CHINA IP SME HELPDESK

European Commission

法兰德斯中国商会 FCCC VCKK
FLANDERS-CHINA CHAMBER OF COMMERCE
VLAAMS-CHINESE KAMER VAN KOOPHANDEL

EU-China Business Association
欧盟中国贸易协会

Waiting for the organisers, the webinar will begin shortly…

Moderator

Moderator:

Peter Sczigel

Project Executive
China IP SME Helpdesk

peter.sczigel@china-iprhelpdesk.eu

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

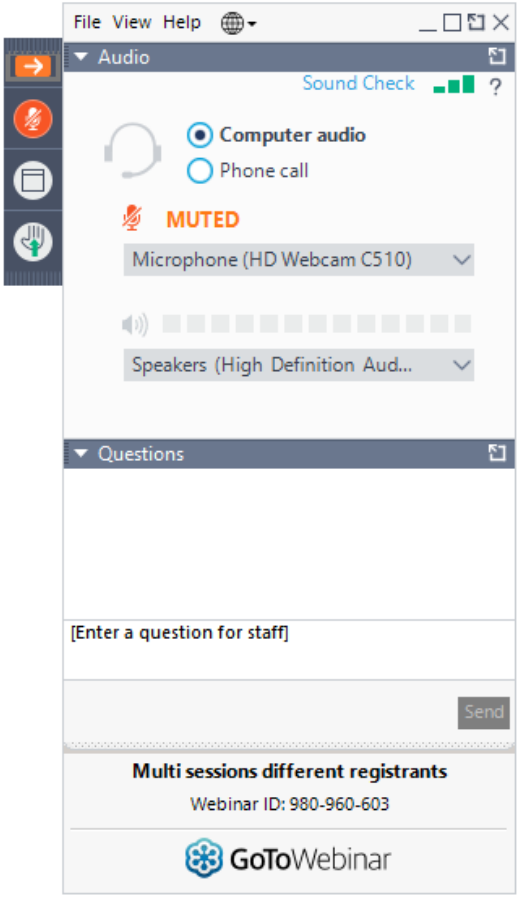
Webinar Interaction Tool

Hide control panel here →

Turn on full screen here →

Raise your hand here →

Send the IP expert a question here →



Webinar 24 hour technical support number: http://support.gotomeeting.com 'Contact Us' section

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

Helpdesk free services

Enquiry Helpline

Training Workshops

Webinars

Website & Blog

Guides & Factsheets

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

CHINA IP SME HELPDESK

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

European Commission

CHINA
IP SME HELPDESK

European Commission

法兰德斯 中国商会 FCCC VCKK
FLANDERS-CHINA CHAMBER OF COMMERCE
VLAAMS-CHINESE KAMER VAN KOOPHANDEL

Speakers

Gwenn Sonck

Executive Director

Flanders-China Chamber of Commerce / EU-China Business Association

Valentin de le Court

IP Expert

China IP SME Helpdesk

Agenda

Time	*Title*	*Speaker*
10:30 – 10:35	**Introduction to the Webinar**	*Peter Sczigel, China IP SME Helpdesk*
10:35 – 10:40	**Presentation of the Flanders–China Chamber of Commerce / EU-China Business Association**	*Gwenn Sonck, FCCC/EUCBA*
10:40 – 11:15	**How to protect your trade secrets in China**	*Valentin de le Court, China IP SME Helpdesk*
11:15 – 11:30	**Q&A**	

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

Introduction to the Flanders-China Chamber of Commerce / EU-China Business Association

Gwenn Sonck
gwenn.sonck@flanders-china.be

Flanders-China Chamber of Commerce (250 members)

- **Advice and expertise:** the FCCC tells you about the latest economic and trade developments via various publications and a weekly newsletter.
- **Meetings with Chinese delegations:** thanks to its extensive network the FCCC plays an important role in welcoming Chinese delegations to our country. We introduce Flemish entrepreneurs to non-traditional investment areas and help facilitate entering the Chinese market.
- **Exchange of experiences and sharing knowledge:** the FCCC regularly organizes conferences and round-tables on China so participants can exchange experiences, facilitate collaboration and create networking opportunities.
- **Privileged partner:** as the secretariat of the EU-China Business Association (EUCBA), the umbrella organization for all European China associations, the FCCC also plays an important role at a European level.

The membership fee for 2021 is:
Small and Middle enterprises: €435,00 (VAT excl.)
Large enterprises: €1.080,00 (VAT excl.)

Contact: http://www.flanders-china.be/en/about/join_fccc

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

EU-China Business Association

EU-China Business Association
欧盟中国贸易协会

The EU–China Business Association (EUCBA) is the EU-wide federation of national non-profit business organizations in the European Union with specialization and particular expertise in exchange of knowledge on investments and trade with China. At current, EUCBA unites 20 members in 20 countries representing more than 20,000 companies – large, medium, and small, in all branches of industry, commerce and the service sector.

