

Intellectual Property and Intellectual Property Management

MN 3060

Session 04: Trade Secrets: Confidential Know-how
&
Unfair Competition

Amali Hettige
amalih@uom.lk

Trade secret

Any information that is:

(1) Not generally known to the relevant business circles or to the public;

(2) Talks some sort of economic benefit on its owner.

(This benefit must originate specifically from the fact that it is not generally known, and not just from the value of the information itself)

Eg: benefits derived from use, costs of developing the TS , licensing offers; etc.

(3) Subject of reasonable efforts to maintain its secrecy.

- Anything that is easily and completely disclosed by the mere inspection of a product put on the market cannot be a trade secrets
- A trade secret continues for as long as the information is maintained as a trade secret. **NO EXCLUSIVITY**

Trade Secrets: Confidential Know-How

Trade secrets are confidential information that has commercial value by virtue of being kept secret and reasonable steps have been taken to keep it secret.



Three essential legal requirements:

1. The information must be secret
2. It must have commercial value because it's secret
3. Owner must have taken reasonable steps to keep it secret

Eg: Reasonable' → case by case

- Reasonable security procedures
- Non-disclosure agreements (NDA)
- Such that the information could be obtained by others only through improper means

Courts will only grant relief if someone has **improperly** acquired, disclosed or used the information

Only theft if wrongful !

Eg: Break Duty of trust, Violation of Confidentiality agreement or NDA, theft, bribery, hacking

TRADE



- Provides competitive advantage
- Potential to make money

SECRET



**Kept
confidential**

“not **generally known** among or **easily accessible** to persons within the circles that normally deal with this kind of information”

Why we protect trade secrets – by law

1. Maintain and promote standards of commercial ethics and fair dealing.
2. To provide an incentive for businesses to innovate by safeguarding the substantial time and capital invested to develop competitively advantageous innovations, both technical and commercial, and especially those that are **not patentable or do not merit the cost of patenting**.
3. If not protected by trade secret law, then competitors could use these innovations without having to shoulder the burden of costs or risks faced in developing the innovations.

Case Study: One of the best-kept trade secrets in the world

The procedures for protecting the formula for Coca-Cola

How it protect

- The written version of the secret formula is kept in a security vault at the Trust Company Bank in Atlanta, and that vault can only be opened by a resolution from the Company's Board of Directors.
- It is the Company's policy that only two persons in the Company shall know the formula at any one time, and that only those persons may oversee the actual preparation.
- The Company refuses to allow the identity of those persons to be disclosed or to allow those persons to fly on the same airplane at the same time.
- The same precautions are taken regarding the secret formulae of the company's other cola drinks- diet Coke, caffeine-free diet Coke, TAB, caffeine-free TAB and caffeine-free Coca-Cola.



