

BELGIAN NATIONAL ASSOCIATION FOR THE PROTECTION OF INTELLECTUAL PROPERTY

Litigation, evidence and trade secrets: what's new?

A cross view from practitioners with an insight in recent case law

11 February 2021

Sophie Lens



Dominique Kaesmacher



Liesbeth Weynants



Welcome

Housekeeping rules



The image shows a LiveWebinar interface. The main area displays a presentation slide with a blue header and white text. The slide title is 'Litigation, evidences and trade secrets: what's new?' and the subtitle is 'A cross view from practitioners with an insight in recent case law'. The date '11 February 2021' is also present. The slide includes logos for 'Sophie Lens' (ALTUS), 'AIPPI BELGIUM', and 'Liesbeth Weynants' (HOYNG ROKH MONEGIER). The bottom of the slide says 'Screen Share by IP & Dispute Resolution ALTIUS'. On the right side of the interface, there are three panels: 'Audio & Video' (showing 'There are no active streams'), 'Participants' (listing 'HOST (1)' and 'ATTENDEE (1)'), and 'Chat' (with a 'Send a message...' input field). The top of the interface shows the 'LiveWebinar' logo and the room ID '828-956-580'. A red box highlights the 'Audio & Video' panel, and another red box highlights the 'Chat' panel. Red arrows point from these boxes to the text 'Micro and camera are turned off' and 'During presentation, questions can be submitted via the chat' respectively.

Micro and camera are turned off

No recording please – Slides will be sent afterwards

During presentation, questions can be submitted via the chat



Dominique Kaesmacher

Senior Consultant in IP, Lecturer (UCLouvain), President Belgian Group AIPPI



Sophie Lens

Attorney-at-law, Counsel Altius, member of the AIPPI Standing Committee on Trade Secrets



Liesbeth Weynants

Attorney-at-law, Partner Hoyng Rokh Monegier



Table of content

1. Introduction
2. Time for basics
3. Enforcement challenges
4. Litigation – Best practices
5. AIPPI SCoTS update



1

Introduction

2020 – A peculiar year...

- To a world of
 - ◆ Globalisation (stronger competition)
 - ◆ Omnipresent devices (personal and company-owned computers, smartphones, tablets), multiple networks & systems (DMS, email)
 - ◆ Sharing & "open mode" (open source, joint development)
 - ◆ External data storage (cloud)
 - ◆ Organised crime & espionage, hacking, cyber-attacks
 - ◆ Job mobility (reduced loyalty)

- 2020 added
 - ◆ Large scale telework
 - ◆ Digital explosion (meetings, conferences, tools)

→ Data and information risks – Data more vulnerable than ever

What when a breach occurs?

■ Before 2018

- ◆ No specific legal framework
- ◆ Typical issue between employer/employee
- ◆ Unfair market practices (Art. VI.104 CEL) + TRIPS (Art. 39)
- ◆ Litigation: Labour / Criminal Courts (+ Company Courts)
- ◆ Often unsatisfying outcomes

■ Since 2018

- ◆ Specific Trade Secrets Act (30 July 2018, entered into force on 24 August 2018)
- ◆ Company Courts (!) (other fora remain available)
 - At the seat of 1 of the 5 Courts of Appeal
 - Even if the parties are not companies
 - Irrespective of the amount at stake
- ◆ Growing body of positive case law

Trade secret = Intellectual capital → "Company Gold"

- Advantages
 - ◆ Potentially unlimited duration
 - ◆ No disclosure of details (<-> patents)
 - ◆ "Universal": for each type of knowledge or information
 - ◆ Informal: immediate protection without formalities
 - ◆ Easy: no strict set of (validity) requirements
 - ◆ Relatively cheap: no substantial investments / costs (safe: internal organisation and measures)
- BUT: Issues re EVIDENCE
 - ◆ Proving existence / validity of trade secret and/or misappropriation = complex
 - ◆ Disclosure issues in litigation setting



2

Time for basics

Trade secret = information [A] that

- **is secret [B]**
- **has commercial value [C]** because it is secret
- **has been subject to reasonable steps [D]** under the circumstances to keep it secret

= Cumulative conditions

A. "Information" =

- Any kind of information

"It is important to establish a homogenous definition of a trade secret without restricting the subject matter to be protected against misappropriation" (Recital 14 Trade Secret Directive 2016/943)