- EUCBA **supports the China business interests** of its members and **acts as a channel of communication with government institutions of the EU and China.**
- The EUCBA adds value to the work of its members **by EXTENDING national work to a European level**
- The EUCBA aims to **facilitate the exchange of information**, views and experiences among its member organisations

www.eucba.org – contact: gwenn.sonck@eucba.org

CHINA IP SME HELPDESK

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

European Commission

TRADE SECRETS PROTECTION IN CHINA

(on the importance of
keeping your secrets… secret)

Valentin de le Court

Flanders-China Chamber of Commerce

13 April 2021

Valentin de le Court

- **DALDEWOLF**
- vdlc@daldewolf.com

Valentin de le Court is a Belgian qualified lawyer with fifteen years of experience in the intellectual property field, including four years of on the ground practice in China. His area of expertise covers contentious and non-contentious IP matters relating to innovation with a strong focus on patent law, trade secrets protection and management, and China related IP strategies and technology transfer. Over the past years Valentin has assisted European MNCs and SMEs active in a wide range of sectors (semiconductors, automotive, mobile gaming, oil & gas, digital communication, F&B, fashion, medical device and design) with their China related IP issues. Today he co-heads the IP/IT team and leads the China Desk at DALDEWOLF, a Belgian business law firm. Valentin is fluent in French, Dutch and English.

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

INTRODUCTION

European Commission

TRADE SECRETS, A HOT TOPIC?

Regulating the internet giants

The world's most valuable resource is no longer oil, but data

The data economy demands a new approach to antitrust rules

South China Morning Post News Comment Lifesty

Chinese Individual Indicted for Alleged Trade Secret Theft from Semiconductor Company

By Kate M. Growley, CIPP/G, CIPP/US and Suzanne Trivette on Oct 23, 2020 01:10 pm

DOJ Indicts Hong Kong Citizen in Attempted Trade Secrets Scheme

By Michelle Chipetine and Joshua M. Rychlinski on Mar 12, 2021 04:39 pm

How China Obtains American Trade Secrets

The New York Times

Companies have long accused Chinese rivals of swiping or seizing valuable technology. Beijing promises to ban those practices, but enforcement could be tough. Jan. 15, 2020

TOPIC

US-China tech war

The US and China are competing for supremacy in the suite of advanced technologies that will affect the means of future economic production. US efforts to curtail China's access to American technology are threatening to unravel decades of globalisation and interdependent supply chains and raising the risk of a confrontation that has been likened to a new cold war.

WEEKLY THREAT REPORT

US warns of Chinese actors exploiting public vulnerabilities

The National Security Agency (NSA) has issued an advisory detailing malicious activity by Chinese state-sponsored cyber criminals.

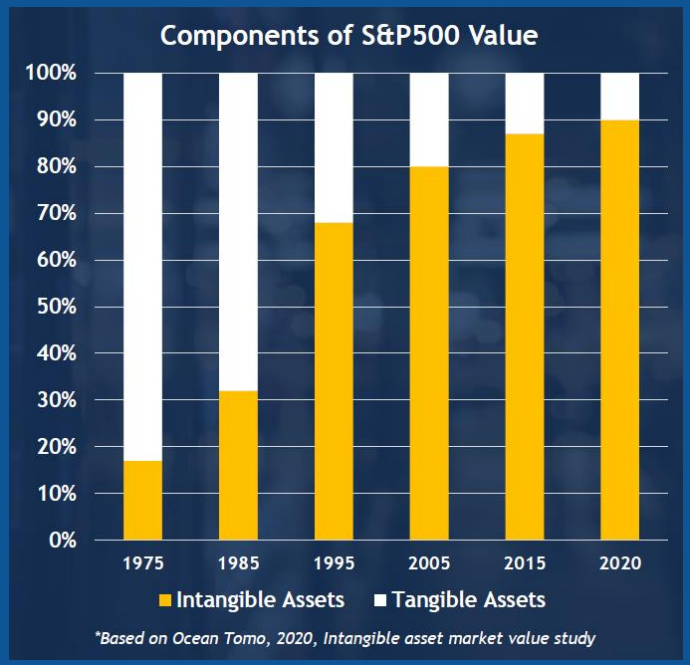
I – TRADE SECRETS,

THE CONTEXT

(1.) THE GROWING IMPORTANCE OF INTANGIBLE ASSETS IN TODAY'S ECONOMY

Forbes / Entrepreneurs

Pay Attention To Innovation And Intangibles -- They're More Than 80% Of Your Business' Value



- "More than 80% of your business' value"
- 1975 → intangible assets = 17% of corporate value
- 2020 → intangible assets = 90% of corporate value

(2.) TWO WAYS TO PROTECT THE RESULTS OF YOUR INNOVATION

1. Intellectual Property Rights ('IP')

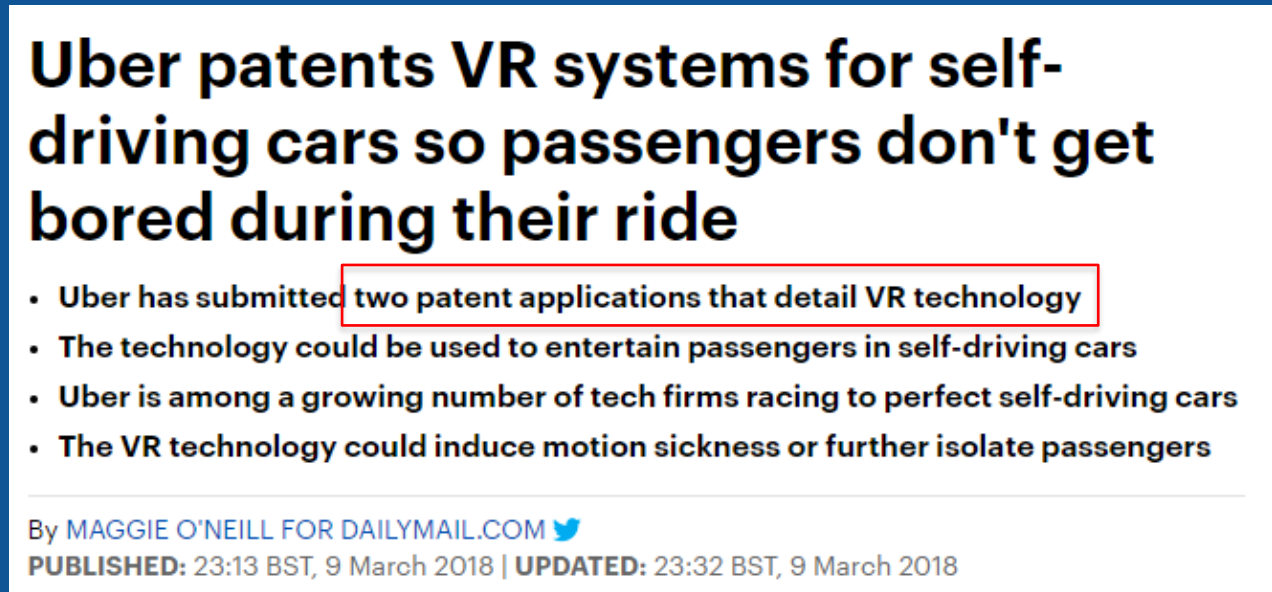
- Exclusive right granted (monopoly)