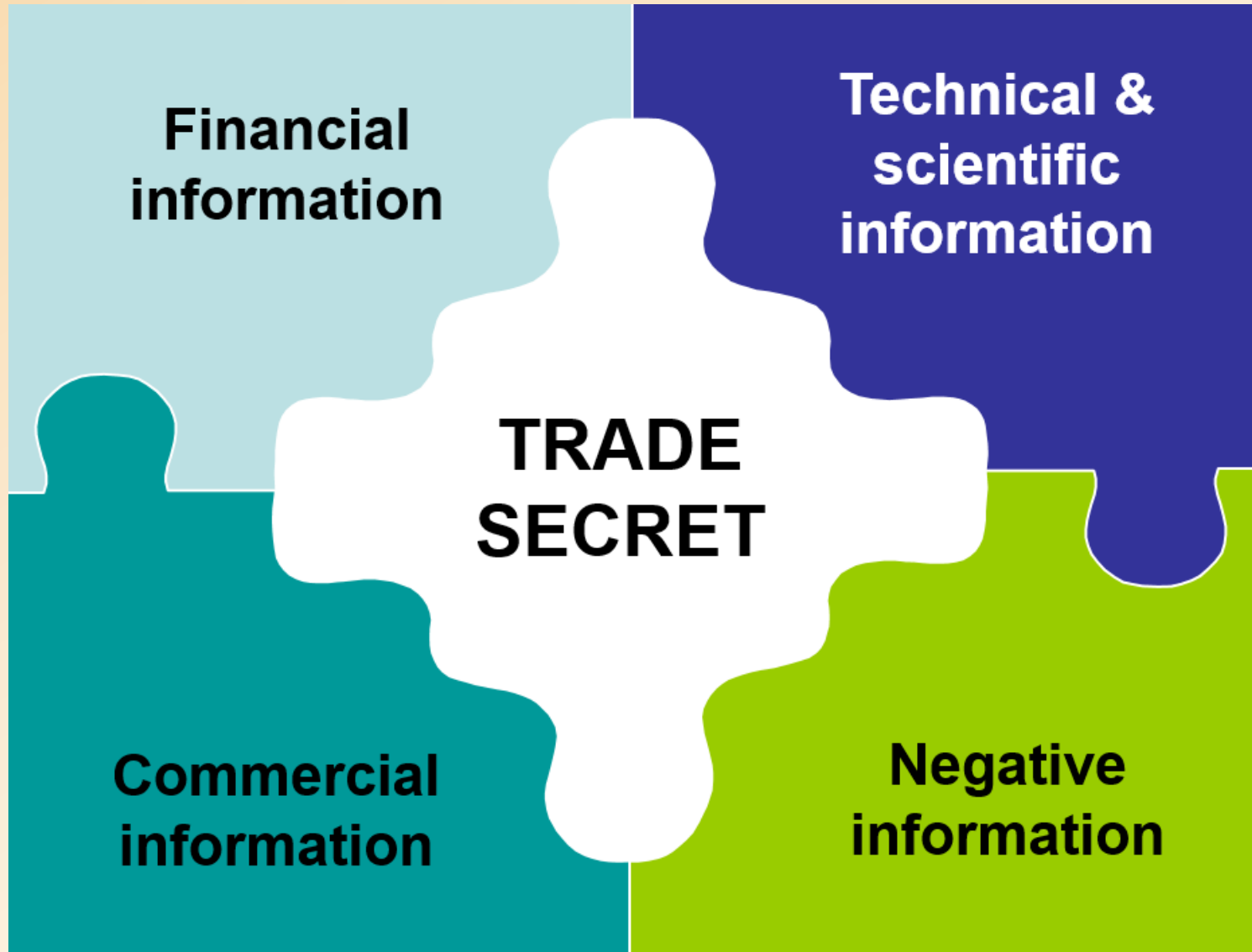
Example of Secret Recipe

Kentucky fried chicken

- The secret recipe of “11 herbs and spices” lies in a bank vault.
- Few people know it, and they are contractually obligated to secrecy.
- The ingredients are mixed by two different companies in two different locations and then combined elsewhere in a third, separate location.
- To mix the final formula, a computer processing system is used to blend the mixtures together and ensure that no one outside KFC has the complete recipe



Type of information that could be a trade secret





Typical examples in the software industry

1. Computer technology

- hardware + software (esp. source code, object code,)
- whether < patent or copyright protection
- algorithms, formulas, data flow charts, specific procedures that are implemented in the software or website
- electronic data compilations

2. Software design documents

3. Technical data about product performance

4. Software development agreements

5. Pending patent applications

General Examples;

- Information relating to a formula, pattern, device or other compilation of information that is used for a considerable period of time in a business
- Technical information used in the manufacturing process for production of goods
- Business plans & strategies
- New product names
- Financial projections
- Marketing plans, unpublished promotional material
- Cost & pricing information
- Sales data
- Customer lists
- Info re: new business opportunities
- Personnel performance
- Product specifications, product characteristics, purchase prices of key raw materials, test data, technical drawing or sketches, engineering specifications, proprietary recipes, formulas, content of laboratory note books
- Agreements containing details of marketing tie-ups, promotional or marketing material under development.

Challenges and limitations of trade secret protection

A trade secret **cannot be protected** against being discovered by fair and honest means,
Eg: by independent invention or reverse engineering

then such a person cannot be stopped from using the information so discovered.

Under these types of circumstances, the owner of a trade secret **cannot take any legal action** against the other person

TS (e.g. new technology or software) developed by employee or developed by external contractor

To avoid disputes:

1. WRITTEN AGREEMENT

+

ASSIGN


in advance all trade secrets developed during employment or commission

2. Contractually forbid reverse engineering

Advantages of trade secret protection

1. Trade secrets involve no registration costs;
2. Trade secret protection does not require disclosure or registration;
3. Trade secret protection is not limited in time;
4. Trade secrets have immediate effect.
5. By keeping valuable information secret, you can prevent competitors from learning about and using it and thereby enjoy a competitive advantage in the marketplace.





Disadvantages of protecting Patentable Inventions as trade secrets

1. The secret embodied in an innovative product may be discovered through “reverse engineering” and be legitimately used.
2. Trade secret protection only protects you against improper acquisition, use or disclosure of the confidential information.
3. A trade secret is difficult to enforce, as the level of protection is considerably weaker than for patents.
4. Another person may patent someone’s trade secret if he has developed the same invention by legitimate means.

Trade Secrets

no registration

- less costs (but: costs to keep secret)
- immediately available

can last longer

- but: limited to economic life
- uncertain lifespan: leak out is irremediable

no public disclosure

- but: practical need to disclose
- if leak out: TS lost

Patents

registration

- fees (registration + maintenance)
- takes time to get patent

limited in time

- generally: max 20y
- but: can be invalidated

public disclosure

- publication 18m after filing
- if P not allowed: no TS

Trade Secrets

Large subject matter

Protection of virtually anything maintained in secret by a business that gives competitive advantage

Only protection against improper acquirement/use

More difficult to enforce

- some countries: no laws
- ability to safeguard TS during litigation

Patents

Subject matter limited:

- Requirements: new, non obvious, useful
- Scope: patent claim

Exclusive rights

monopoly to exploit the invention

"Power tool"

How are trade secrets lost or stolen ?

- Reverse engineering
- Independent discovery
- Improper licensing
- Thefts by professional criminals targeting specific technology
- Network attacks (hacking)
- Laptop computer theft
- Inducing employees to reveal TS
- Departing or disgruntled employees
- Unavoidable (knowledge acquired)
- By ignorance

TS protection may be based on...

