

Intellectual Property Teaching Kit

IP Advanced Part II

Trade marks, copyright,
trade secrets and know-how

**Trade secrets
and know-how**



IP Advanced Part II

Trade secrets and know-how

Part of the IP Teaching Kit

Table of contents

Content	Slide	Page
Introduction		4
About IP Advanced Part II		5
IP Advanced Part II	1	6
TRADE MARKS		
1 Trade marks		9
Slides	2 – 31	11
2 Trade mark case study		83
Slides	32 – 50	85
3 Trade mark exercises		125
Slides	51 – 74	127
COPYRIGHT		
4 Copyright		179
Slides	75 – 102	181
5 Copyright case study		239
Slides	103 – 124	241
6 Copyright exercises		287
Slides	125 – 149	289
TRADE SECRETS AND KNOW-HOW		
7 Trade secrets and know-how		341
Slides	150 – 180	343
8 Trade secrets and know-how case study		407
Slides	181 – 192	409
9 Trade secrets and know-how exercises		435
Slides	193 – 223	437
Terms of use		501
Imprint		502

Introduction

Intellectual property reaches into everyone's daily lives. A basic awareness and understanding of IP is therefore essential for today's university students, who are the engineers, researchers, lawyers, politicians and managers of tomorrow.

It is vital that students become acquainted with elementary aspects of IP, so that they can benefit from it fully in whatever career they eventually pursue. Students and universities should be aware too of how they can utilise the incomparable wealth of technical and commercial information to be found in IP documentation, and understand the need for universities to convert their research into IP rights, manage their IP portfolios and engage in technology transfer to industrial partners for value creation and the benefit of society as a whole.

Last but not least, students and universities should be aware of the consequences of failing to protect IP assets correctly, including the risk of reverse engineering, blatant copying and even industrial espionage.

This is where the IP Teaching Kit comes in. Produced by the European Patent Academy in association with the Academy of the EU's Office for the European Union Intellectual Property Office (EUIPO), the IPTK is a collection of materials — including PowerPoint slides, speaking notes and background information — which can be used to put together lectures and presentations on all kinds of IP, including patents, utility models, designs, trade marks, copyright, trade secrets and know-how. The materials can be tailored to the background of the students (science or engineering, business or law), their knowledge of the topic, the time available and their learning objectives.

IP Advanced Part II is the third part of the kit to be produced, following on from the introductory IP Basics and IP Advanced Part I. It contains the tools and information you need to deliver more in-depth lectures on the main aspects of trade marks, copyright, trade secrets and know-how.

With the IP Teaching Kit you have at your disposal an extensive set of freely accessible, professional teaching materials which represents one of the most comprehensive IP teaching resources in the world.

About IP Advanced Part II

IP Advanced II is part of the IPTK. It has been designed for teachers of students with little prior knowledge of intellectual property (IP), in order to provide them with advanced teaching material about trade marks, copyright, trade secrets and know-how.

In addition to the main presentations, IP Advanced Part II contains case studies and exercises on trade marks, copyright, trade secrets and know-how that demonstrate their use in the real world.

IP Advanced Part II consists of ready-made PowerPoint slides with speaking notes and additional background information. The speaking notes can be read out as they stand. The background information provides additional details which will help you prepare for the more advanced questions that students might have. It is not intended for this information to be included in the lecture.

For online access to the extensive IPTK collection, plus updates and further learning opportunities, go to www.epo.org/learning-events/materials/kit.html where you will also find a tutorial for teachers and lecturers.