2. Trade secrets ('TS')

- No exclusive right granted
- Protection against unlawful acts

WHAT IS A PATENT?

- A patent is an exclusive right granted for an invention
  - "exclusive right" = a right to exclude others from making, using, offering for sale or selling the invention without the patentee's authorization
- Invention must be new, inventive, applicable industrially
- A patent is **PUBLIC**



Uber patents VR systems for self-driving cars so passengers don't get bored during their ride

- Uber has submitted two patent applications that detail VR technology
- The technology could be used to entertain passengers in self-driving cars
- Uber is among a growing number of tech firms racing to perfect self-driving cars
- The VR technology could induce motion sickness or further isolate passengers

By MAGGIE O'NEILL FOR DAILYMAIL.COM

PUBLISHED: 23:13 BST, 9 March 2018 | **UPDATED:** 23:32 BST, 9 March 2018

European Commission

(19) **United States**

(12) **Patent Application Publication**

Donnelly et al.

(10) **Pub. No.: US 2018/0040162 A1**

(43) **Pub. Date: Feb. 8, 2018**

(54) **VIRTUAL REALITY EXPERIENCE FOR A VEHICLE**

(71) Applicant: **Uber Technologies, Inc.**, San Francisco, CA (US)

(72) Inventors: **Richard Donnelly**, Pittsburgh, PA (US); **David McAllister Bradley**, Pittsburgh, PA (US)

(21) Appl. No.: **15/229,923**

(22) Filed: **Aug. 5, 2016**

Publication Classification

(51) **Int. Cl.**

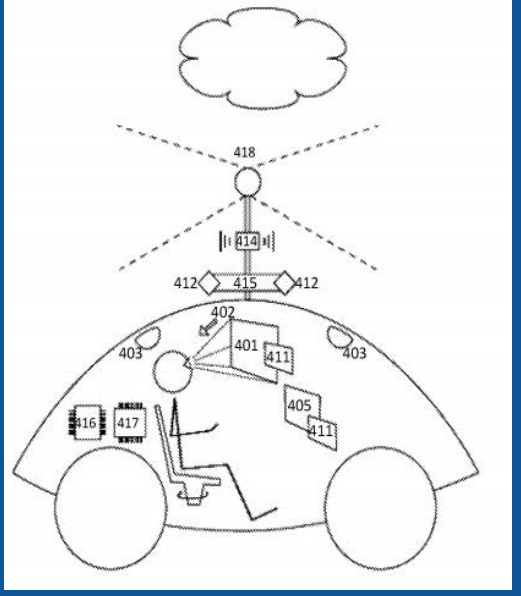
G06T 19/00	(2006.01)
G02B 27/00	(2006.01)
G05D 1/02	(2006.01)
G02B 27/01	(2006.01)

(52) **U.S. Cl.**

CPC ***G06T 19/006*** (2013.01); ***G02B 27/0179*** (2013.01); ***G02B 27/0093*** (2013.01); ***G05D 1/0246*** (2013.01); ***G05D 1/0278*** (2013.01); *G02B 2027/0187* (2013.01); *G05D 2201/0212* (2013.01)

(57) **ABSTRACT**

A virtual reality system is disclosed that provides autonomous vehicle (AV) sensor data to applications such as games and augmented reality overlays to enhance experiences for riders in the autonomous vehicle. Virtual reality headsets offer users unique and interesting experiences, but when used in a changing environment such as a moving vehicle, external stimuli can impair the virtual reality experience. AV sensors can predict these stimuli so that applications can take measures to reduce their impacts on virtual reality experiences. In addition, sensors can include cameras that send live video feeds to virtual reality devices to render improved views of the environment around the AV and of landmarks in a city. Furthermore, virtual reality devices can take advantage of the AV's computing resources in order to offer better performance and more features to applications.



What is claimed is:

1. A virtual reality system for an autonomous vehicle (AV) comprising:

one or more processors; and

one or more memory resources storing instructions that, when executed by the one or more processors, cause the virtual reality system to:

interface with a vehicle control system to receive environmental data while the AV is being operated autonomously by the vehicle control system through an environment;

generate virtual content using at least the environmental data; and

render the virtual content for a virtual display system.

WHAT IS A TRADE SECRET?