1. Contract law

- When there is an agreement to protect the TS
NDA/CA
anti-reverse engineering clause
- Where a confidential relationship exists
attorney, employee, independent contractors

2. Principle of unfair competition

- Misappropriation by competitors who have no contractual relationship
theft, espionage, subversion of employees

3. Criminal laws

- For an employee to steal trade secrets from a company
- Unauthorized access to computers
- theft, electronic espionage, invasion of privacy, etc.
- circumvention of technical protection systems

4. Specific trade secret laws

- **US: Uniform Trade Secrets Act; Economic Espionage Act**

In Sri Lanka

Identified as UNFAIR COMPETITION AND UNDISCLOSED INFORMATION

Definition of Unfair Competition

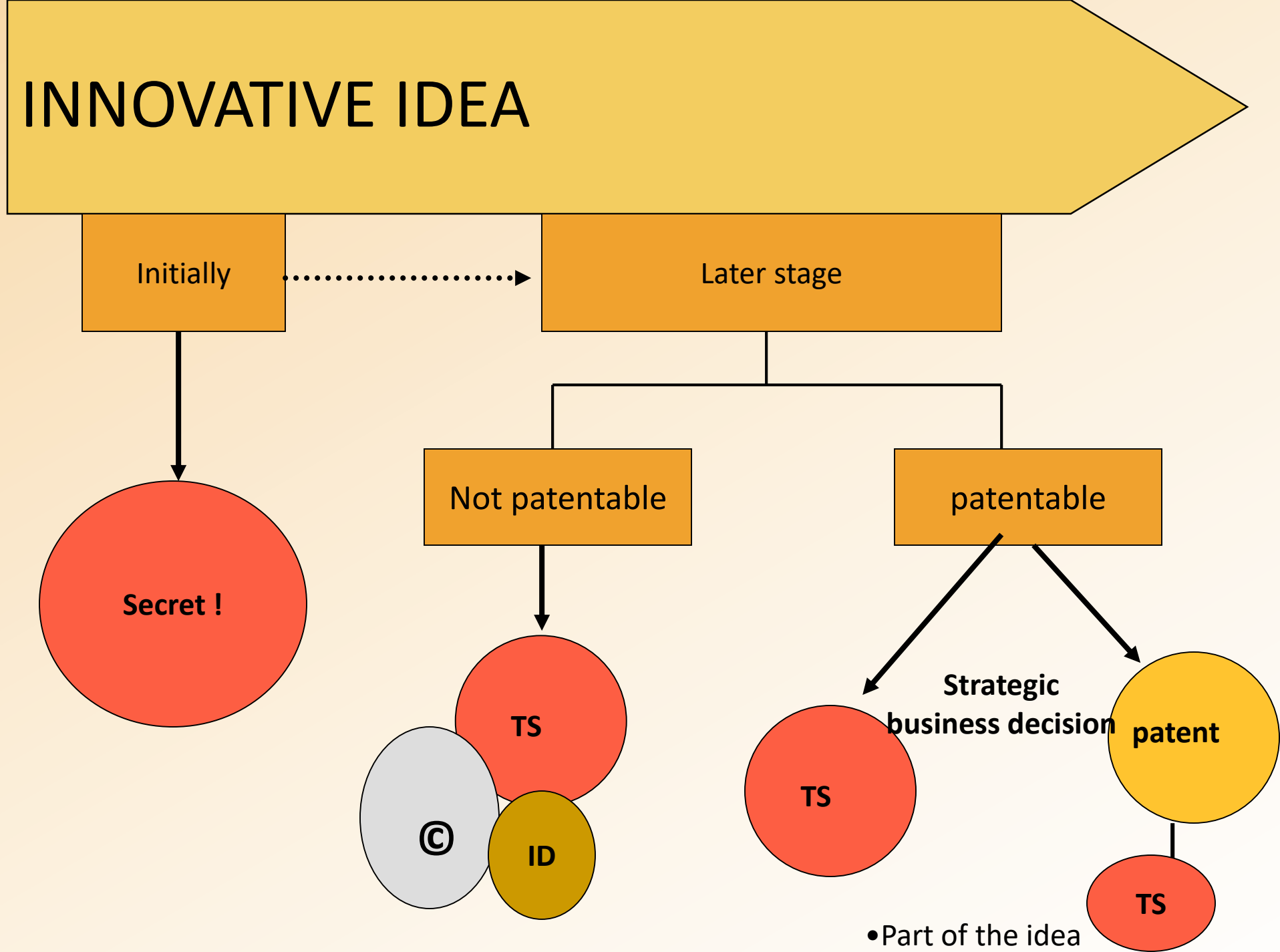
Any act or practice carried out or engaged in, in the course of industrial or commercial activities, that is contrary to honest practices shall constitute an act of unfair competition

Things to bear in mind

1. ANY innovative idea should be kept as a **secret** in the beginning

- to preserve option of patenting (or industrial design) at later stage

INNOVATIVE IDEA



Things to bear in mind

2. Choice between patent or TS must be made both from legal and business perspectives

(if patentable)

Protection Strategies

- Identify Trade Secrets
- Develop Protection Policy; Document it
- Educate Employees; Monitor Compliance
- Restrict Access
- Mark Documents
- Physically Isolate and Protect
- Maintain Computer Secrecy
- Restrict Public Access to Facilities
- Deal Cautiously with Third Parties; Confidentiality Agreements and Nondisclosure Agreements
- Be Careful and Consistent with Unwanted Submissions
- Security/Trade Secret Audit; internal / external
- Coordination of integrated security enterprise-wide

Identify Trade Secrets

a. The basic questions to ask –

What information would hurt my business if my competitors get it? - And how much will it hurt?

What is the value of the information for your company?

What is the potential value for your competitors?

How much effort/money spent in developing it?

b. A related question to ask –

Do you have staff specifically assigned to record keeping, data security, or for preservation of trade secrets?

Have measures been taken to guard its secrecy?

How difficult would it be for others to acquire, collect or duplicate it?

C. Accurate record keeping

Make a written list of the information to be protected and organize it into the different types of information, depending on its value to the business and the type of protection measures that would be needed to protect it.

Develop Protection Policy

The information security policy

A procedure designed to protect the information assets from disclosure to any person or entity not authorized to have access to that information, especially information that is considered sensitive, proprietary, confidential, or classified (as in national defense).

a. Written information security or trade secret protection policy.

