEM partnerships and other similar arrangements. To mitigate risks during these transactions, the following terms are crucial:

- clearly identify trade secret documents and files, the ownership and permitted use of trade secrets contributed by each party;
- enter into non-disclosure agreements or have a confidentiality clause in place;
- mandate that all parties involved implement reasonable measures to safeguard confidential information; and
- return or destroy the confidential materials upon the termination of the joint venture.

2.4 Industrial Espionage

Industrial espionage usually constitutes a violation of the TSA.

Furthermore, under the recently amended National Security Act, if the offender misappropriates trade secrets for an entity connected to a foreign country, Mainland China, Hong Kong, Macau or foreign hostile forces, and the misappropriated trade secret involves “national core

key technologies”, the penalties imposed may be significantly more severe.

The National Science and Technology Council is responsible for reviewing and determining the scope of “national core key technologies”. Relevant regulations are currently under discussion and will be finalised in the near future.

3. Preventing Trade Secret Misappropriation

3.1 Best Practices for Safeguarding Trade Secrets

While the primary goal of protecting trade secrets is to ensure their security, their ultimate purpose is to generate revenue. As such, the safeguarding and utilisation of trade secrets may present conflicting objectives, requiring the owner to find a balance between efficient use and adequate protection. The ideal approach is not necessarily the most secure measure, but rather one that achieves an optimal equilibrium between these two aspects.

The court precedents in Taiwan suggest that whether measures safeguarding trade secrets are reasonable shall take account of the following factors: the owner’s manpower, financial capability, currently available techniques, and differentiating access in accordance with different duty requirements.

With the above in mind, the common practices for protecting trade secrets include the following:

- identification of confidential information;
- setting up company policy protecting confidential information;

- have employees and business partners execute NDAs and confidentiality agreements;
- limit access to confidential information on a need-to-know basis;
- implement physical and digital security measures of access control, such as firewalls, encryption, password, prohibition of USB devices, etc; and
- periodical audit and monitoring security measures.

In certain industries or situations, additional or specialised measures might be necessary. For example:

- for computer software, implement an information security system with access controls, use encryption techniques and conduct vulnerability tests regularly; and
- for chemical formulas, secure laboratories access and use a “need-to-know” policy when sharing information about specific formulas or processes.

3.2 Exit Interviews

According to the TSA, the employment contract, the company policies, etc, the departing employees must not take away or disclose the trade secrets of the current employer. It is standard to remind the departing employee of his/her legal obligations above.

The exit interview is common practice in Taiwan and typically includes the following steps:

- remind the employee of their obligation to protect the employer’s confidential information;
- ask for written assurance for not violating the employer’s policy protecting confidential information;

- return the employer’s property and documents, or destroy the same on the employer’s instruction; and
- enquire about the employee’s new position to ensure no violation of the non-compete clause, if any.

While the measures mentioned above are common during an exit process, departing employees are not required to make commitments beyond what the law or existing contracts mandate. For instance, employees may decline to agree to a new non-compete clause. Although employers can inquire about the nature of the employee’s new position, the employee is under no obligation to provide any information in response.

4. Safeguarding Against Allegations of Trade Secret Misappropriation

4.1 Pre-existing Skills and Expertise

A distinction exists between general knowledge or skills and trade secrets, as the former is typically known by individuals in the relevant industry, while the latter is not.

In Taiwan’s court precedents, the “inevitable disclosure” doctrine, which is recognised under US law, can be considered if a plaintiff seeks to enjoin a defendant from working for a new company. However, convincing the court to adopt this doctrine can be difficult, as the plaintiff must provide evidence to support all relevant factors, such as the similarity of the old and new positions of the employee, the inevitability of using the plaintiff’s trade secrets in the new position, the lack of good faith on the employee’s part, and so on.

4.2 New Employees

When onboarding a new employee, employers can take several steps to minimise the risk of trade secret misappropriation:

- conduct a background check to make sure the employee did not breach non-compete, non-disclosure or other agreements with their former employer;
- request that the new employee provide a written assurance that they will not bring any trade secrets or confidential information belonging to third parties into the new company;
- segregate the employee's training and restrict his or her access to confidential information until they fully understand their confidentiality obligations; and
- ask the employee to maintain journals on their research progress in the new company. This can provide evidence, if necessary, that the work is original and not taken from any third party.