- **Confidential** information (+ other conditions)

- **Factual protection** (< nature of the information + way it is handled)

- Can cover a **wide variety** of information:
  - Technical *(Unpatented inventions, Technical drawings, Manufacturing processes, Know-how,…)*
  - Commercial and financial (Consumers' profiles, clients list, Costs/price data,…)

- Protection against unlawful acts (**no exclusive right**)

(3.) COMPLEMENTARY ROLE of trade secrets and IP to protect innovations

- Innovative EU firms use both patents and trade secrets
- Use more trade secrets than patents for protecting innovations
  - by most types of companies
  - in most economic sectors
  - in all EU member states

EUIPO,
July 2017

(4.). TRADE SECRETS THEFTS ARE ON THE RISE

Increased flow of information

- Internet & digitalization
- Open innovation
- Globalization of supply chains
- Mobility of workers (high employee turnover in China)
- Hacking (state sponsored and other forms; increased risks in COVID19 times)

Majority of trade secrets theft by people close to the business

- By (ex)-employees & partners

- **USA**: "*According to an analysis of federal court cases filed over a 58-year period, 85 percent of trade secret theft was committed by employees or business partners*"

https://www.laboremploymentperspectives.com/2015/07/13/thieves-among-us-protecting-trade-secrets-from-employee-theft/

(5.) HOW TO PROTECT YOUR TRADE SECRETS?

Trade secrets protection requires:

(1.) An appropriate **LEGAL FRAMEWORK**

(2.) An **INTERNAL STRATEGY** for the management and protection of trade secrets

5.1. GLOBAL AWARENESS: THE NEED TO REINFORCE THE PROTECTION OF TRADE SECRETS

USA 2016
Defend Trade Secret Act

CHINA 2017, 2019, 2020
Anti-unfair competition law revised in 2017 & 2019
SPC JI 2020 + other texts

UE 2016
Trade Secrets Directive 2016/943

BE 2018
BE law on Trade Secrets

All share the same legal source: the **TRIPS agreement (art. 39)**

IMPROVED LEGAL FRAMEWORK

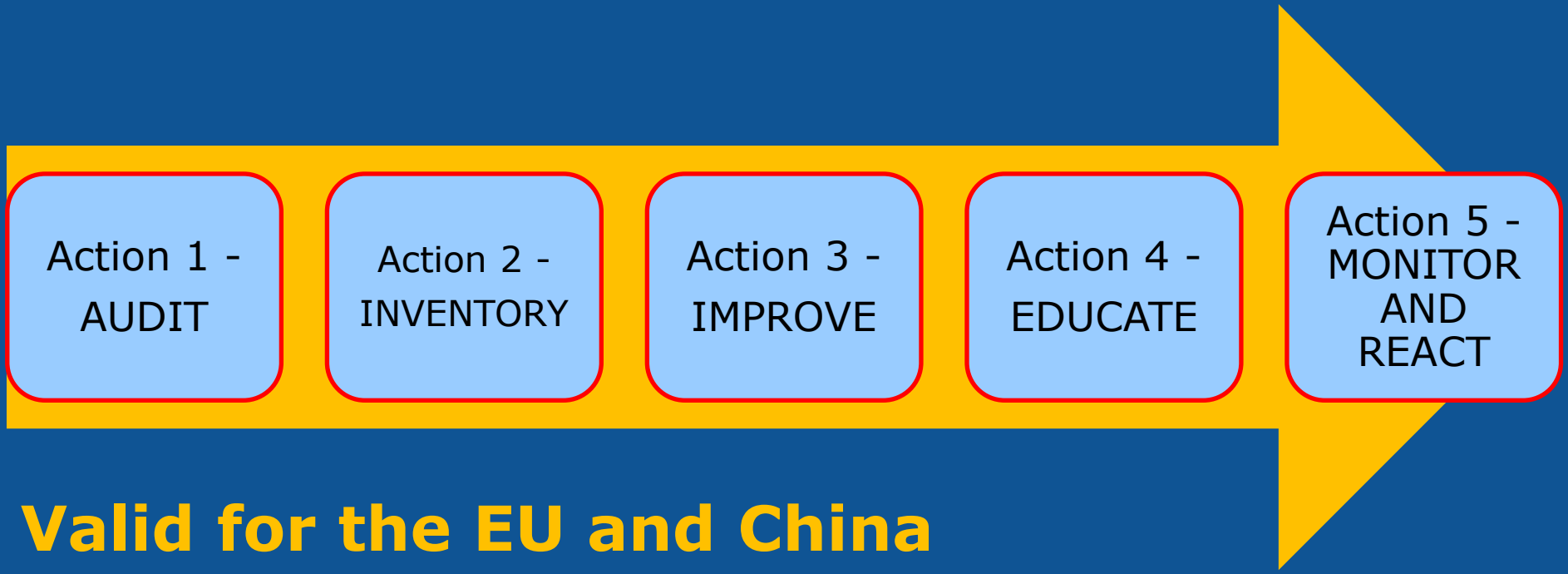
5.2. INTERNAL TRADE SECRETS MANAGEMENT AND PROTECTION STRATEGY

- Most EU businesses lack a clear internal TS management and protection strategy

- **Questions to you**: does your company
  - ✓ *perform trade secrets and IP audit ?*
  - ✓ *have a trade secrets inventory?*
  - ✓ *actively manages access to its trade secrets?*
  - ✓ *implement a TS awareness policy?*
  - ✓ *involves the HR in the trade secrets protection strategy?*
  - ✓ *monitor and enforce its trade secrets ?*

Pro-active TS management is <u>the only way</u> for effective protection

HAVE A TRADE SECRET ACTION PLAN



Valid for the EU and China

PART II – TRADE SECRETS PROTECTION IN CHINA

I. THE LEGAL FRAMEWORK

1. Main Chinese legal framework

➔ **The centrepiece:** Anti-Unfair Competition Law (AUCL – revised in 2017 & 2019)