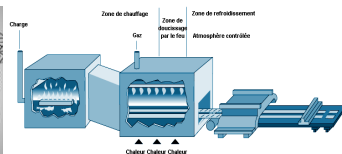
- Regardless of mode of expression or medium

Technical

Unpatented / unpatentable inventions
Algorithms
Improvements or modifications of patented inventions
(Production) processes / methods
Recipes
Chemical formulas
Plans, drawings, schematics

Commercial

Prices / Discount schemes
Information on business strategy
Customer / Supplier lists
Offers to customers
Contracts used in business
Organization charts
Satisfaction survey
Turnover / Margins



B. "Secret" =

"It is not, as a body or in the **precise configuration and assembly** of its components [1], **generally known** among or **readily accessible** [2] to **persons within the circles** that normally deal with the kind of information in question [3]" [4]

[1] Combination of elements must be secret

[2] "Generally" = more than a few people

"Readily accessible" = materially, intellectually and legally

Presence on the Internet ≠ necessarily "readily accessible"

[3] Reference framework = "interested circle"

[4] NOT required that information is used/applied

Parallel with "novelty" and "inventive step" in patent law

B. "Secret" =

Case-law examples

- ☒ General accounting data fed into an online application
"Data is also included in invoices sent to clients and can easily be reconstructed by competitors" – Antwerpen Commercial Court (Pres.), 16 October 2019

- ☒ Specific way of connecting / assembling standard machines in a manufacturing line
Antwerpen Commercial Court, 9 mei 2019

C. "Commercial value" =

- Value because secret
- Information likely to improve competitive position (→ intrinsic or sentimental value is NOT sufficient)
- Potential or real value
- Indicators – Judge's appreciation on a case-by-case basis:
 - ◆ Competitive advantage(s) due to secrecy
 - ◆ R&D costs to obtain information
 - ◆ Investments made to keep information secret
 - ◆ Licenses granted / Price paid to obtain right to use information
 - ◆ Information difficult to find / reproduce, etc.

C. "Commercial value" =

Case-law examples



Manufacturing line

"Unique set-up of manufacturing line and secret character of detailed information in that respect entails commercial value" – Antwerpen Commercial Court, 9 May 2019



Enhanced extraction method

Brussels Commercial Court, 12 March 2020



General accounting data fed into an online application

Reminder that the "value" must exist because of information is secret – Antwerpen Commercial Court (Pres.), 16 October 2019



Inbox with "thousands of e-mails"

"Internal emails wherein the holder of the alleged trade secret expresses his opinion on a competitor and its products, do not have commercial value even in the hands of the competitor concerned" – Brussels CoA, 27 August 2020

D. "Reasonable steps" =

- To keep information secret (→ **Active** protection policy – "best effort")
- By trade secret holder
- "Reasonable under the circumstances" – Indicators:
 - ◆ Nature of information to be protected
 - ◆ Size / Financial means of undertaking
 - ◆ Sector of activities
 - ◆ Reasonable costs
 - ◆ Impact of measures (no undue disruption of work)
- Trade secret strategy
 - ◆ Identification / Classification
 - ◆ Effective protection measures
 - Contractual – **NDA, Confidentiality clause**, Non-compete clauses, etc.
 - Digital – Encryption measures, Authentication right, Access restriction, Network inaccessibility, etc.
 - Physical – "Stamping", securing all or part(s) of building, "need-to-know", identification badges, etc.
 - ◆ Organization of protection
 - Policies – re IT, copying/printing/destroying documents, etc.
 - Training – Entry interview, exit interview, etc.

D. "Reasonable steps" =

Case-law examples

✓ Technical product information

Reasonable measures are "obvious technical and legal measures to shield information from interested parties for whom it is not intended" – e.g. ICT infrastructure with limited access, use of secure login and password, contractual confidentiality obligation – Ghent Commercial Court, 24 June 2020

✓ Set-up of production lines

Sufficient reasonable measures, even if shown that alleged infringer (independent service provider) was NOT bound by any written agreement / confidentiality obligation – Other measures sufficient (e.g. data security on servers, users' limited access rights according to their tasks within the company + "stamped" documents) – Antwerpen Commercial Court, 9 May 2019, TBH, 2020, p.382

"Trade secret holder" =

"**Any** natural or legal person **lawfully controlling** a trade secret"

→ Broad: License holders, lawful acquirer by reverse engineering

"Infringing goods" =

"Goods of which the design, characteristics, operation, production process or placing on the market **benefit significantly from** trade secrets which have been unlawfully acquired, used or disclosed"

"Infringer" =

- "Direct" infringer
 - "Any natural or legal person who has **unlawfully** acquired, used or disclosed a trade secret"
- "Indirect" infringer (Art. XI.332/4, §4 CEL)
 - ◆ Third-party who knew or should have known that secret information is the result of unlawful acts (use, disclosure)
 - ◆ Actual knowledge or suspicion of third-party is sufficient – NO active unlawful act required
- Importer of "infringing goods"

What is considered "infringing"?