5. Trade Secret Litigation

5.1 Prerequisites to Filing a Lawsuit

Initiating a civil lawsuit based on trade secrets in Taiwan is similar to filing any other civil lawsuit. However, starting from 30 August 2023, retaining an attorney is mandatory under the newly amended IPCAA.

5.2 Limitations Period

The time limit for bringing a trade secret claim is identical to that for tort claims, which is either two years from the date when the injured party/trade secret owner became aware of the injury and the party responsible for compensation, or ten years from the date of the tortious act.

5.3 Initiating a Lawsuit

Starting from 30 August 2023, when the newly amended IPCAA becomes effective, it will be mandatory for parties involved in a trade secret lawsuit to be represented by a lawyer. In order to initiate a trade secret lawsuit, the trade secret owner must file a written complaint with the court, similar to other civil lawsuits, with the assistance of a qualified attorney.

5.4 Jurisdiction of the Courts

After the newly amended IPCAA becomes effective on 30 August 2023, trade secret claims must be filed with the Intellectual Property and Commercial Court, a specialised court for trade secret and other intellectual property disputes.

5.5 Initial Pleading Standards

The submission of concrete or hard evidence of misappropriation is not mandatory for a civil complaint to be valid. However, during the legal procedures, the plaintiff is responsible for providing sufficient evidence to prevail in the case.

Under the IPCAA, if the trade secret owner establishes a prima facie case for misappropriation, the burden of proof will shift to the defendant, and the court will require the defendant to present concrete evidence and facts to support their denial of misappropriation. If the defendant fails to do so, the court may consider this as evidence and accept the owner's claim as true.

5.6 Seizure Mechanisms

The court may grant an ex parte motion to seize or preserve accused products or other evidence if (i) the evidence is likely to be destroyed or become difficult to present in court, or (ii) there is a legal interest that requires ascertaining the status quo of a fact or object.

The motion must be filed with the court where the relevant lawsuit is pending or, if no lawsuit has been initiated, the court with jurisdiction over the evidence. In addition to the above requirements, the court may also request that the applicant provide prima facie evidence of the validity of its trade secret and explain why the trade secret has been misappropriated.

The motion to perpetuate evidence may be made before the court concludes the trial procedures, but the court may reject the application if it is not made in a timely manner to avoid procedural delays.

5.7 Obtaining Information and Evidence

In a lawsuit, a party may request that the court order another party or a third party to submit relevant documentary evidence in their possession, provided that the evidence is likely to prove important facts and the party in possession of the evidence is obligated to make the submission. The obligation to submit evidence may arise if, for example, the evidence has been cited by the other party, is relevant to the applicant's interest, constitutes commercial books or records, or is made in relation to the dispute at hand.

When deciding whether to grant the order, the court will also take into account whether the evidence contains confidential or private information, and whether the submission of such evidence may cause substantial damage to the party in possession of it.

5.8 Maintaining Secrecy While Litigating

Under the IPCAA, either party has the right to request that the court issue an order to preserve the confidentiality of information and prevent the other party and related individuals from using the information for any purpose other than the

lawsuit. The information covered by the order will be kept in a separate dossier in the court and maintained in secrecy from third parties.

5.9 Defending Against Allegations of Misappropriation

Defendants in trade secret litigation often contest that the information claimed by the plaintiff does not meet the necessary requirements for trade secret protection, such as secrecy, reasonable measures and economic value. Additionally, defendants may argue that the information they possess is different from the plaintiff's information.

It is also common for defendants to resist allowing plaintiffs to examine seized documents by claiming that such documents contain confidential information that is irrelevant to the lawsuit.

5.10 Dispositive Motions

If the complaint fails to meet the required formalities, or if it is based on malice, unjust purposes or gross negligence without any legal or factual basis, the defendant has the right to request that the court dismiss the suit before the trial begins. However, there is no mechanism similar to summary judgment under US law in Taiwan.

5.11 Cost of Litigation

When initiating a lawsuit in the district court, the plaintiff is required to pay a fee which is approximately 1.1% of the damages sought. If the plaintiff appeals to a higher instance, the fee increases to around 1.65%. Ultimately, the losing party will be responsible for paying some or all of the court fees, depending on the outcome of the case.