Provides clarity on all aspects that need to be addressed. - It should explain the why and how of doing so.

Prescribe how to reveal or share such information in-house or with outsiders.

Demonstrate the commitment of the business to protect its trade secrets

b. Information security can be implemented at various levels

- Physical controls

- Administrative controls

- Technical controls.

Educate Employees

All employees on issues related to information security

- a. Always hire an employee on the basis of his competence knowledge and skills and not because of his access to trade secrets of a former employer.
- b. All employees should acknowledge that they have understood the policy and that they agree to abide by it. Periodically, reiterate the policy.
- c. Avoid hiring a person bound by a non-compete agreement. If unavoidable then do so only after taking advice from an independent and competent lawyer.
- d. Indemnifying a new employee, who is bound by a non-compete agreement to a previous employer, should be avoided, as doing so raises suspicion of wrong doing and may result in a financial obligation if wrong doing is proved in a court case
- e. Remind your employees not to disclose trade secrets to unauthorized individuals or entities and to follow the security procedures; do so by way of notices, memos, network e-mails, newsletters, etc.
- f. Hiring away more than one employee from a competitor would raise suspicion of wrong doing, and, therefore, it should be avoided as far as possible.

Summary: Educate and train:

- Clear communication and repetition
- Copy of policy, intranet, periodic training & audit, etc.
- Make known that disclosure of a TS may result in termination and/or legal action

Measures for Employees

1. Current employees

- Prevent inadvertent disclosure (ignorance)
- Train and educate
- NDA for particular task

2. New employees

- Brief on protection expectations early
- Obligations towards former employer!
- Assign all rights to inventions developed in the course of employment
- NDA/CA
- Non-compete provision

3. Departing employees

- Further limit access to data
- Exit interview
- Letter to new employer
- Treat fairly & compensate reasonably for patent work

(4) Importance of exercising care in hiring an employee of a competitor

- a. Educate and train employees on information security policy.
- b. Transform every employee into a potential security officer.
- c. Every employee must contribute to create a secure environment.
- d. Prevent inadvertent disclosure that may take place due to ignorance.
- e. The employees should be trained to recognize and properly protect trade secrets.

- Separate locked depository
- Authorization
- Access control
 - log of access: person,
 - document reviewed
 - biometric palm readers
- Company premises
 - guards, surveillance
 - cameras
- Shredding
- Oversight; audit trail

Restrictions for Writing

Include reasonable restrictions in writing, in all contracts Signing a good confidentiality or non-disclosure agreements

- Make departing employees aware of their obligations towards former employer.
- Do so by conducting exit interviews that should also focus on issues related to confidentiality, trade secrets, etc.
- If necessary or desired, they should be made to sign a new or updated confidentiality agreement.
- You may write a letter to new employer informing him about the relevant aspects of your trade secret concerns so that the departing employee is not put by the new employer on projects or activities where inevitable disclosure of your trade secrets would occur or is most likely to happen

Apply to only those persons having a **need to know** the information

Restrict access to paper records

- Restrict access to paper records To prevent unauthorized access to records classified as confidential, sensitive, or secret, limit access to only those employees who are duly approved, or cleared, to see them on a need to know basis.
- This may be done more easily by proper labeling of records (e.g., with a stamp such as confidential or secret) or using special colored folders (e.g., red or orange), and by keeping such marked records physically isolated or segregated in a secure area or in locked filing cabinets.
- Depending on the size and nature of the trade secret, the location of the separated information can vary from a locked file cabinet, to a security patrolled warehouse or storage facility.
- There has to be proper access control through appropriate authorization and accountability and tracking system for employees provided access to classified information.

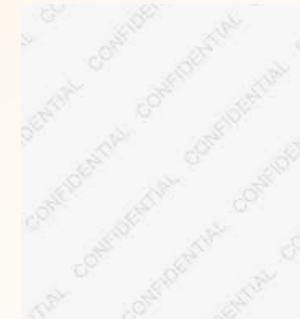
Mark documents

Various types of useful ways for marking confidential or trade secret information.

- a. MAKE NO COPIES
 - b. THIRD PARTY CONFIDENTIAL
 - c. DISTRIBUTION LIMITED TO
 - d. COVERED BY A NON-ANALYSIS AGREEMENT
- The CRITICAL, MAXIMUM, MEDIUM, and MINIMUM labels

- Help employees recognize TS prevents inadvertent disclosure
- Uniform system of marking documents
 - paper based
 - electronic (e.g. 'confidential' button on standard email screen)

Labels should provide brief but clear direction to the user on how to handle the information.



Office management be aware of

- a. Mobile or cellular phones discussing sensitive topics over a cellular phone is a dangerous practice.
- b. Fax machine is located in a common area with unrestricted access and it is typically unattended. The second problem with fax transmissions is that they utilize phone lines, which can be tapped quite easily.
- c. Photocopying It is not unusual for an employee to make copies of a secret or confidential document, pick up the copies and walk away, leaving the original in the copier for the next user to find.
- d. Shredding a better method for disposition of all paper records, of course, is shredding them.
- e. Internal literature Newsletters, magazines, and other in-house publications often contain information useful to snoops, including new product announcements, results of market testing, and names of employees in sensitive areas (who are potential contacts).
- f. Waste bins It is not safe to put them into a nearby office waste paper or trash bin, as anyone with access to the trash might make use of those records for gathering competitive intelligence.
- g. The compulsive talker and loose talk Employees are deluding themselves if they think their lunchtime or coffee break conversations and any discussion of company business on the metro, subway, bus stop, train station, or a restaurant is wholly private. It is not at all unusual for people nearby to hear clearly these conversations.