Starting point: Trade secret \neq IP right

- Lawfully obtained information can be used and disclosed, EVEN IF regarded as a trade secret by a third-party
- SOLELY protection against **unlawful** acquisition / use / disclosure
- NOT possible to prohibit **lawful** acquisition / use / disclosure

Who bears the burden of proof?

- **Principle** = Claimant → Trade secret holder must prove:
 - ◆ Existence of "trade secret"
 - ◆ Unlawful acquisition, use and/or disclosure
 - ◆ Reality / extent of suffered damage (if damages are claimed)
- Essential for trade secret holder to **DOCUMENT** not only the **information** considered to be a trade secret, but also the **measures** taken to keep it secret
- **Temperament** – Parties (incl. defendant) must loyally contribute to the burden of proof
 - ◆ “Shared” burden of proof insofar trade secret holder is required to provide “negative evidence”

e.g. If claimant makes it plausible that information is "secret", judge may invite defendant to prove that, to the contrary, information is "generally known" and/or "easily accessible" – Brussels Commercial Court, 12 March 2020 (also see Antwerpen Commercial Court, 9 May 2019)
 - ◆ Increased tendency to share burden of proof depending on acts performed by alleged infringer *in tempore non suspecto*
 - Recognition of secret character of the claimant’s know-how in a letter – Brussels Commercial Court, 12 March 2020
 - Claim that information was known and available on internet does not stand up to scrutiny as it has been proven that defendant took data from the claimant’s database and copied it to USB key – Ghent Commercial Court, 24 June 2020, unpublished

Degree of precision required to prove "secret"

- "Majority" trend: necessary to identify precisely which document, or even which information in said document constitutes the trade secret
 - ◆ Antwerpen Commercial Court, 26 March 2020
 - ◆ Corr. Leuven, 12 November 2019
- BUT: some judges agree to qualify a whole set of documents as trade secrets without need for further clarification
 - ◆ Antwerpen Commercial Court, 9 May 2019



3

Enforcement challenges

Protection of trade secrets & evidence in litigation setting

- **Confidentiality in legal proceedings in which trade secret is involved** (Art. 871*bis*, §1 CCP)

Prohibition of use or disclosure for "parties, their lawyers or other representatives, magistrates and judicial staff, witnesses, experts and any other person who, through their participation in legal proceedings or through their access to the documents forming part of such proceedings, has become aware of an (alleged) trade secret which the judge, at the reasoned request of an interested party or on his own initiative, has classified as confidential"
- **Confidentiality measures** (Art. 871*bis*, §2 CCP)
 - ◆ Restrict access to documents
 - ◆ Restrict access to hearings
 - ◆ Non-confidential versions of judgments

→ Balancing of interests (fair trial / legal interest / damage - Art. 871*bis*, §3 CCP)
- **Fine** (500 to 25.000 €) – Penalty payment (Art. 1385*bis* CCP)

Protection of trade secrets & evidence in litigation setting

- Exceptional set of measures → Some previously unknown in Belgium
- Effectively applied in practice (!)
 - ◆ Confidential + non-confidential version of decision
 - *Solvay / Mr. B.* – see below
 - ◆ Confidentiality club
 - *Tecnicas Reunidas / Yara Belgium* – see below
 - *Solvay / Mr. B.* – see below

Protection of trade secrets & evidence in litigation setting

→ Composition of confidentiality club may lead to "case within case" – Examples:

- ◆ Brussels Company Court, 31 October 2019, *FN/Secubit*
 - Legally binding mandate NOT required for membership of confidentiality club
 - Patent attorney with expert knowledge of patent in suit NOT automatically excluded
- ◆ Antwerp CoA, 13 May 2020, *Melis Events/Lilse Bergen*
 - Law prescribes "at least one natural person of each party"
Court allows "attorneys only" as "lack of appointment of a natural person for one of the parties may not lead to paralyze the proceedings"
 - (!) Court excludes online Webex hearing (even if mandatory / available pursuant to COVID-measures) to safeguard trade secrets