In addition to the court fee, a foreign company without a registered branch or assets in Taiwan may also be required to provide a bond to

cover the defendant's potential court fees in the appeals process.

Contingency fee litigation for civil claims is permitted in Taiwan, as long as the compensation is not based on the damages awarded. For instance, the fee could be a fixed amount rather than a percentage of the damages awarded by the court.

6. Trial

6.1 Bench or Jury Trial

In Taiwan, trade secret cases are adjudicated by professional judges and there is no involvement of a jury.

6.2 Trial Process

Trade secret trials in Taiwan can last for approximately nine to 18 months, or even longer if the case is complex or involves a significant amount of documentation.

During the early stages of the trial, the court may clarify points that are undisputed and disputed, arrange for parties to examine files, and discuss evidence to be investigated.

Afterwards, the court will summon witnesses and investigate other evidence before concluding the trial procedures and rendering a judgment.

Throughout the process, both parties will have the opportunity to present their opinions on each step and provide a general summary of their arguments before the trial procedures come to a close.

6.3 Use of Expert Witnesses

Once the amended IPCAA comes into effect on 30 August 2023, expert witnesses will be permitted in trade secret trials in Taiwan. With the court's permission, each party will be allowed to present its own expert witness to assist the court in understanding relevant facts, evidence, and empirical rules in professional areas, such as finance, accounting, corporate governance, science and technology.

The expert witness must submit their written opinion initially and then respond in writing to questions raised by the other party's expert witness. If subpoenaed, the expert witness will present their opinion and answer questions from the parties and judges in the court.

There is no limit on the compensation for an expert witness, but such information will be disclosed and contained in their written opinion.

7. Remedies

7.1 Preliminary Injunctive Relief

In order for the court to grant a preliminary injunction, such as prohibiting the respondent from selling an accused product or working for a competing company, the applicant must provide prima facie evidence that:

- the preliminary injunction can prevent substantial damage or imminent danger;
- the trade secret in question is valid;
- there is a fact of infringement;
- the interest of the applicant in obtaining the order is greater than the impact on the respondent;
- the impact on public interest; and
- the likelihood of prevailing in the relevant lawsuit.

The duration of the preliminary injunction is generally the period of the relevant lawsuit. The bond amount will be decided on a case-by-case basis, primarily based on the potential damage that the respondent would suffer due to the preliminary injunction.

7.2 Measures of Damages

In a trade secret dispute, the plaintiff may seek damages through one of the following methods:

- compensation for the actual damages and lost profits suffered by the plaintiff as a result of the trade secret misappropriation; or
- the income obtained by the defendant as a result of the misappropriation of the trade secret, or the profit derived from such income if the cost can be proven.

If the misappropriation of the trade secret was intentional, the court may award the plaintiff damages up to three times the actual damages suffered. In practice, the key to recovering damages is to establish a causal link between the misappropriation of the trade secret and the plaintiff's damages/lost profits or the defendant's income.

7.3 Permanent Injunction

Under the TSA, the owner of a trade secret is entitled to claim for the removal of any infringement of the trade secret or prevention of any probable infringement. In addition, the owner may request that the object produced from the infringement and the object that is exclusively for the purpose of infringement be destroyed or disposed otherwise.

For example, a trade secret owner may seek a permanent injunction on a particular product and initiate enforcement proceedings to enforce a recall of the product.

Additionally, the TSA can be used as a basis for enjoining an employee's subsequent employment with a competitor. However, the duration of such an injunction may be limited and difficult to obtain without a non-compete clause in the employment agreement.

7.4 Attorneys' Fees

The plaintiff may only recover their attorneys' fees in certain circumstances.

- If the parties agree in advance in the relevant agreement (such as an employment or co-operation agreement) that attorneys' fees will be included in the damages.
- If the law requires an attorney for the litigation.

Once the newly amended IPCAA takes effect on 30 August 2023, all trade secret lawsuits will require an attorney by law, allowing the plaintiff to recover their attorney's fees. However, the amount of the attorney's fee will be subject to a statutory limitation that will be announced later. If the fee exceeds the limit, the plaintiff may not be able to recover the entire amount.