Maintain computer secrecy

For most computer systems at least two security measures

- a. Use of passwords for a user to access the system
- b. Automated audit trails to enable system security personnel to trace any additions or changes back to whoever initiated them, and to indicate where and when the change was carried out.

Access control is a means of enforcing authorizations.

There are a variety of access control methods that are based on different types of policies and rely on different security mechanisms.

- a. Rule based access control is based on policies that can be algorithmically expressed.
- b. Identity based access control is based on a policy which applies explicitly to an individual person or host entity, or to a defined group of such entities. Once identity has been authenticated, if the identity is verified to be on the access list, then access is granted.



How trade secrets get stolen

- a. External threats include corporate spying with professional criminals targeting specific technology, initiating network attacks (hacks), laptop computer thefts:

accessing source code, product designs, marketing plans, customer lists - approaching employees to reveal company information etc. Businesses strive to protect their trade secrets by enacting corporate security measures and confidentiality clauses in employment, technology licensing, distributorship and joint venture agreement

- b. Internal theft by disgruntled workers or former employees is also intentional. Some of these people allow themselves to be exploited by competitive intelligence operatives, either for money or merely for spite.


They may include seemingly innocent persons such as research analysts, business analysts, information specialists, and potential employees or customers, who gain employees' trust for obtaining proprietary information by inducements, gifts or blackmail.



Protection of trade secrets

Most countries do not have a specific law for trade secrets.

The owner of trade secrets has to rely on relevant provisions of the national law against unfair competition and/or by court action under the law of torts and by appropriate clauses or provisions in employment agreements and other types of business agreements in accordance with the contract law of the country



(1) Unfair competition law / Principles of tort When misappropriation is done by competitors who have no contractual relationship or indulge in an act of theft, espionage, or of subversion by employees.

The law of tort is judge-made law in 'common law' countries

(2) Contract law When the agreement between the parties seeks to protect the trade secret by using a non-disclosure clause or confidentiality clause, through an anti-reverse engineering clause, or where an implied confidential relationship exists, such as between an attorney and his client, or an employer and his employee, etc.

(3) Criminal law When an employee steals trade secrets from a company or someone does espionage or is involved in acts that may be considered as invasion of privacy, etc., or circumvention of technical protection measures of IT / non-IT systems



Violation of trade secrets

1. How to establish violation of trade secrets

Main issues are:

- (1) Was the information indeed secret?
- (2) Were reasonable steps taken to maintain the secrecy?

To establish violation of trade secret rights, the owner of a trade secret must be able to show the following:

- (1) Infringement by or competitive advantage gained by the person/company which has misappropriated the trade secret.
- (2) The owner had taken all reasonable steps to maintain it as a secret.
- (3) There is misuse as the information obtained has been used or disclosed in violation of the honest commercial practices.

Remedies for Violations

- (1) A court order restraining the person from further benefiting from or misusing the trade secret.
- (2) A court order for monetary compensation in the form of damages, based on the actual loss caused as a result of the misuse of trade secret. (For example, lost profits or unjust enrichment)
- (3) Removal order by the court, based on a civil action, which may include a search of the defendant's premises in order to obtain evidence to establish the theft of trade secrets at trial.
- (4) Precautionary for misused trade secrets, or the products resulting from its use or misuse.
- (5) A court may order the destruction of the products made by the infringing act, and/or destruction of the equipment used to carry out the infringing act.
- (6) Some countries permit the imposition of punitive damages for willful encouragement of trade secret theft.



Trade secret audit

How to conduct a trade secret audit

- (1) Identify significant trade secrets Consult with research and development, manufacturing, MIS, sales and marketing and human resources;
compare your company's advantages vis-à-vis manufacturing processes, raw material ingredients, information management, contacts with customers, etc., as compared to competitors.
- (2) Verify the company's title to trade secrets Contact legal and human resources to determine if assignments from employees, consultants or other predecessors in interest are complete.
- (3) Verify that confidentiality procedures are followed Contact security, human resources and departments that maintain the trade secrets.
- (4) Verify that employees, consultants, vendors, customers and other third parties do not disclose trade secrets of third party Contact human resources to determine if new employees and consultants agree in writing not to disclosure confidential information from former employers; contact legal, purchasing, sales and marketing, research and development, MIS and manufacturing regarding other third party agreements.



Trade Secrets Be Sold Or Licensed ?

Sale

Most TS Sales Occur As Part Of The Sale Of The Business

License

In Combination With Patent License

Software License For Highly Specialized Program

TS protection for financial, commercial & (secret) technical information:

- develop effective internal TS program to maintain trade secret status

TS protection for Software:

- restrict access
- impose obligation of confidentiality to anyone who has access

Certain aspects of software cannot be maintained as a trade secret

- information or technology that must be disclosed to the public in order to market the product
- information or technology which is part of a product sold to the public and can be reverse-engineered
- mass-marketed software
- where competition is so intense, that very likely to be independently developed by others within short time
- if great deal of personnel movement between competitors
- if customers require access to software for archive, back-up, updating, maintenance, debugging, etc.

Alternative or additional protection for software:

- make reverse engineering difficult (compiled code)
- technological protection measures
- copyright protection
- software patents



Be careful about signing confidentiality agreements

Definition : Unfair Competition

Any act of competition contrary to honest practices in industrial or commercial matters shall constitute an act of unfair competition.