➔ **Set of other laws and regulations :** PRC contract law (negotiations/tech licences), Company law, labour law, labour contract law, criminal law,…

➔ **Recent trade secrets LEGISLATIVE DYNAMISM**

- Draft Trade Secret Protection Rules released by the State Administration for Market Regulation (SAMR) for public comment – 4.09.2020 (administrative enforcement)
- Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Cases of Disputes over Infringements on Trade Secrets – 10.09.2020 (civil litigation)
- Supreme People's Procuratorate Explanations of Several Issues Concerning the Specific Application of Laws in Deciding Criminal Cases Involving Infringement of Intellectual Property Rights – 13.11.2020 (criminal IP judicial interpretation includes criminal trade secrets)

➔ **Political will to STRENGTHEN TS PROTECTION and enforcement**

2. Centerpiece of Chinese trade secrets legislation: Art.9 AUCL (definition of TS + unlawful acts)

The operator shall not commit the following infringement of trade secrets:

(1) Obtaining the trade secrets of the right holder by theft, bribery, fraud, coercion, electronic intrusion or other improper means;

(2) Disclosing, using or allowing others to use the trade secrets obtained by the previous means;

(3) Disclosing, using or allowing others to use the trade secrets in violation of the confidentiality obligations or in violation of the right holder's requirements for keeping the confidentiality of trade secrets.

(4) Instigating, tempting, and helping others to violate confidentiality obligations or to violate the right holder's requirements for keeping the confidentiality of trade secrets to acquire, disclose, use or allow others to use the right holder's trade secrets.

Natural persons, legal persons and unincorporated organizations other than the operator committing the illegal acts listed in the preceding paragraph shall be deemed to have infringed on trade secrets.

If a third person knows or should know that the employee, former employee or other unit or individual of the trade secret right holder has implemented the illegal acts listed in the paragraph 1 of this Article and still obtains, discloses, uses or allows others to use the trade secret, it shall be deemed to infringe the trade secret.

The term "trade secrets" as used in this Law refers to commercial information such as technical information, business information and etc. that are not known to the public, have economic value and for which reasonable efforts to maintain secrecy have been made by the right holder.

Recent changes in article 9 AUCL

Strengthening of the legal tools

→ *More information may qualify as TS*

→ *More acts qualify as misappropriation*

→ *More people may be held liable*

(1.) Broadened definition of "Trade Secret"

- Now includes all "commercial information"
  (not limited to technical / business information)

(2.) Expanded scope of trade secrets misappropriations

- Hacking (electronic intrusion)
- Indirect infringement (liability of those who contribute to or induce others to commit trade secret theft)

(3.) Clarification of who is liable for misappropriation (Article 9)

- No limitation to "business operators"
- includes individuals, legal persons, and non-legal organizations

3. SPC Judicial interpretation adopted on 10.09.2020

"*Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the* ***Trial of Civil Cases of Disputes over Infringements on Trade Secrets***"

- SPC Judicial interpretation = official interpretation by SPC on the application of certain laws → has legal binding force

- Intends to reflect current judicial practices by providing guidance
  - **To courts** → on how to analyze trade secret infringement cases
  - **To companies** → on how to protect their trade secrets

II. TRADE SECRETS PROTECTION REQUIRES TRADE SECRETS IDENTIFICATION

(1.) WHAT IS A 'TRADE SECRET'?

1. **UNDER CHINESE LAW?** art.9 AUCL

"commercial information such as technical information, business information and etc. that are not known to the public, have commercial value and for which reasonable efforts to maintain secrecy have been made by the right holder"

2. **UNDER EU LAW?** Art.2(1) EU Directive 2016/943

"information which meets all of the following requirements: (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; (b) it has commercial value because it is secret; (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret"

UNDER BOTH CN AND EU LAW

1. **INFORMATION** - Know-how, business and technical information (open notion)

2. **SECRET**
   - "*not known to the public*" - art.9 CN AUCL
   - "*not generally known or readily accessible*" - art.2 EU TS Directive

3. **COMMERCIAL VALUE** because it is secret
   - "*has commercial value*" - art.9 CN AUCL
   - "*has commercial value because it is secret*" - art.2 EU TS Directive

4. **REASONABLE STEPS** to keep it secret
   - "*reasonable efforts to maintain secrecy*", Art.9 CN AUCL
   - "*reasonable steps (…) to keep it secret*" - art.2 EU TS Directive

Requirement #1: INFORMATION

Know-how, business and technical information

- "*commercial information such as technical information, business information and etc.* ", Art.9 CN AUCL
- A **broad & open notion**

- ✓ Algorithms,
- ✓ Analytical data,
- ✓ Data sets,
- ✓ Screen designs prototypes,
- ✓ Source code,
- ✓ Software prototypes,
- ✓ Software development methodologies
- ✓ Sales methods,
- ✓ Consumers' profiles,
- ✓ Supplier info
- ✓ Costs/price data
- ✓ M&A projects,
- ✓ Targeted strategic partnerships
- ✓ Advertising strategies,
- ✓ Know-how,
- ✓ Technical drawings,
- ✓ Unpatented inventions,
- ✓ Manufacturing processes