7.5 Costs

In Taiwan, the litigation fee will be borne by the losing party or by both of the parties proportionally, depending on how the case is finally decided.

The litigation fee includes the court fees for initiating a lawsuit or appeal, attorney fees if the attorney is required by law, and fees paid to the court-appointed experts. However, the litigation fees do not cover expenses such as transportation, phone calls, fax, printing, travel expenses or taxes.

8. Appeal

8.1 Appellate Procedure

An aggrieved party may file an appeal within 20 days after receiving the written judgment if they lose in the first instance of litigation.

If the order of the court is not a judgment, it is usually appealable within ten days unless the law specifically states otherwise. Procedural orders are generally not appealable unless they have a significant impact on the parties' procedural interests. For instance, an order denying the party's request to examine court files is procedural but appealable.

The appeal process for an order typically lasts a few months, whereas the appeal on a judgment (ie, the second and third instance) would take more than a year.

8.2 Factual or Legal Review

In Taiwan, the court of the second instance reviews both legal and factual issues and holds live arguments similar to the court of the first instance. However, the court of the third instance, which is the Supreme Court, only reviews legal issues.

The court of the second instance generally does not repeat the factual investigation conducted in the first instance, such as subpoenaing the same witnesses. Moreover, parties are usually not permitted to raise new arguments in the second instance unless, for example, relevant facts emerge after the first instance or the party was unable to present the argument in the first instance.

9. Criminal Offences

9.1 Prosecution Process, Penalties and Defences

According to the TSA, anyone who violates someone else's trade secrets may face criminal penalties, including up to five years of imprisonment (or one to ten years if committed for extraterritorial use) and a fine ranging from TWD1 million to TWD10 million (or TWD3 million to TWD50 million if committed for extraterritorial use). If the interest from the offense is higher than the statutory maximum, the fine can be increased. Moreover, violating trade secrets that have been recognised as "national core key Technology" will be imposed with much more severe penalties, as stated in [2.4 Industrial Espionage](#).

An owner of misappropriated trade secrets can file a criminal complaint with either the criminal court or the prosecutor's office. However, in practice, owners rarely choose to file directly with the criminal court because it is difficult to obtain evidence of misappropriation without the assistance of a prosecutor. If the prosecutor's investigation reveals that the defendant likely violated the TSA, the prosecutor will file the criminal complaint with the court, and the owner may retain an attorney to present their interest in court.

It is essential to work with experienced lawyers when dealing with the prosecutor's office to present important evidence, explain technical information and fill out special forms to support the legal grounds of the trade secret claims.

10. Alternative Dispute Resolution (ADR)

10.1 Dispute Resolution Mechanisms

While Taiwan offers alternative dispute resolution mechanisms, such as mediation or arbitration, they are not commonly used in trade secret disputes. This is because the arbitration/mediation tribunals have limited power to investigate evidence, which can be unfavourable to the owner of the trade secret, who often lacks sufficient evidence to prove misappropriation. Although the tribunal may order the preservation of evidence, either party seeking preliminary injunctions, provisional seizure or other interim measures must still apply through the court system.

Trends and Developments

Contributed by:

Jane Tsai, Aaron Chen, Yi-Chen (Sally) Yang and Yu-Ting (Tina) Lee
Lee, Tsai & Partners

Lee, Tsai & Partners is a full-service boutique local firm servicing the Greater China region. The firm's headquarters are in Taipei, co-operating with a local partner law firm in Shanghai and a representative office of local IP consulting firm in Beijing. The firm's trade secrets law practice group includes former judges, a former prosecutor and experienced attorneys and is led by Dr Chung-Teh Lee. The firm has substantial experience representing companies in all instances of Taiwan courts and on landmark

cases. Lee, Tsai & Partners also regularly advises clients on the strategic planning and management of IP rights in relation to the high-tech industry, including obtaining patents and trademarks, IP licensing issues and litigation. The firm's client profile includes the largest online search engine providers, airlines, semiconductor manufacturers, telecommunications companies, pharmaceutical companies, infrastructure providers, banks, insurance companies, private equity funds and venture capitalists.