Chapter XXXII Unfair Competition And Undisclosed Information

Intellectual Property Act, No. 36 OF 2003, Sri Lanka

Acts of unfair competition shall include the following:-

- (a) all acts of such a nature as to create confusion by any means whatsoever with the establishment, the goods, services or the industrial or commercial activities of a competitor;
- (b) a false allegation in the course of trade of such a nature as to discredit the establishment, the goods, services or the industrial or commercial activities of a competitor;
- (c) any indication of source or appellation of origin the use of which in the course of trade is liable to mislead the public as to the nature, manufacturing process, characteristics, suitability for their purpose or the quantity of goods;
- (d) making direct or indirect use of a false or deceptive indication of the source of goods or services or of the identity of their producer, manufacturer or supplier;
- (e) making direct or indirect use of a false or deceptive appellation of origin or imitating an appellation of origin even if the true origin of the product is indicated, or using the appellation in translated form or accompanied by terms such as "kind", "type", "mark", "imitation" or the like.

Legal Framework for Unfair Competition in Sri Lanka

- **Intellectual Property Act, No. 36 of 2003:**

This is the primary law governing intellectual property rights in Sri Lanka, which includes provisions on unfair competition. It aligns with international standards such as the TRIPS Agreement (Trade-Related Aspects of Intellectual Property Rights).

- **Consumer Affairs Authority Act, No. 9 of 2003:**

This law protects consumers from unfair trade practices, such as misleading advertising, false descriptions, and unfair selling techniques. The Consumer Affairs Authority (CAA) is responsible for enforcement.

Key Areas Covered by Sri Lankan Laws

Misleading Advertising:

Misleading or deceptive advertising is prohibited under the Consumer Affairs Authority Act. This can include false descriptions of products or services that confuse or deceive consumers.

•Trade Secrets:

Trade secret protection is available under the Intellectual Property Act, but the act does not provide specific procedural guidelines. Sri Lanka's trade secret protection mainly aligns with common law principles and requires companies to take reasonable measures to safeguard their confidential information.

•Passing Off:

This doctrine, under the IP Act, is intended to prevent one business from misrepresenting its goods or services as those of another, thereby "passing off" their products and confusing consumers.

•Counterfeiting and Piracy:

The IP Act also covers the protection against counterfeit goods and infringement of trademarks, patents, and copyrights, which can be considered forms of unfair competition.

3. Enforcement and Challenges

- **Court Actions:** Individuals and companies can file cases against competitors for acts of unfair competition. Courts may grant injunctions, award damages, or impose fines.
- **Consumer Affairs Authority:** The CAA investigates complaints of unfair trade practices, particularly from consumers, and can take action against businesses engaging in such practices.
- **Challenges:**
 - Limited awareness of unfair competition laws among businesses and consumers.
 - The absence of a specific Unfair Competition Act can make enforcement less clear-cut compared to countries with dedicated laws like Japan.
 - Enforcement of IP and unfair competition provisions can be slow due to the court system's backlog and procedural delays.

Practice of Japan Using the Unfair Competition prevention act

Trade Secret and Unfair Competition Prevention Act (UCPA)

- Enacted in 1993 (revised periodically)
- Purpose: Prevent acts of unfair competition, protect business interests, and promote fair competition.
- Complements other IP laws (patent, trademark, copyright).

Free competition is only allowed to the extent that it does not interfere with fair competition.

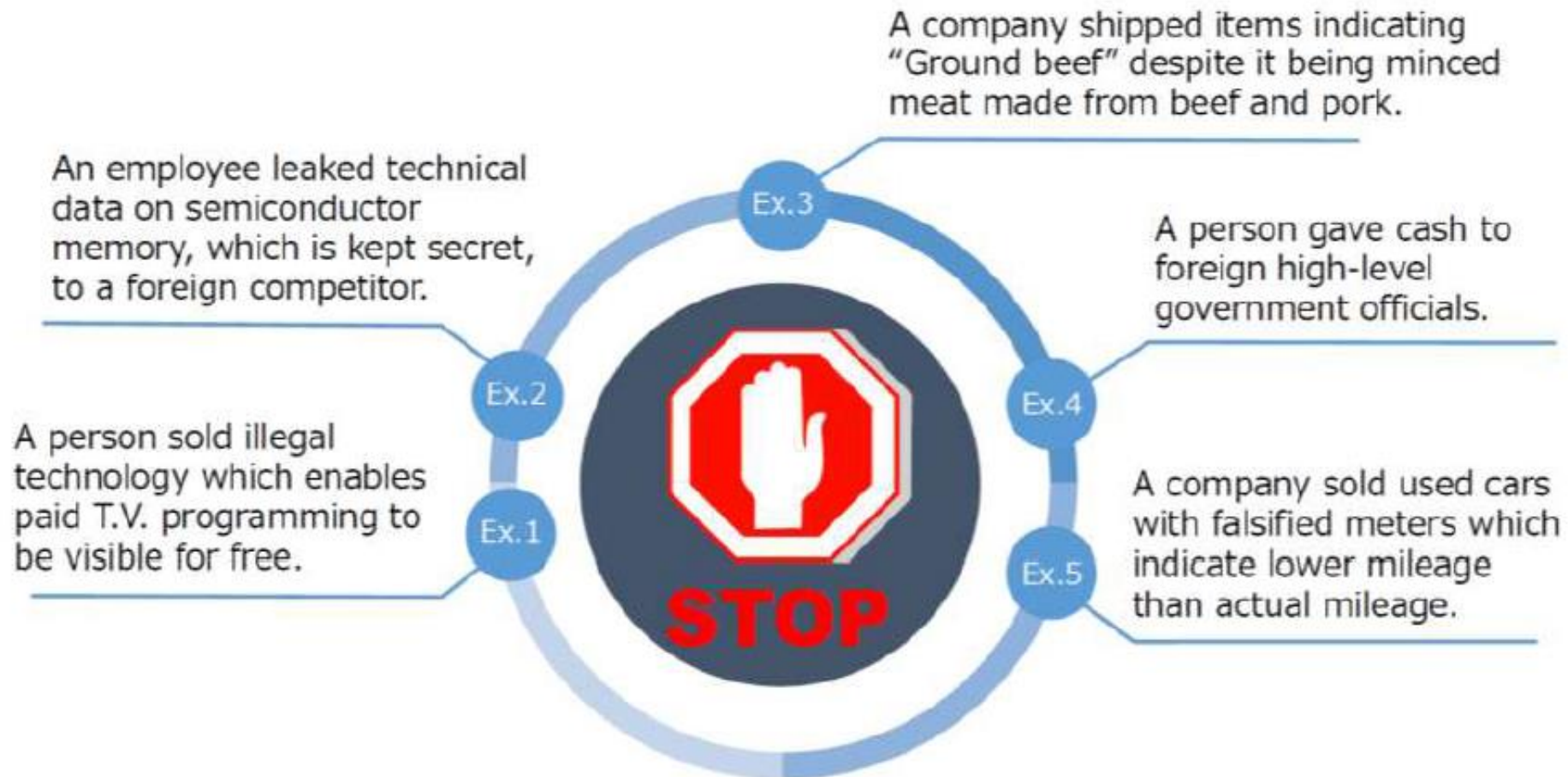
The UCPA aims to regulate unacceptable competition and maintain a fair competitive order.