Gathering and preserving evidence of misappropriation

- NO "descriptive seizure (beschrijvend beslag/saisie-contrefaçon)" (!) (despite strong inspiration from IPR Enforcement Directive 2004/48)
- Ratio
 - ◆ Search and seizure orders not explicitly in Trade Secret Directive 2016/943
 - ◆ NO new intellectual property right
 - ◆ Extension to trade secrets could give rise to abuse ("fishing expeditions") according to Belgian legislator

Gathering and preserving evidence of misappropriation

If no "saisie-contrefaçon" available, **how to prove** that trade secret was:

- Unlawfully acquired / used / disclosed by the "infringer"?
- Used for developing / producing "infringing goods"? → Difficulty to prove that...
 - ◆ ...allegedly infringing goods "**benefit significantly from**" trade secret...
 - ◆ ...trade secret information has become unlawfully available...
 - ◆ ...trade secret has been used unlawfully......by just examining a product (// process patent infringement)

Gathering and preserving evidence of misappropriation

→ Description / seizure of evidence (Art. 584, §3 CCP)

- Alternative to "descriptive seizure" to gather/preserve evidence
- "Absolute necessity" or "extreme urgency" required
- Decision in a few days (to be followed up by an *inter partes* action)
- Bailiff + court-appointed expert carry out the *ex parte* measures
- Expert report with evidentiary exhibits within a time period set in the court order
- Motion to set aside the *ex parte* order, in full or in parts, can be filed by any interested party
- Court can set a deadline for main infringement action

Admissibility of evidence

Typical example = ex-employee's e-mail correspondence

- GDPR issues
 - ◆ Evidence obtained with disregard of GDPR
 - Not *in se* unlawful (majority case law / doctrine)
 - But can be unlawful depending on circumstances
 - ◆ Submitting ex-employee's e-mails *can* constitute GDPR violation → Unlawfully obtained evidence
 - ◆ Proportionality test
- Antigone case law (Cass., 10 March 2008, No. S.07.0073.N.)
 - ◆ Even if evidence was found to be "unlawfully obtained"
 - Only inadmissible if: "the unlawfulness of its acquisition: (i) makes it unreliable, (ii) jeopardizes the right to a fair trial, or (iii) follows from violation of rule subject to nullity" ("op straffe van nietigheid voorgeschreven")
 - Court does not *have to* reject evidence (most courts even accept that evidence may be unlawful in itself)
 - ◆ Case law applied by majority lower courts (recent trend in less flexible approach towards unlawfully obtained evidence)



4

Litigation – Best Practices

Overview

- *Ex parte* – Description / seizure of evidence
 - ◆ CoA Ghent, 4 April 2016, *Umicore / EL Research Consultancy*
 - ◆ Brussels Company Court, 9 September 2020, *Tecnicas Reunidas / Yara Belgium*
- *Inter partes* – (Accelerated) main action
 - ◆ Brussels Company Court, 12 March 2020, *Solvay / Mr. B*

CoA Ghent, 4 April 2016, *Umicore / EL Research Consultancy*

- Facts: ex-employee taking secret Umicore information to Turkish competitor
- Prior to adoption of Belgian Trade Secrets Act: "descriptive seizure" not accepted hence:
 - ◆ *Ex parte* request (extreme urgency/absolute necessity)
 - ◆ For descriptive + protective measures & expert appointment: private house search re all communication and info re Turkish competitor re products at stake, expert filters
- *Ex parte* request
 - ◆ Granted & upheld (even broadened) in third-party opposition
 - ◆ Dismissed on appeal ("too broad" & "amounting to a private house search" & "fishing with an excessively large net") + Confirmed by the Supreme Court
- Key take-aways
 - ◆ Lost for lack of evidence
 - ◆ Required:
 - Detailed description of relevant information &
 - Clear and targeted definition of scope of expert's mission

Brussels Company Court, 9 September 2020, *Tecnicas Reunidas / Yara Belgium* (ongoing)

- Post-adoption of Belgian Trade Secret Act: "descriptive seizure" (explicitly / currently) not provided by law
- Alternative approach: *ex parte* request (extreme urgency/absolute necessity) for descriptive + protective measures & expert appointment
- *In casu*
 - ◆ ***Ex parte* request**
 - Partially granted
 - Collection / seizure of evidence by expert – ✓
 - Selection / examination of relevant evidence – ✗ → to request in *inter partes* proceedings
 - Upheld in third-party opposition proceedings – Appeal pending
 - ◆ Follow-up ***inter partes* cease-and-desist action**
 - Second expert appointed as a preliminary investigation measure