Authors



Jane Tsai is a partner at Lee, Tsai & Partners with over twenty years of experience. She specialises in intellectual property matters and is internationally recognised for her

expertise in trade marks, patents and trade secrets. She has a record of achieving success on behalf of her clients in complex intellectual property litigation in Taiwan. Ms Tsai further frequently assists her clients in intellectual property rights planning, including global trade mark strategic planning and internal trade secret protection mechanisms.



Aaron Chen is a partner at Lee, Tsai & Partners who specialises in competition law, intellectual property, the Company Act, commercial arbitration and litigation. He has a proven

record of successfully representing clients in landmark competition cases, including the intersection of IP and competition law. Mr Chen also regularly advises clients on their cross-strait investments and corporate governance matters. He frequently assists clients on intellectual property protection, licensing and dispute matters in Taiwan and China.

Contributed by: Jane Tsai, Aaron Chen, Yi-Chen (Sally) Yang and Yu-Ting (Tina) Lee, **Lee, Tsai & Partners**



Yi-Chen (Sally) Yang is an associate at Lee, Tsai & Partners. She works on various legal issues and specialises in trade secret laws, competition laws, construction laws, and government procurement laws. Ms Yang is an experienced litigator and has represented clients before the civil court and administrative appeal. She advises companies on competition law analysis, group M&A and China-related compliance matters.



Yu-Ting (Tina) Lee is an associate at Lee, Tsai & Partners. She has experience advising on a wide range of commercial disputes concerning both litigation and international arbitration. She assists well-known corporations and multinational enterprises in multiple aspects of legal services, including general corporate legal affairs, litigation and international arbitration. She also has particular experience in the technology, biotechnology and medical industries.

Lee, Tsai & Partners

9F, 218 Tun Hwa S. Road
Sec. 2, Taipei
106033
Taiwan

Tel: +886 2 23785780
Fax: +886 2 23785781
Email: lawtec@leetsai.com
Web: www.leetsai.com



A GREATER CHINA LOCAL FIRM

Introduction

Taiwan has recently strengthened its legal framework for the protection of trade secrets by substantially revising the law governing the trial system for trade secret misappropriation cases and enhancing the protection of trade secrets related to national core key technologies.

Taiwan's Substantial Revisions to the Law Governing the Trial System for Trade Secret Misappropriation Cases

In Taiwan, the enforcement of trade secret misappropriation cases has been criticised for lacking professionalism and efficiency. To tackle such problems, Taiwan has recently substan-

tially revised the law governing the trial system for trade secret litigation, namely the Intellectual Property Case Adjudication Act (IPCAA).

This amendment is the most significant amendment since the enactment of the law in 2007. It is expected to clarify intellectual property litigation procedures, establish exclusive jurisdiction regulations for intellectual property actions, expand expert participation in the trial and strengthen the protection of trade secrets in litigation procedures. Amendments to IPCAA were promulgated on 15 February 2023, to be effective on 30 August 2023. Major revisions include the following.

Criminal actions involving trade secrets to be heard by the Intellectual Property and Commercial Court (“IPC Court”) instead of the current jurisdiction of the district court

In the past, the district court heard trade secret criminal actions. Nevertheless, the district courts have long been criticised for lacking professionalism and efficiency in handling trade secret espionage cases.

Because of the above issues, the IPCAA stipulates that criminal actions involving trade secret espionage shall be under the exclusive jurisdiction of the IPC Court (Article 54 and Article 58 of the IPCAA).

Civil actions involving trade secrets to be under the exclusive jurisdiction of the IPC Court instead of the current priority jurisdiction

Trade secret civil actions, such as requesting the removal of trade secret misappropriation or damage claims were applied to “priority jurisdiction” instead of “exclusive jurisdiction”. In the first instance, civil actions involving trade secrets can be heard by either the district court or the IPC Court. The superior court cannot invalidate the original judgment for the wrong jurisdiction.

Considering the technicality and legal expertise explicitly required for trade secret civil actions, the IPCAA stipulates that the first instance, appeal and interlocutory appeal procedures of trade secret civil cases will be exclusively under the jurisdiction of the IPC Court, except for “consensus jurisdiction” and “deemed consensus jurisdiction” under the Code of Civil Procedure which directs the jurisdiction to respective district courts (Article 9, Paragraph 1, and Article 48 of the IPCAA).