Slide 1
IP Advanced Part II

Title slide



IP Advanced Part II

Intellectual Property Teaching Kit

7 Trade secrets and know-how

Trade secrets and know-how

List of slides

Slide 150	Trade secrets and know-how
Slide 151	Contents
Slide 152	Trade secrets
Slide 153	What is a trade secret?
Slide 154	Summary – trade secrets
Slide 155	Know-how
Slide 156	What is know-how?
Slide 157	Common features of trade secrets and know-how
Slide 158	How to protect trade secrets and know-how rights
Slide 159	It must not just BE secret – it must be KEPT secret
Slide 160	What is confidential information?
Slide 161	What in law is NOT confidential?
Slide 162	Confidentiality pros and cons
Slide 163	How to disclose information confidentially
Slide 164	Constantly review your trade secrets and know-how
Slide 165	Practical steps to maintain confidentiality
Slide 166	How to enforce trade secrets and know-how
Slide 167	Contracts are EVERYTHING
Slide 168	Restrictive covenants
Slide 169	Typical protection clauses in restrictive covenants
Slide 170	Non-disclosure agreements (NDAs)
Slide 171	Enforceability – reliance on contracts
Slide 172	Know your IP rights
Slide 173	How to extract value from trade secrets and know-how
Slide 174	Patents or trade secrets?
Slide 175	Ways of ‘working’ trade secrets and know-how
Slide 176	All IP – registrable or non-registrable – has value (I)
Slide 177	All IP – registrable or non-registrable – has value (II)
Slide 178	Common to all IP
Slide 179	Is any one form of IP right more important than another?
Slide 180	Facts of enforcement in Europe

Slide 150

Trade secrets and know-how

TRADE SECRETS AND KNOW-HOW

Intellectual Property Teaching Kit

150

This presentation explains how trade secrets and know-how can be valuable and strategically important forms of intellectual property.

Slide 151

Contents

By the end of this presentation students should be able to:

1. Define trade secrets and know-how.
2. Understand how best to protect confidential information.
3. Recognise the potential economic value and competitive advantage offered by trade secrets and know-how.

Students should also be able to discuss case studies involving legal arguments about trade secrets and know-how.

Trade secrets and know-how are valid and often valuable forms of IP.

Intellectual property is more or less what the term says – it is non-physical property that arises from intellectual activity. It can be a specific use of technology, described in a patent. It can be a surface design that makes a product distinctive. It can be an artistic work such as a film, a novel, or a piece of music. It can be a piece of graphic design used as a company logo.

It can be unique and confidential knowledge gained through experience. Knowledge that is kept secret because it is the key to doing something more successfully – and that gives an advantage over competitors.

For example, two companies might use exactly the same equipment and processes but get very different results. The more successful company might use a counter-intuitive machine setting, discovered by trial and error, that significantly increases productivity. The company keeps the setting secret.

Another company might be more successful than its competitors because it has a larger and more detailed database of potential customers. It keeps the database secret.

The essence of trade secrets and know-how is that it is information that is kept secret and only disclosed in complete, legally binding confidence.

That makes trade secrets and know-how the opposite of other forms of IP right – patents, registered designs, copyright, trade marks – which require information to be disclosed publicly.

In this regard, Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure seeks to harmonise the protection of trade secrets all across the European Union in three main areas, namely:

- The definition of what is a “trade secret” and how they will be protected;
- The remedies available to trade secrets holders in the event of misuse or misappropriation of their trade secrets; and
- The measures the Court can use to prevent the disclosure of trade secrets during legal proceedings.

Member states shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 9 June 2018.

Contents

- Trade secrets
- Know-how
- How to protect and enforce trade secrets and know-how
- How to extract value from trade secrets and know-how

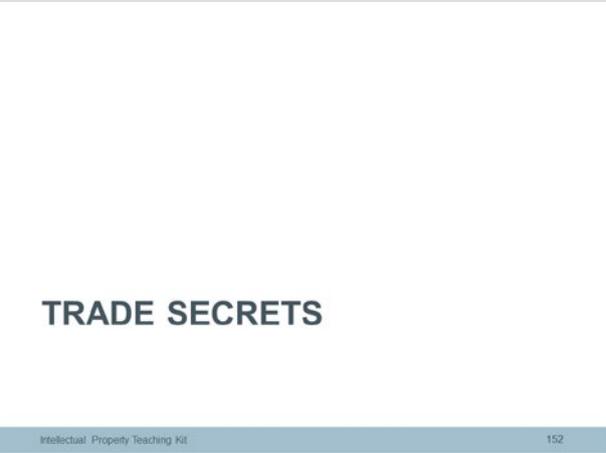
The presentation sheds light on two lesser-known but important ways of protecting IP: trade secrets and know-how.