Art.1 SPC JI of 10.09.2020

TECHNICAL information

Information concerning
- *structure,*
- *raw materials,*
- *components,*
- *formulas,*
- *materials,*
- *samples,*
- *patterns,*
- *propagation material for new varieties of plants,*
- *processes, methods or steps thereof,*
- *algorithms, data, computer programs*

in relation to **technology** and relevant documents

BUSINESS OPERATION information

Information concerning
- *creativity,*
- *management,*
- *sales,*
- *marketing,*
- *financing,*
- *planning,*
- *samples,*
- *bidding materials,*
- *customer information,*
- *data, etc.*

in relation to **business operation** activities

➔ ***Close to any kind of information***

Requirement #2: SECRECY / CONFIDENTIALITY

"***not known to the public***" - art.9 CN AUCL

- "*not widely known and easily accessible to those relevant in the field when the alleged infringing act occurs*" (art.3 SPC JI 2020, // EU definition)

Guidance < SPC JI of 2020

- SECRET: is not known to the public → "*any new information formed by sorting out, perfecting and processing information known to the public and other means*" → (art.4 SPC JI 2020)
- NOT SECRET: Information that is public (art.4 SPC JI 2020)
  - (I) "*is of general knowledge or industry practice in the field*"
  - (II) relates to the product and "*is directly available to those relevant in the field by observing the marketed product*"
  - (III) "*has been publicly disclosed in a public publication or other media outlet*"
  - (IV) "*has been made public through public presentations, exhibitions, etc.; *" [TIP: be careful at trade fairs!]
  - (V) "*is available from other publicly available sources to those relevant in the field*"

QUESTION to ask : What secret information do you have?

- List of (new) information not generally known / not readily accessible / not made public
- *In concreto* analysis

Requirement #3: COMMERCIAL VALUE BECAUSE IT IS SECRET

- "***has commercial value***" - art.9 CN AUCL (// EU definition "*has commercial value because it is secret*", art.2(1)b. TS Directive 2016/943)

- "*practical or potential market value because it is not known to the public*" (art.7 SPC JI 2020)

- Broad notion
  - Information must provide a COMPETITIVE ADVANTAGE because of its secrecy
  - Potential value is (in theory) enough

QUESTION to ask : COMMERCIAL VALUE < SECRECY?

- Does the information bring any economic benefit to your business?
- Would it hurt your business if it was leaked?
- Example of evidence of commercial value: sales invoices showing that use of the trade secret generates profit

REQUIREMENT #4: ADOPT REASONABLE STEPS TO KEEP INFORMATION SECRET

- Need to take proactive measures to protect secrecy (protection is not automatic)
  - Information *"for which reasonable efforts to maintain secrecy have been made by the right holder"* (art.9 AUCL)
  - *"Reasonable confidentiality measures taken by the right holder to prevent trade secret leakage before the alleged infringing act occurs"* (art.5 SPC JI 2020)
- No measures = information is no trade secret → loss/ absence of protection
- The first thing a judge will check (!) - Assessment by the court *"based on the nature of the carrier of the trade secret, the commercial value of the trade secret, the identifiable degree of confidentiality measures, the correspondence level between confidentiality measures and the trade secret, and the right holder's confidentiality intention, etc"* (Art.5 SPC JI 2020 no one size fits all)

WHAT reasonable steps to implement?

Art.6 SPC JI 2020: Non-exhaustive list of confidentiality measures

(I) Signing a confidentiality agreement or stipulating confidentiality obligation in the contract; (contracts)

(II) Providing confidentiality requirements through articles of association, trainings, rules and regulations, written communication, etc., providing confidentiality requirements on employees, former employees, suppliers, customers, visitors, etc. who can access or obtain trade secrets; (training and regulations)

(III) Restricting visitors to or providing segregated management to confidential production and business premises such as factories and workshops; (physical barriers)

(IV) Distinguishing and managing trade secrets and carriers thereof by means of marking, classification, separation, encryption, sealing and restricting the scope of persons who can reached or access, etc.;(access management!)

WHAT reasonable steps to implement?

Art.6 SPC JI 2020: Non-exhaustive list of confidentiality measures

(V) Taking measures of prohibition or restriction of using, access, storage, duplication, etc. on computer equipment, electronic equipment, network equipment, storage equipment, software, etc. that can access or obtain trade secrets.; (IT measures)

(VI) Requiring employees about to leave their jobs to register, return, clear and destroy any trade secrets and the carriers thereof that they have accessed or obtained and to continue to bear the confidentiality obligation; (HR management)

(VII) Other reasonable measures of confidentiality" (open notion)

➔ Useful guidance

What reasonable steps?

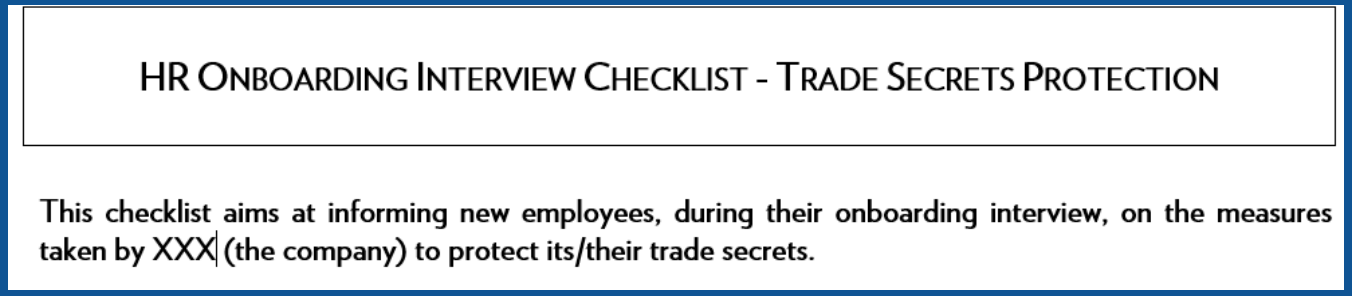
1. Company wide confidentiality policy
   - Employees/Key consultants/service providers/strategic partners
   - Keep track of communication + awareness trainings
2. Access control: restrict to 'need to know basis'
   - If freely accessible in-house → no protection
3. Contracts
   - NDAs + Ad hoc clauses in contracts (employees, consultants, suppliers, partners, etc.)
4. Organizational measures in place
   - Who is in charge?
   - Document marking (« CONFIDENTIAL »)
   - Trade secrets storage/ handling /disclosure