Brussels Company Court, 9 September 2020, *Tecnicas Reunidas / Yara Belgium* (ongoing)

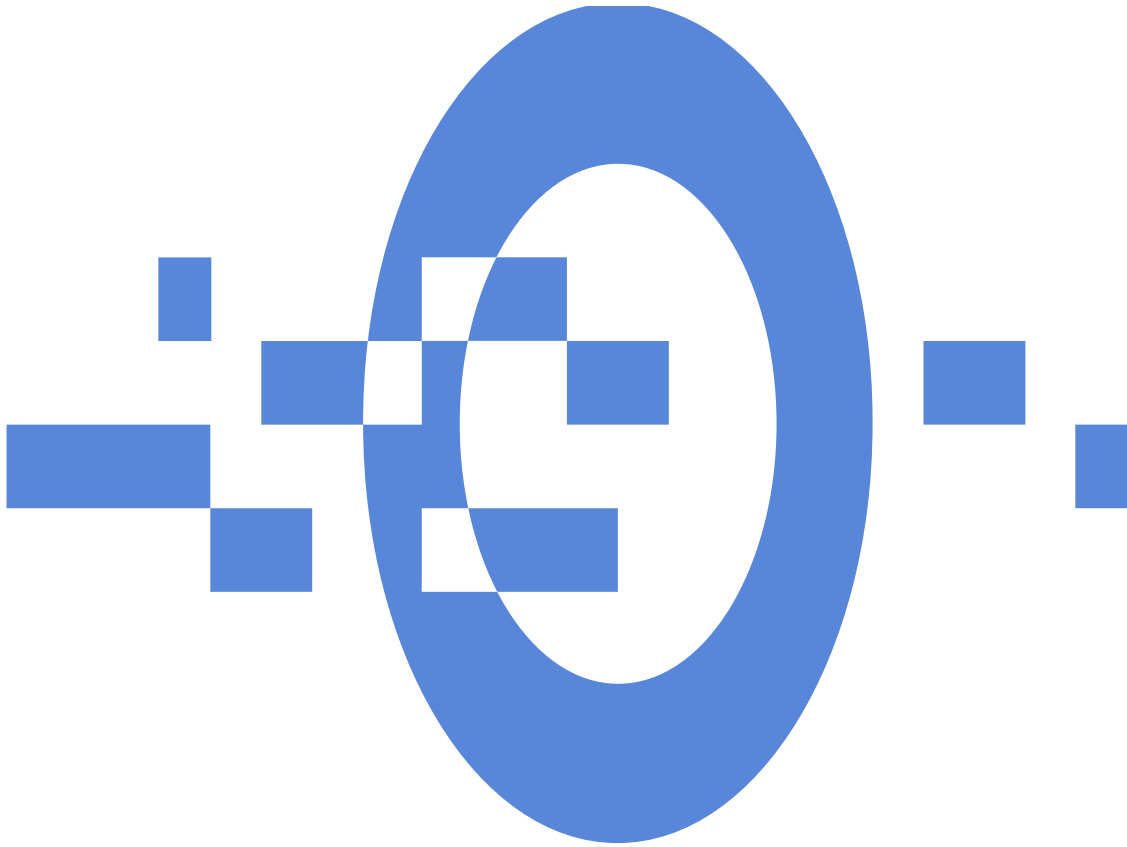
- Key take-aways
 - ◆ Detailed description of relevant information
 - ◆ Clear and targeted definition of scope of expert's mission
 - ◆ Two-step approach in order to "circumvent" exclusion of "descriptive seizure"
 1. Expert for seizure and collection of evidence
 2. Expert for description and analysis of evidence (+ expert report)

Brussels Company Court, 12 March 2020, *Solvay / Mr. B.*

- Post-adoption of Belgian Trade Secret Act
- Cease-and-desist action against former employee based on Solvay's trade secrets
- Procedural aspects – Mutual request for confidentiality of proceedings granted
 - ◆ "Confidentiality club" for access to submissions and exhibits
 - ◆ Limited access to hearing
 - ◆ Confidential and non-confidential version of judgment

Brussels Company Court, 12 March 2020, *Solvay / Mr. B.*

- *In casu*: cease-and-desist action granted based on multiple indications of unlawful use / disclosure of Solvay's trade secrets
- Key take-aways
 - ◆ Interesting point re "burden of proof" (cf. "shared " burden of proof)
 - ◆ Increasing expertise & willingness of Belgian courts re trade secrets