Trade secrets and know-how are closely related. What unites them is a dependence on confidentiality for their effectiveness.

Any business – whether in manufacturing or services – can potentially benefit from protecting trade secrets or know-how.

It is perfectly possible for know-how or a trade secret to be your most valuable form of IP right.

Slide 152
Trade secrets



Let's look first at trade secrets.

Slide 153

What is a trade secret?

According to the World Intellectual Property Organization, the most common form of protection used by business is secrecy; even more than the best known areas of IP such as patents, copyright, trade marks or design.

Trade secrets consist of confidential business information which provides an enterprise a competitive edge. Moreover, according to the general standards which are referred to in Art. 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights, the following criteria must be met:

1. The information must have a business, commercial or economic value from not being known:

The requirement that information must have **independent economic value** to qualify as a trade secret tends to be overlooked, so it's worth dealing with first.

A trade secret is information that, if it became generally known, would cause financial loss to the owner of that information. Or more accurately – to the **former** owner of that information.

The exact nature of the loss may take several forms but they will all derive from the same fact: information that denied competitors an advantage is now freely available to those competitors.

Therefore, the owner of confidential information should at least in theory be in a position to say: 'If that information became known to one or more competitors, it would cost us €X per year.'

2. The information in a trade secret must be not generally known or easily discovered:

More important though – if only because it can be very difficult to achieve – is that **a trade secret can only be a trade secret for as long as it remains secret**. Serious effort must be made to keep it a secret – not just in the short term, but potentially forever.

3. Reasonable efforts to maintain the secrecy of the information must be demonstrated:

Moreover, the owner of a trade secret must be able to demonstrate to a standard acceptable in a lawsuit that the practical steps taken to keep the information secret and secure were reasonable and robust.

All this may require an unusual level of diligence from owners of confidential information. In looser, less formal company cultures it may be a challenge to take the duty of confidentiality sufficiently seriously – but taken seriously it must be!

It is no good merely saying that a body of information is a secret and otherwise doing little to protect it. If a court finds elementary flaws in security and concludes that the information could not have been secret because it was not treated as secret, then that may well be the end of any claim to own a valuable trade secret.

Following the same line, according to the Directive on Trade Secrets, a 'trade secret' means information which meets all of the following requirements:

- 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;
- c. Has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

You can ask the students to suggest types of information that might become worthwhile trade secrets, and contribute examples of your own.

What is a trade secret?

- Any information that is deliberately not disclosed and that:
 - Economically benefits its owner for as long as it remains secret
 - May economically harm its owner, or benefit competitors, if disclosed against its owner's wishes
- A powerful and valuable form of intellectual property (IP) with a potentially unlimited life
- Not enough to call it a secret. It must be actively kept a secret

The term 'trade secret' may sound old-fashioned. In an age of instant internet searches, very little seems to be unknown or unknowable. But trade secrets still have – and probably always will have – an important role to play in giving businesses a competitive edge.

What makes a trade secret? A trade secret is any information that is deliberately not disclosed and that economically benefits its owner for as long as it remains secret and that may economically harm its owner, or benefit competitors, if it is disclosed against the owner's wishes.

A major advantage is that there is no time limit for protection – unlike patents, registered designs, trade marks or even copyright.

Most importantly, a secret is not a secret unless it is actively KEPT a secret – potentially indefinitely. That's where the difficulty may lie!

Slide 154

Summary – trade secrets

A trade secret can potentially be any information that has 'independent economic value' and remains out of the public domain.

In the technical domain, trade secrets may be particularly useful for protecting products or processes that are difficult to reverse engineer.

Two well-known examples of trade secrets – in the sense that their existence is known but not their content – are the recipes for Coca-Cola and Colonel Sanders' Kentucky Fried Chicken. It is worth noting that the Coca-Cola recipe has so far been a secret for over a hundred years. Is that good luck, or good confidential information management?

The subject matter of trade secrets is usually defined in broad terms and includes sales methods, distribution methods, consumer profiles, advertising strategies, lists of suppliers and clients, and manufacturing processes.

DISCUSSION: Using students' experience, knowledge or conjecture, what else might potentially be a trade secret?