5. Physical security

- Safe lockers / Facilities: area access control
- External measures (security, log book, badges,…) - if freely accessible in-house → no protection - e.g. Huawei

6. Adapt HR policies

- Confidentiality clauses in employment contracts (+ non-compete for key staff)
- Regular training
- Entry and exit briefings with newly hired employee + departing employee



HR ONBOARDING INTERVIEW CHECKLIST - TRADE SECRETS PROTECTION

This checklist aims at informing new employees, during their onboarding interview, on the measures taken by XXX (the company) to protect its/their trade secrets.

7. IT Security

Policy actions

These actions should be carried out by staff responsible for determining the overall cyber security policy.

- ☐ Identify and record essential data for regular backups.
- ☐ Create a password policy.
- ☐ Decide what access controls your users need so they can access only the information and systems required for their job role.
- ☐ Decide what staff need access to USB drives
- ☐ Sign up to threat alerts and read cyber local advice e.g. briefing sheets/threat reports from www.actionfraud.police.uk/signup.
- ☐ Create an inventory of approved USB drives and their issued owners, and review whether the ownership is necessary periodically.

Technical actions

These actions should be carried out by technical staff responsible for the setup and configuration of devices, networks and software.

- ☐ Switch on your Firewall.
- ☐ Install and turn on Anti-virus software.
- ☐ Block access to physical ports for staff who do not need them.
- ☐ Consider making a password manager available to your staff to secure their passwords. Review the star ratings before choosing one from an app store.
- ☐ Ensure data is being backed up to a backup platform e.g. portable hard drive and/or the cloud.
- ☐ Set automated back-up periods relevant to the needs of the business.
- ☐ Switch on password protection for all available devices. Change default passwords on all internet-enabled devices as per password policy.
- ☐ Install and turn on tracking applications for all available devices e.g. Find my iPhone.
- ☐ Enable two-factor authentication for all important accounts (e.g email).
- ☐ Apply restrictions to prevent users downloading 3rd party apps.
- ☐ Install the latest software updates on all devices and switch on automatic updates with periodic checks.
- ☐ Ensure all applications on devices are up to date and automatic updates have been set to download as soon as they are released. Schedule regular manual checks on updates.
- ☐ Set up encryption on all office equipment. Use products such as Bitlocker for Windows using a Trusted Platform Module (TPM) with a PIN, or FileVault (on mac OS).

Training and awareness actions

These actions should be carried out by staff responsible for implementing staff training and awareness. Every member of the team (including board members) needs enough knowledge to understand how cyber security impacts on their area of focus.

- ☐ Provide secure physical storage (e.g a locked cupboard) for your staff to write down and store passwords.
- ☐ Create a Cyber Security training plan that you can use for all staff.
- ☐ Include details of your 'Password' policy explaining how to create a non-predictable.
- ☐ Include how to spot the obvious signs of phishing.
- ☐ Include details of your reporting process if staff suspect phishing.
- ☐ Include details on how your business operates and how they deal with requests via email.
- ☐ Include details of Wi-Fi hotspot vulnerabilities and how to use alternative options (e.g VPN/ Mobile network).

QUESTION to ask: What confidentiality measures are taken today?

An NDA is a good start… but is not enough (!)

- Identify and organize a trade secrets inventory
- Access control - restrict to 'need to know basis'
- Implement legal measures
- Implement physical & organizational measures
- Adapt HR policies
- Implement IT Security measures (!)

→ Important to DOCUMENT your confidentiality measures

III – ENFORCING TRADE SECRETS REMAINS A CHALLENGE

(1.) WHAT IS TRADE SECRETS INFRINGEMENT?

Trade secret infringement - art.9 CN AUCL

- Obtaining trade secrets through theft, bribery, fraud, coercion, electronic intrusion or other improper means

- Disclosing, using, allowing others to use illicitly acquired trade secrets (incl. in breach of confidentiality obligation)

- Second degree infringer (new employer knows or should have known) [TIP: don't become a target yourself]

(2.) REMEDIES

- **Civil enforcement**: **Injunction + Damages**
  - Increased damages for malicious infringement + maximum statutory damages (increased to RMB 5 million; 650.000EUR) (Art.17, 21 AUCL)
  - Specialized IP courts (professionalization / technical advisors / technical advisers)
  - IP Division of SPC (a.o. appeals of patent & technology-adjacent IP judgments before the Supreme People's Court)

  → **A will to improve the system**

- **Administrative / criminal enforcement**: fine + damages

(3.) ENFORCEMENT IS DIFFICULT

- **High evidentiary burden**
  - ✓ Qualification as trade secret?
  - ✓ Evidence of misappropriation (unauthorized use/ disclosure/ acquisition)
  - ✓ Now limited reverse burden of proof in civil litigation (article 32 AUCL) → shift to the defendant if can prove access + high likelihood of infringement
- **Low win rate**
- **Recent legislative changes** → positive signal but effectiveness will depend on how applied and interpreted
  - ✓ Very recent CN case law : SPC judgment of Feb.26, 2021 - highest ever damages for a trade secrets case – Rmb 159 million (+/- 20million EUR)