AIPPI

5

AIPPI SCoTS update

Internal organization

- SCoTS =
 - ◆ 32 members from 20 countries (principle / country: 2 lawyer members + 1 extra "in house")
 - ◆ 36 observers from 19 countries (unlimited)
- Subgroups
 - ◆ Company Trade Secrets Policies (1 "head" + members)
 - ◆ Cross Border issues (1 "head" + members)
 - ◆ Implementation of EU Trade Secrets Directive (1 "head" + members)
 - ◆ Trade Secret in Court Proceedings and Preservation of Evidence (1 "head" + members)
- Meetings – Calls
 - ◆ SCoTS: every 2 months
 - ◆ Subgroups: case by case

Activities

■ 2019-2020

- ◆ Suggestion for panel session on "Trade secret with employees on the move" for **Annual Congress 2020** (cancelled due to pandemic)
- ◆ **WIPO Symposium on Trade Secrets and Innovation** (Geneva, Switzerland, November 2019) – SCoTS moderated a panel re "Integration of Trade Secrets in Business Strategies and Knowledge Management" (see Report of March 2020 – https://www.wipo.int/meetings/en/doc_details.jsp?doc_id=474461)
- ◆ **Artificial Intelligence Colloquium** (Torino, Italy, March 2019) – SCoTS spoke during panel re "AI in the Non-Patent IP Landscape", and made a presentation re "AI and IP – The trade secrets arena" (see <https://ficpi.org/library/presentations/5230>)
- ◆ **AI consultation from USPTO** (January 2020) – SCoTS contributed to reply input from AIPPI (see "General News Stories" @ <https://aippi.org/news/aippi-in-the-news/>)
- ◆ **Annual World Congress 2020** (online) – SCoTS organized, moderated and/or participated to
 - Virtual Roundtable re "Trade Secret: Hot Topics" (7/10)
 - Panel Session re "Enforcement of Trade Secrets: The Practical Realities" (12/10)
 - Panel Session re "Protecting Confidentiality during Litigation: Trade Secrets and More" (13/10)

Activities

- 2021-2022
 - ◆ Panel suggestions for Annual **World Congress** (2021 or 2022)
 - "Trade secret with employees on the move"
 - "Practices and management of trade secrets" (in collaboration with IHC)
 - ◆ **Webinar** (TBD)
 - ◆ **Study Question** suggestion for 2022 re "Trade Secret Protection in Court Proceedings" (complement to Q247, 2015)

Projects in the pipeline

- Subgroup – Trade Secrets in Court Proceedings and Preservation of Evidence
 - ◆ Study question drafted and suggested for 2022
 - ◆ Drafting table on trade secrets issues encountered in court proceedings in various countries (incl. collection of cases with principle trade secrets issues)

- Subgroup – Company Trade Secrets Policies
 - ◆ Drafting table on Company Trade Secrets Policies and Best Practices in various countries (in collaboration with IHC)
 - ◆ Drafting of do's and don'ts list and check-list to help companies to set up a trade secret policy (based on above table)
 - ◆ Drafting recommendation report for companies based on the tables and spreadsheets drafted in 4 subgroups
 - ◆ Planning panel for Annual Congress 2021 re "Practices and management of trade secrets" (in collaboration with IHC)