Mandatory representation by attorneys in civil actions

Legal representation was not compulsory in trade secret cases, but taking into consideration the high levels of legal professionalism and complications regarding trade secret civil actions, the IPCAA stipulated that representation by attorneys is mandatory for civil actions involving trade secrets in the first instance, the second instance, the third instance, the retrial procedures and the preservation procedures (such as petition recusal, evidence preservation) (Paragraph 1 of Article 10 of the IPCAA).

Addition of the Verification System

The “Verification System” is included in the IPCAA to relieve the trade secret holders’ burden of proving trade secret misappropriation. The parties may move for the court to appoint a neutral technical expert (the “Verifier”) to verify the documents or devices, or equipment (the “Verified Objects”) in the possession or under the management of another party or a third party (the “Verified Party”) after a complaint is filed (Article 19 of the IPCAA).

To ensure the neutrality of the Verifier, the person who has a particular relationship with the parties or a third party shall not be appointed as a verifier by the court, and the parties or third party may also refuse the appointment of the Verifier (Article 20 of the IPCAA).

A Verifier is appointed by the court to perform a legally compulsory evidence collection procedure. A Verifier must take an oath when verification or court trial is conducted and is subject to a penalty of perjury if there is any false verification or statement concerning important matters to the case. A Verifier is also penalised for violating trade secrets if he or she reproduces, uses or

discloses trade secrets learned during the verification (Article 74 of the IPCAA).

After conducting the verification, the Verifier shall file a verification report with the court, and the court shall serve the report on the Verified Party. If trade secrets are involved, the Verified Party shall move for the court within a specific period for a ruling to prohibit the disclosure of the verification report in whole or in part (Article 23 of the IPCAA).

Enhancing the effectiveness of the Confidentiality Preservation Order

In the past, the parties concerned could move for the court to issue a Confidentiality Preservation Order on the other party to protect the trade secrets that may be disclosed during the trial. Any person subject to a Confidentiality Preservation Order shall not use the trade secrets for purposes other than those related to the case, nor shall he disclose said trade secrets to those not subject to the order.

The issue is that the court can only issue the Confidentiality Preservation Order upon the parties' petition. The court will disclose the information to the other party only after an order is issued. The problem is that some parties hinder or delay the information disclosure by not moving for the court to issue such an order. To deal with this problem, the IPCAA empowers the court with the authority to ask the parties concerned to move for the Confidentiality Preservation Order and may issue such an order upon the request of the other party or a third party (Article 36 of the IPCAA).

Taiwan's Recent Amendments to the National Security Act Aiming to Strengthen the Protection of Trade Secrets of National Core Key Technologies

By referring to the USA Economic Espionage Act, the Taiwan government amended the National Security Act (NSA) and the Statute Governing Relations between the People of the Taiwan Area and the Mainland Area (the "Amended Statute") to strengthen the level of protection and prevent the leak of national core key technologies. The Amendment to the NSA was promulgated on 6 June 2022, with the effective date to be set by the Executive Yuan.

Under the NSA's authorisation, the National Science and Technology Council (NSTC) announced two draft regulations on 30 December 2022, and sought public comments, namely, the draft "Regulations on Determination of National Core Key Technologies" and the draft "Regulations on Identification of Government Subsidised, Commissioned or Funded National Core Key Technologies Projects". As of the date on which this article was written in April 2023, the two draft regulations are yet to be officially promulgated by NSTC.

Definition of "national core key technology"

"National core key technology" refers to a technology whose inflow into foreign countries, Mainland China, Hong Kong, Macau or hostile overseas forces will significantly undermine national security, industry competitiveness or economic development and which meets one of the following two conditions: (i) control should be imposed based on "international conventions, national defense needs, or national key infrastructure security protection considerations", or (ii) the "technology can lead to the generation of leading technologies or significantly enhance

the competitiveness of important industries in Taiwan”.

Procedure for the determination of national core key technologies

According to the draft “Regulations on Determination of National Core Key Technologies”, the NSTC will establish the National Core Key Technology Review Committee (the “Review Committee”) to handle the determination or modification of national core key technologies (the “Key Technologies”). The Review Committee, having 21 to 27 members, shall comprise representatives from national defense, intelligence, Mainland China affairs and other government agencies, scientific and technological research institutions, and leading technologies or industry experts.