Some trade secrets need to be 'worked' within the company to have any function at all, so access to the confidential information has to be given – but it must be tightly controlled.

The most common ways of controlling access are legally binding contracts or non-disclosure agreements (NDAs), which will be dealt with in more detail later. In general though, common sense dictates that access to confidential information should be restricted to as few people as possible.

Summary – trade secrets

Scope
Can be any information that is genuinely kept secret

Access
Must be strictly limited and controlled by contract – for example NDAs

Benefit
Can be of substantial long-term commercial value to its owner



Images from www.coca-cola.com

Intellectual Property Teaching Kit 154

What can be protected by a trade secret? Just about anything. No one can tell you: ‘You can’t protect that’. Unlike patents, where you can be refused protection for the whole or part of your technical solution.

The most famous example – but far from the only one – is Coca-Cola. A multinational, iconic, 129-year-old business worth countless billions of dollars – all based on a secret recipe for a fizzy drink.

Trade secrets can be shared with other people – inside or outside the business – yet still protected. We’ll look at ways of doing this later.

It should go without saying, though, that any sharing must only be done on legally binding terms of confidentiality.

What are the benefits of keeping important information secret? They might be modest or they might be huge, but they will be positive.

Slide 155
Know-how



Now let's move on to know-how.

Slide 156

What is know-how?

Most general definitions talk of expert skills or bodies of knowledge that:

- impart an ability to cause a desired result,
- are not ‘obvious’ to other experts in that field,
- are not known either inside or outside (‘the public domain’) the relevant field.

Stricter legal definitions talk about know-how as essentially a production factor. It is:

- industrial information or technique likely to assist in the manufacture or processing of goods and materials.

According to this legal definition, it is possible to regard negative information as know-how. For example, if experience teaches you how not to do something, then that may potentially be know-how if it ‘assists’ by eliminating trial and error or by preventing well-intentioned mistakes.

As with trade secrets, the test of know-how as an IP right is how successfully the know-how has been kept secret. The moment it is no longer secret, it is no longer know-how.

The case law provides a more specific definition of know-how.

‘Know-how is generally defined as factual knowledge not capable of precise, separate description. However, when used in an accumulated form, after being acquired as the result of trial and error, gives to the one acquiring it an ability to produce something which otherwise would not have known how to produce with the same accuracy or precision found necessary for commercial success.’

[Hooker Chemical Corp. v. Velsicol Chemical Corp., 235 F. Supp. 412 (W.D. Tenn. 1964)]

Know-how gives the person using it an advantage over others.

Many companies may have know-how without realising it. For example, an accepted form of know-how is a specific supplier list for certain ingredients.

Consider a chemical process for producing Compound X. What is generally known is that:

- When compounds A and B react, Compound X is formed.
- The reaction occurs in the temperature range of 40-400°C.
- Higher temperatures work best, but greatly increase production costs.

Company 1 and Company 2 cannot make Compound X for the price Company 3 charges.

This is because Company 3 has learned through experience (historic trial and error) the precise temperature and pressure that produces the highest and most cost-effective yield of Compound X.

That precise knowledge is Company 3’s know-how. Were it to become known by either or both other companies, Company 3’s competitive advantage would be lost.

Company 3 therefore has a very strong incentive to keep this know-how permanently secret.

DISCUSSION: Ask the students what in their experience or knowledge might count as know-how.

What is know-how?

- Any secret or restricted information or knowledge that improves its owner's **ability** to produce a desired outcome
- May enable a business to:
 - source materials more cheaply than a competitor
 - manufacture more efficiently than a competitor even when both use the same equipment and processes
- Can be **tangible**: blueprints, formulae, instructions, specifications
- Or **intangible**: process management skills, market intelligence, quality control techniques

Intellectual Property Teaching Kit

156

Another term for know-how is expert knowledge. This special knowledge is not known to the great majority of people. Maybe not even to other experts in that field.

It is the ability to do something with more skill or efficiency than someone without that knowledge, for example to source materials more cheaply than a competitor or to manufacture more efficiently than a competitor even when both use the same equipment and processes.