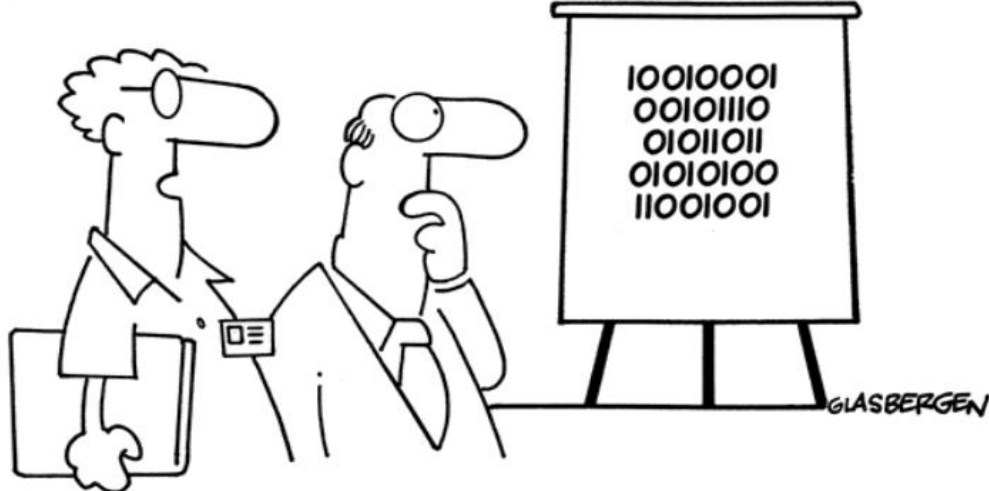
Projects in the pipeline

- Subgroup – Cross Border Issues
 - ◆ Survey on key cross-border harmonization issues
 - ◆ Preparing summary report on cross-border survey
 - ◆ Preparing recommendation report based on global view of survey results
- Subgroup – Implementation of EU Trade Secrets Directive
 - ◆ Updating and enlarging of EU Trade Secret Directive Implementation Document (initially prepared for London 2019)
 - ◆ Preparing a document on the synergies between EU Trade Secrets Directive subgroup and Cross-Border subgroup
 - ◆ Study question drafted and suggested for 2022
- SCoTS
 - ◆ Discussion with AIPPI to optimize use of results of projects carried out within SCoTS and make them as accessible as possible to AIPPI members
 - ◆ Preparation of repository of principle decisions on trade secrets throughout the world

Any questions?

LiveWebinar ID: 828-956-580

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



“We’ve devised a new security encryption code.
Each digit is printed upside down.”

Screen Share by IP & dispute Resolution ALTIUS

Made with ♥ by LiveWebinar

Audio & Video

There are no active streams
Successfully connected to media server
You are not allowed to start your camera or microphone

Participants

HOST (1)

IP & dispute Resolution ALTIUS
Brussels Belgium

ATTENDEE (1)

IP & dispute Resolution...
Brussels Belgium

Chat

Send a message...

Feedback

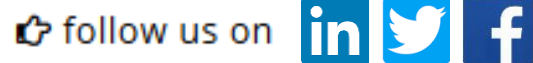
Option 1 – Click on the micro icon next to your name in the list of attendees and wait to be given the floor

Option 2 – Type your question in the chat

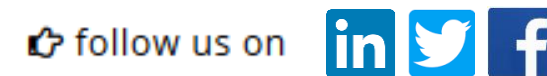
Thank you!



Sophie.Lens@altius.com
www.altius.com



Liesbeth.Weynants@hoyngrokh.com
www.hoyngrokhmonegier.com



- Employment relationship

- ◆ Article 17, 3° of Belgian Act on Employment Contracts

The employee has an obligation, both during the contract and after its termination, to refrain from revealing "any trade secrets, business secrets or secrets in connection with personal or confidential matters of which he may become aware in the course of his work"

- ◆ Article 309 of the Criminal Code

"Anyone who has maliciously or deceptively communicated the 'secrets of the factory' [more restrictive than 'trade secrets'] in which he has been or is still employed shall be punished by imprisonment from three months to three years and with a fine from 50 € to 2.000 €"

- **General provisions** (trade secrets holder – third parties)
 - ◆ Article VI.104 of the Code of Economic Law – Unfair market practices

"Is prohibited, any act contrary to honest market practice by which a undertaking prejudices or may prejudice the professional interests of one or more other undertaking"
 - ◆ Article 1382 Civil Code – Extra-contractual liability