Certain entities may apply for a determination or modification of the Key Technologies. For example, the NSTC may set up an office in charge of the assessment of Key Technologies (KTO), and the KTO may request the Review Committee for the above determination. Competent agencies that govern relevant industries may also actively apply for the Review Committee’s decision on the Key Technologies based on their initiatives or under requests from holders of the alleged vital technologies.

The submission for the determination of Key Technologies shall include the description, characteristics and efficacy of the alleged technologies, explanations as to why such technologies shall be protected under Key Technologies, and relevant technological and/or industry experts’ opinions, among others.

When determining whether alleged technologies should be protected as the Key Technologies, the Review Committee may invite the repre-

sentatives of interested parties and other relevant experts to provide their opinions during the review process.

Finally, the Review Committee may resolve to determine whether the submitted technologies should be deemed or removed from the Key Technologies by simple majority votes. Once the Review Committee renders its decision, it should be further announced by the Executive Yuan, followed by a recordal in the Legislative Yuan.

Prohibited conduct

Under the amended NSA, no person may engage in any of the following acts for any foreign countries, Mainland China, Hong Kong, Macau, hostile overseas forces, or other organisations, institutions, or groups they establish or substantially control.

- Obtaining trade secrets of the Key Technologies by way of theft, embezzlement, fraud, duress, unauthorised reproduction, or other improper methods, or using and disclosing them after obtaining them.
- Knowing or possessing trade secrets of the Key Technologies and reproducing, using or disclosing such trade secrets without authorisation.
- Possessing trade secrets of the Key Technologies and failing to delete, destroy or conceal such trade secrets after being notified by the trade secrets’ owner to do so.
- Obtaining, using or disclosing trade secrets of the Key Technologies with the knowledge that they are learned or possessed in violation of the preceding three subparagraphs.

The amended NSA also prohibits any person who intends to use trade secrets of Key Technologies in a foreign country, Mainland China,

Hong Kong or Macau, from performing any of the conduct above.

Criminal liability and exclusive jurisdiction of the IPC Court

Any person violating one of the above prohibited conducts shall be punished by imprisonment of five to 12 years and may be fined TWD5 million to TWD100 million (approximately USD150,000 to USD3 million). Any person who intends to use trade secrets of the Key Technologies in a foreign country, Mainland China, Hong Kong or Macau through any of the prohibited conducts shall be punished by imprisonment of three to ten years and may also be fined TWD5 million to TWD50 million (approximately USD150,000 to USD1.5 million).

Criminal actions regarding the trade secret misappropriation of Key Technologies are to be heard by the second instance of the IPC Court.

It is also worth noting that a confidentiality preservation order (“Confidentiality Order”) may be granted during criminal investigations by a prosecutor and court proceedings by a judge. Under the amended NSA and IPCAA, violation of a Confidentiality Order involving the protection of trade secrets of Key Technologies will trigger more significant criminal liabilities than the violation of such a Confidentiality Order concerning normal trade secrets. In addition, anyone who violates such Confidentiality Orders outside of the territory of Taiwan will still be subject to the above criminal liabilities.

Travel restrictions under the Amended Statute

Business personnel involved in Key Technologies may also be restricted from traveling to Mainland China Area under the Amended Statute. In sum, it is required that the individuals or members of juristic persons, groups or other institutions who have been engaging in projects involving Key Technologies that are commissioned, subsidised, or funded by Taiwan government agencies or institutions up to a certain threshold, obtain prior approval by an examination committee (led by the Ministry of the Interior in conjunction with related agencies) before traveling to the Mainland China area. Such a restriction also applies to those to whom such commissioning, subsidy or funding has been terminated or who have left their employment for less than three years. Violation of this requirement shall be subject to a fine of TWD2 million to TWD100 million (approximately USD700,000 to USD3 million).

According to NSTC’s draft “Regulations on Identification of Government Subsidised, Commissioned or Funded National Core Key Technologies Projects”, the threshold above is set as “more than half”, which means technology research and development projects involving Key Technologies that receive more than half of their funds from government agencies’ support will be subject to the above travelling restriction.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com