ENFORCEMENT – Reverse Burden of Proof (1)

- **Article 32.1 of the Anti-Unfair Competition Law:**

  "During civil trials of trade secrets infringement cases, where the preliminary evidence provided by the right holder of trade secrets can prove that it has taken measures to keep the confidentiality of its trade secrets and can reasonably indicate that such trade secrets have been infringed, the alleged infringer shall prove that the trade secrets claimed by the right holder do not fall within the scope of trade secrets as provided in this Law"

- **Requirements**

  i. Information qualifies as trade secret
  ii. Importance of confidentiality measures
  iii. Preliminary evidence and reasonable indication of infringement

  → Defendant to prove information does not qualify as a trade secret
  → Burden of proof regarding state of secrecy shifted to the defendant

ENFORCEMENT – Reverse Burden of Proof (2)

- **Article 32.2 of the Anti-Unfair Competition Law:**

  "Where the right holder of trade secrets provides preliminary evidence that can reasonably indicate that the trade secrets have been infringed and provides one of the following evidence, the alleged infringer shall prove that there is no infringement of any trade secret:
  (1) there is evidence showing that the alleged infringer has access to or opportunities to obtain such trade secrets and the information used by the alleged infringer is substantially identical to such trade secrets;
  (2) there is evidence showing that such trade secrets have been or have the possibility of being published or used by the alleged infringer;
  (3) there is any other evidence showing that such trade secrets have been infringed by the alleged infringer"

- **Requirements**

  i. Preliminary evidence and reasonable indication of infringement
  ii. Elements of **access** (*'alleged infringer has access'*) **+ similarity** (*'substantially identical'*)

→ Burden of proof regarding absence of misappropriation shifted to the defendant (back up claim of independent development with evidence < JI 2020)

CONCLUSION:
What to remember?

TAKE AWAY

1. Trade secrets are widely used (crown jewels of a company)

2. Trade secrets enforcement is challenging in China

- Burden of proof rests on the plaintiff
- Identify your trade secrets (inventory)
- Document all transfers + your confidentiality measures

3. Pay special attention to employees and business partners

4. Prevention is key & pro-active TS management is the only way to protect your trade secrets

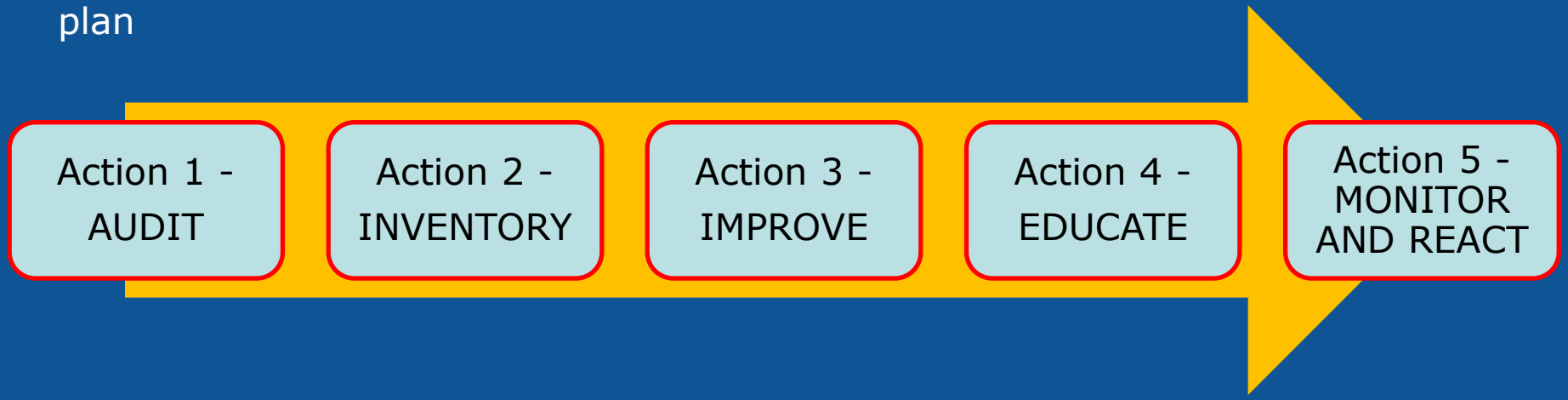
5. Positive legislative changes

- Political will to STRENGTHEN TS PROTECTION and enforcement
- Effectiveness will depend on how applied and interpreted

TAKE AWAY

6. Implement a TRADE SECRET ACTION PLAN

1. AUDIT - Identify trade secrets + protection measures
2. INVENTORY - inventory + trade secrets classification
3. IMPROVE - Review contracts, confidentiality policies & processes, cyber security measures,… → implement "reasonable steps"
4. EDUCATE - Raise awareness among employees, suppliers, biz partners
5. MONITOR AND REACT - Have a person in charge + TS misappropriation action plan



Any question, drop me a line!

Valentin de le Court
IP Partner DALDEWOLF
China IP SME Helpdesk Expert
vdlc@daldewolf.com

Questions?

HELPLINE

free, fast & confidential

3 working days

question@china-iprhelpdesk.eu

CHINA
IP SME HELPDESK

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.

European Commission

Stay connected!

@iprchina

@ChinaIPR-hd

© European Union, 2021. Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU OJ L 330, 14.12.2011, p.39.