Let's say that a patent for a manufacturing process states that the process needs to operate at between 5 and 25 degrees Celsius. Someone who knows the process well has found that the best operating temperature is

10 degrees Celsius. That's valuable information, known to hardly anyone else. That's know-how. Without it, you're left with trial and error.

Obviously there's some overlap between know-how and trade secrets. Roughly speaking, know-how qualifies as a trade secret when it can be said to have independent economic value.

Slide 157

Common features of trade secrets and know-how

Because trade secrets and know-how are not registrable IP rights, there are fewer costs incurred in protecting confidential information compared with patents. In particular, separate rights are not needed for separate countries, as is the case with patents, registered designs and trade marks.

The downside is that precisely because there is no registration, and so no statutory protection, it may take a very expensive court case to prove that a trade secret or know-how exists at all.

A patent is a published document that defines the boundaries of what is claimed as an IP right. There can be no such clarity with trade secrets and know-how until the courts have examined all the specific circumstances of that case.

(However, one should not think that a court case involving a patent will necessarily cost less than one involving trade secrets or know-how!)

Common features of trade secrets and know-how

- There is no official register, and so no statutory protection
- Protection depends entirely on keeping information secret
- There is no geographical limitation
- As long as secrecy is maintained, protection can last indefinitely

Intellectual Property Teaching Kit

157

In a real sense, trade secrets and know-how are at opposite ends of the IP scale from patents and registered designs. Not in terms of importance but in terms of function.

The whole point of patents in particular is that they encourage the protected DISCLOSURE of ideas. Apply for a patent, and 18 months later it's published and the whole world knows about it.

The whole point of trade secrets and know-how is that NOTHING is publicly disclosed. Perhaps forever, as in the case of the Coca-Cola recipe.

For that reason, it's impossible to have a register of trade secrets and know-how. It would be absurd. It would completely defeat the object.

It's also impossible to put geographical limits on secrets. A piece of information with commercial value cannot sensibly be unknown in one country but common knowledge in another.

As long as a trade secret or know-how is kept secret, it remains valuable IP. But the moment the secret gets out, the IP disappears. That's why maintaining secrecy is central to trade secrets and know-how.

Slide 158

How to protect trade secrets and know-how rights

HOW TO PROTECT TRADE SECRETS AND KNOW-HOW RIGHTS

Intellectual Property Teaching Kit

158

So you've got your trade secret or you've got your know-how. Let's now look at how you go about protecting it.

Slide 159

It must not just BE secret – it must be KEPT secret

The stress here must be on the burden of responsibility. If a company decides that for strategic reasons it needs to keep certain information confidential, then it and it alone is responsible for putting in place adequate (legal strength!) measures for keeping that information permanently confidential.

It is no use simply telling employees to keep something secret and expecting that to be enough. It certainly would not satisfy a court.

With the aim of protecting trade secrets effectively, the World Intellectual Property Organization provides a list of precautionary measures to be taken by SMEs. In fact, many SMEs rely almost exclusively on trade secrets for the protection of their IP, although they may not be aware that trade secrets are legally protected.

- The measures suggested include: Considering whether the secret is patentable and, if so, whether it would not be better protected by a patent.
- Making sure that a limited number of people know the secret and that all those who do are well aware that it is confidential.
- Including confidentiality agreements within employees' contracts –even if under the law of many countries, employees owe confidentiality to their employer even without such agreements. Note that the duty to maintain confidentiality on the employer's secrets generally remains, at least, for a certain period of time after the employee has left the employment,
- Finally, signing confidentiality agreements with business partners whenever disclosing confidential information.

It must not just BE secret – it must be KEPT secret

- Protection depends entirely on the IP owner's ability to keep information secret. It is no one else's responsibility
- The owner must make a positive effort to keep trade secrets or know-how confidential and beyond the reach of competitors
- This may not be easy!

If you have a piece of information or body of knowledge that you don't want to share with your competitors, it's your responsibility to make sure it stays secret.

That may not cost you anything additional, but it may mean making a lot of effort!

Slide 160

What is confidential information?

When does information known only under controlled conditions to a privileged few lose its ability to be credibly regarded as 'secret'?

In most companies there is a turnover of key personnel. The more people who over time have access to confidential information, even under very stringent contractual conditions (dealt with later), the less confident one can be that the information remains genuinely confidential.