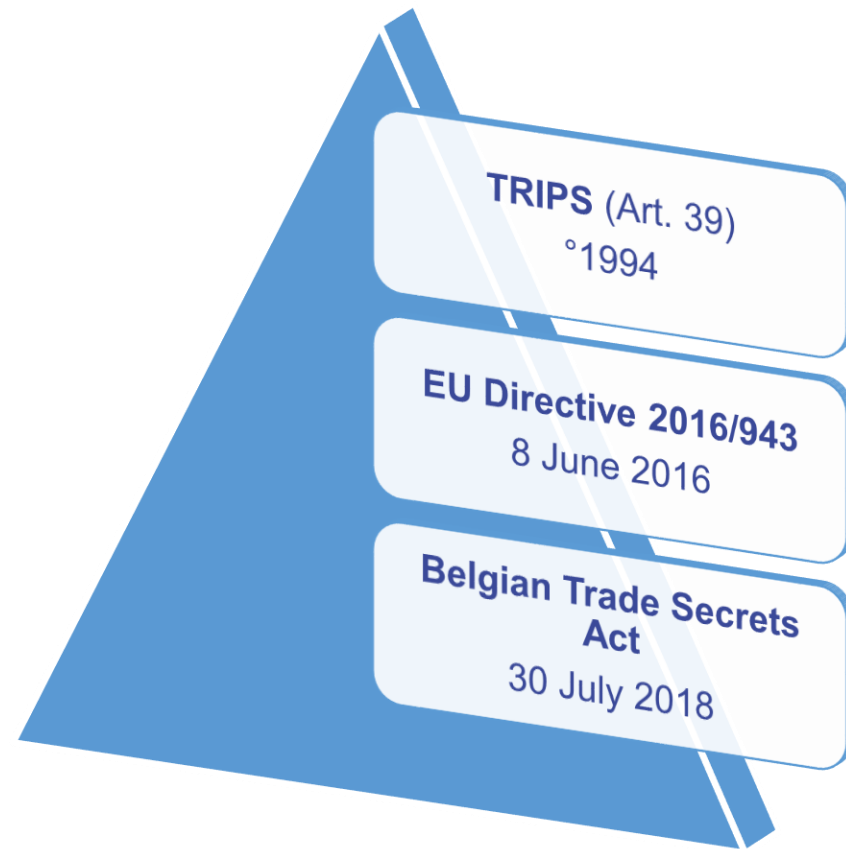
"Any act of man, which causes damage to another, obliges the one by whose fault it occurred, to make reparation"
 - ◆ Article 491 Criminal Code – Abuse of trust

"Anyone who fraudulently misappropriates, or dissipates to the prejudice of another person, money, goods, bills, receipts, writings of any kind containing or operating an obligation or discharge, and which were handed over to him on condition that he returns them or uses them for a specific purpose or use, shall be punished by imprisonment of one month to five years and a fine of 26 € to 500 €"

- Article 39 of the TRIPS-agreement

"Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their consent in a manner contrary to honest commercial practices¹⁰ so long as such information:

- a) 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) has **commercial value** because it is secret; and
- c) has been subject to **reasonable steps** under the circumstances, by the person lawfully in control of the information, to keep it secret"



- Ratio of legislative action
 - ◆ More uniform and streamlined approach to prevent misappropriation of confidential information
 - ◆ Protection was:
 - Fragmented
 - Not harmonized
 - Not adapted to increasing importance and risks

Unlawful acts

ACQUISITION	USE	DISCLOSURE
<ul style="list-style-type: none"> • unauthorized access/appropriation/copying of documents, objects, materials, substances or electronic files that contain the trade secret or from which it may be inferred • any other conduct contrary to fair market practices <p>(Art. XI.332/4, §1 CEL)</p>	<p>by anyone who:</p> <ul style="list-style-type: none"> • has unlawfully acquired trade secrets (e.g. theft, bribery) • breaches a confidentiality agreement or any other obligation not to disclose the trade secret • breaches contractual or any other obligation to limit the use of trade secrets <ul style="list-style-type: none"> • carrying out commercial acts (production, offering or placing on the market, importation, exportation, storage) in relation to "infringing goods" (art. 17/1, 4° CEL) – know or ought to have known is sufficient. 	<p>(Art. XI.332/4, §4 CEL)</p>
<p>by a third party who <u>knew or should have known</u> that the secret information is the result of unlawful acts (use, disclosure); → actual knowledge or suspicion of third party acquirer is sufficient – NO active unlawful act required</p> <p>(Art. XI.332/4, §3 CEL)</p>		

Lawful acts

ACQUISITION	USE	DISCLOSURE
<ul style="list-style-type: none"> independent discovery or creation; observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret ("reverse engineering"); exercise of the right of workers or workers' representatives to information and consultation in accordance with European Union law, national laws and practices; any other practice in conformity with honest commercial practice. <p>(Art. XI.332/3, §1 CEL)</p>	<ul style="list-style-type: none"> prescribed by or in accordance with a provision of EU or national law link with art. XI.332/2 CEL - safeguard clause on fundamental rights 	<p>(Art. XI.332/3, §2 CEL)</p>

Exceptions

Protection of trade secrets must not impede legitimate acquisition, use and/or disclosure of information in following cases (Art. XI.332/5 CEL)

- Application of fundamental rights (e.g. freedom of expression)
- General public interest (e.g. whistleblowers, investigative journalists)
- Legitimate interest recognized by law