The purpose of this Act is to provide measures, etc. for the prevention of unfair competition and for the compensation for loss or damage caused by unfair competition, in order to ensure fair competition among companies, and proper implementation of international agreements related thereto, thereby contributing to the sound development of the national economy.

Unfair Competition Prevention Act (UCPA)



The Act can prevent the following cases.



Unfair Competition Prevention Act (UCPA)

Key Provisions of UCPA

•Key Sections:

- **Protection of Trade Secrets:**

Criminal and civil sanctions for unauthorized acquisition, use, or disclosure of trade secrets.

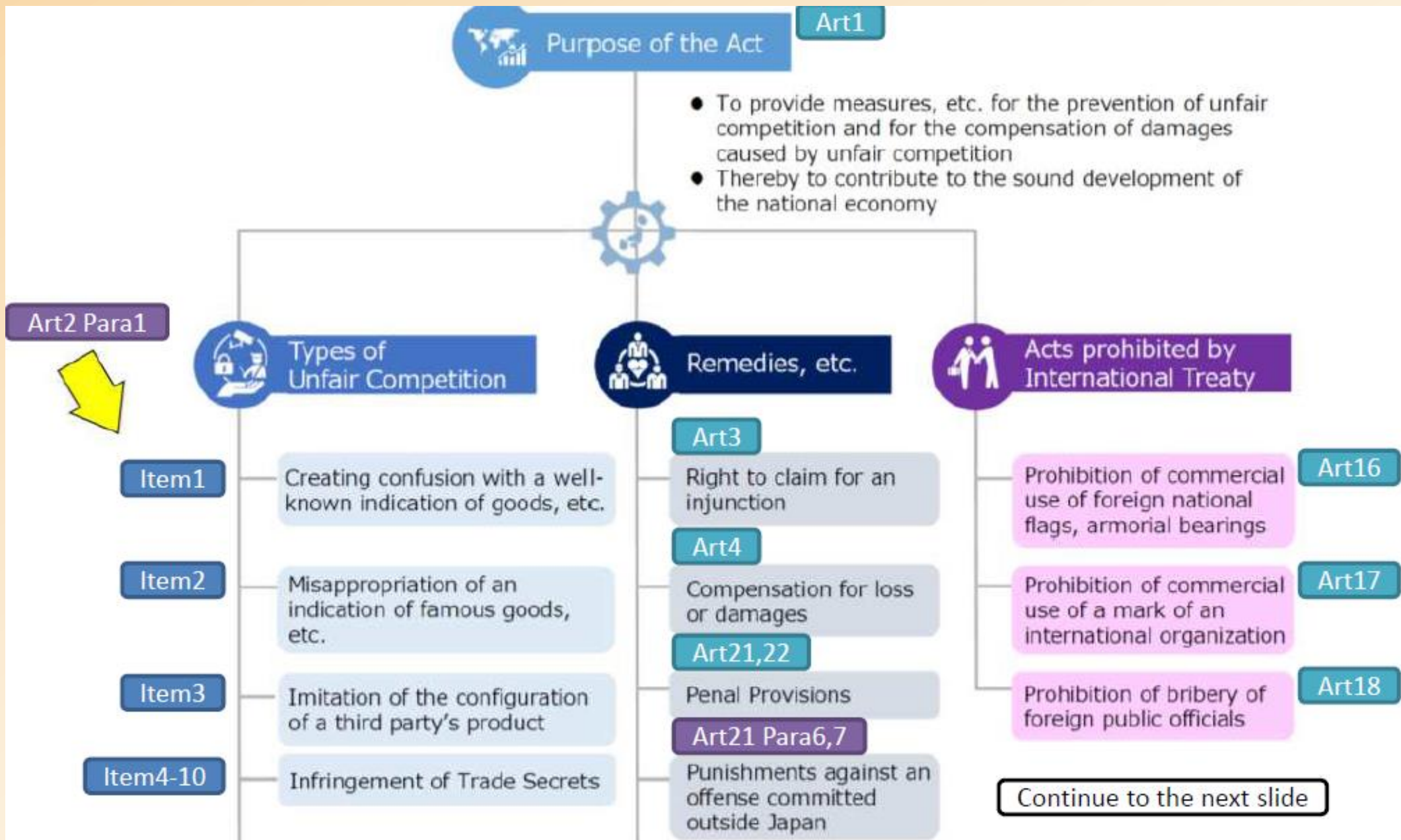
- **Prohibition of Acts Creating Confusion:**

Addresses consumer deception.