Keeping information confidential can be a major concern for companies, which is why restrictive covenants and NDAs have such significance. See the following slides.

What is confidential information?

- First, it must be Information that actually is confidential
- Second, it is information that if shared with a third party must be disclosed only in conditions of strict mutual confidentiality

It is not enough to CLAIM that a certain piece of information is confidential. You must be able to PROVE that it was kept confidential and secure. Information that is known to “only” 50 people is unlikely to be truly confidential. So in the event of a dispute, this proof is the first thing a court will want to see.

Also, if shared with a third party, confidential information must be disclosed in conditions of strict mutual confidentiality only.

Slide 161

What in law is NOT confidential?

'Public domain' may to some extent be misleading, as it implies information that is common knowledge to nearly everyone. Most specialised technical or commercial information is unlikely ever to be general knowledge.

'Public domain' may, however, have validity as long as there is no more exact term for information that cannot be said to belong exclusively to one person or one organisation.

What in law is NOT confidential?

- Information already in the public domain
- Information already known to the receiving party
- Information disclosed to a third party without restrictions
- Information whose public disclosure is required by law or statutory regulation

Sometimes it can be simpler to understand what counts as confidential information by looking at what is not confidential.

The first two bullet points are self-explanatory.

The third relates to information that you may have disclosed BEFORE deciding you want it to be secret. If you don't start thinking of IP from the word go, this can be a very easy trap to fall into.

The fourth covers perhaps rare situations where you can't call information secret if the law makes you disclose it. An example might be food ingredients that have to be listed on the packet.

Slide 162

Confidentiality pros and cons

Pros

1. The indefinite duration of confidentiality is in contrast to other forms of IP such as patents (20 years), trade marks (around 50 years) and copyright (variably 50, 70 or 100 years after the death of the work's creator).
2. There is potentially no geographic limitation as long as the information remains a secret in **every** relevant country. This is another big advantage over registrable forms of IP, where there is a cost for each country in which protection is sought.
3. It cannot be said that protecting confidential information is free, as there will be costs associated with legal advice and services (extremely strongly recommended), and possibly with some physical means of protecting information. There will also of course be a substantial litigation cost if the confidentiality of the information needs to be tested in court.

Cons

1. Once information is leaked, even by an act of malice, it is no longer confidential and so your trade secret or know-how may become worthless. If you identify the leaker you can sue for misappropriation or breach of contract, but the damage is done. The trade secret or know-how is no longer exclusive to you.
2. Ownership of a trade secret gives you no right to stop someone else discovering that information by their own independent effort. They might even apply to patent it precisely because it is not in the public domain – and you cannot stop them.
3. You cannot sue someone simply because your confidential information is no longer confidential. You have to prove that the disclosure has caused, or is certain to cause, actual damage to your economic interests. This may not be straightforward.

Confidentiality pros and cons



✓ Potentially indefinite period of IP protection

✓ Potentially unlimited global protection

✓ No registration required



✗ Lose confidentiality = lose IP protection

✗ Can't stop a third party from independently discovering and using the same information

✗ Law requires proof of damage before providing a remedy

Because of their confidential nature which requires disclosure to obtain legal protection, trade secrets are not protected in the same way as other forms of IP.

Trade secrets are protected without any registration or the fulfilment of any formal requirements or procedures to any official authority of protection. Therefore a trade secret can be protected without limitation of time, potential unlimited global protection; as long as it is kept confidential.

However, trade secret protection is generally weak and more difficult to enforce. Trade secrets protection only protects against improper acquisition, use or disclosure of confidential information. If the secret is disclosed, anyone may have access to it. The disadvantages of trade secrets are also high costs connected with the implementation of the safety and information protection policy, control, surveillance. Furthermore others may discover it independently or may patent it.

Slide 163

How to disclose information confidentially

It is important to point out that it is no use having a non-disclosure agreement (NDA) with one party but talking freely to another. For example, in a family-run business there may be a low standard of confidentiality for family members and a much higher standard for 'outsiders'. This will not do! The higher standard must apply to **everybody**.