- **Prohibition of False Representations:**

Prevents false labeling and misleading information.

Unfair Competition Prevention Act (UCPA)



Unfair Competition Prevention Act (UCPA)

Continue from the previous slide

Types of Unfair Competition

- Item11-16** — Wrongful acquisition, usage of Protected Data (this will be effective on July 1st, 2019)
- Item17,18** — Providing a product which circumvents technological restriction measures
- Item19** — Wrongful acquisition, usage of a domain name
- Item20** — Misleading representation regarding the place of origin, quality, etc.
- Item21** — Act of injuring business reputation of a competitor
- Item22** — Misappropriation of a trademark by an agent of the trademark owner

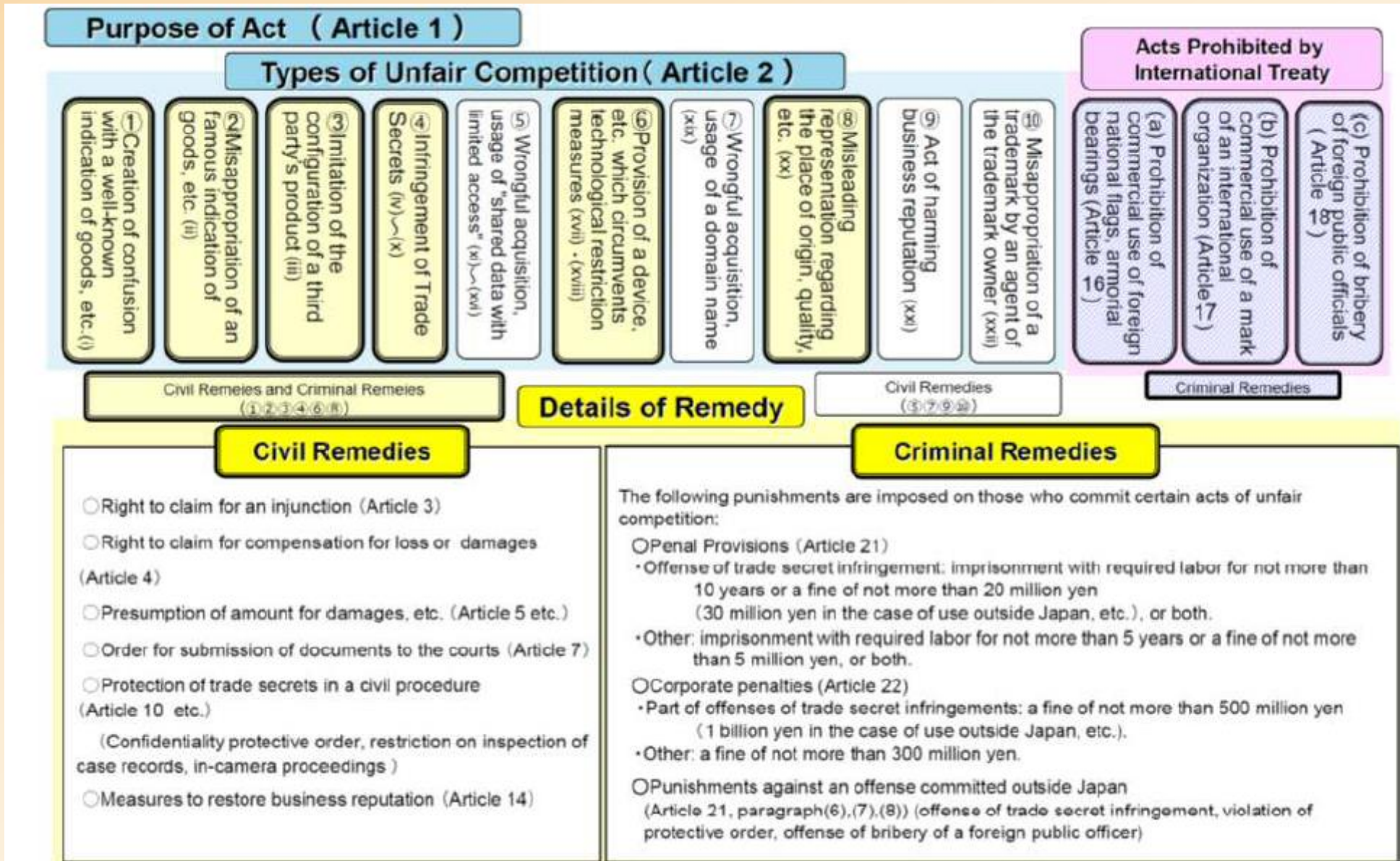
Remedies, etc.

- Art22 Para1** — Corporate penalties
- Art5** — Presumption of amounts for damages
- Art7** — Order to submit documents to the courts
- Art10,11** — Confidentiality protective orders
- Art14** — Measures to restore business reputation



Art2 Para1

Unfair Competition Prevention Act (UCPA)



Thank you!