Confidentiality must also apply to all communications to people outside the business. For example, you cannot reasonably ask everyone who receives an e-mail from you to sign an NDA before reading it. What you must do, though, is ensure that there is **nothing** in even the most casual e-mail that a court might interpret as a disclosure of information that you want to claim as confidential.

How to disclose information confidentially

- Legally binding contracts
 - **Restrictive covenants** for employees, suppliers, subcontractors etc.
 - **Non-disclosure agreements** (NDAs – also known as confidential disclosure agreements or CDAs) for less 'tied' parties such as potential licensees, technical advisers, ad-hoc project contributors
- Disclosures should be kept to an absolute minimum

Intellectual Property Teaching Kit

163

Common sense says you don't share secrets, but often a business can't run without some sharing. Those who typically need access to confidential information include employees and essential suppliers of goods and services.

If access is unavoidable, it must be controlled by legally binding agreements. The handshake and 'my word is my bond' approach just won't do.

Examples of such contracts include restrictive covenants for employees and suppliers, and non-disclosure agreements for potential licensees, technical advisers and the like.

The golden rule is, no matter how legally binding, disclosure should be kept to an absolute minimum.

Slide 164

Constantly review your trade secrets and know-how

It is realistic to expect your trade secrets and know-how to become more widely known over time, as other people acquire their own independent experience and learn from their own trial and error.

If you own a trade secret you should take measures to protect and maintain its confidentiality and assess **continuously** how much of your 'secret' information remains exclusive to you.

Constantly review your trade secrets and know-how

- Today's trade secret may become tomorrow's common knowledge – in which case you lose your IP
- Equally, what you assume is common knowledge may actually be known only to you – in which case you may acquire valuable IP
- So continuously evaluate the information that helps run your business. It could be more (or less) valuable than you think
- If in doubt, **keep it confidential**. Whatever it is – if it's not your secret, you'll get little or no commercial advantage from it

It is important to bear in mind that everything changes with time, so review your trade secrets and know-how status regularly.

Look for THREATS – which can include your own complacency and carelessness. Today's trade secret may become tomorrow's common knowledge.

Look also for OPPORTUNITIES – new situations that may give rise to more trade secrets and more know-how. What you assume to be common knowledge may actually be known only to you.

If in doubt: keep it confidential.

Slide 165

Practical steps to maintain confidentiality

Stress that (probably) the easiest and cheapest way of keeping information confidential within a company is to disclose that information only on the strictest need-to-know basis. If nobody else needs to know, then tell nobody else.

University researchers may possibly be more prone to leaking secrets inadvertently, as in an academic environment there is a tradition of sharing information, coupled with less exposure to the commercial pressures that justify NDAs and restrictive covenants.

Financial penalties for breaching confidentiality may be worth considering, but if not 'sold' sensitively, there may be a risk of losing the goodwill of key employees.

As mentioned before, the World Intellectual Property Organization provides a set of recommendations and practical steps with the aim of maintaining confidentiality, including:

- Considering whether the secret is patentable and, if so, whether it would not be better protected by a patent.
- Making sure that a limited number of people know the secret and that all those who do are well aware that it is confidential.
- Including confidentiality agreements within employees' contracts –even if under the law of many countries, employees owe confidentiality to their employer even without such agreements. Note that the duty to maintain confidentiality on the employer's secrets generally remains, at least, for a certain period of time after the employee has left the employment,
- Finally, signing confidentiality agreements with business partners whenever disclosing confidential information.

Practical steps to maintain confidentiality

- **Label** all confidential information as *CONFIDENTIAL*
- **Restrict access** to sensitive information. If it needs to be kept secret, keep it in a secure, off-limits area
- **Use NDAs** rigorously and consistently
- **Train employees** to be aware of the importance of non-disclosure
- Consider including **sanctions for breaching confidentiality** in contracts of employment
- Ask yourself: would a court agree that appropriate steps have been taken to safeguard your trade secrets and know-how?

Intellectual Property Teaching Kit

165

Practical steps to maintain confidentiality include labelling all confidential information as confidential, restricting access to sensitive information, using NDAs rigorously and consistently and training employees to be aware of the importance of non-disclosure.

The acid test is the one shown at the bottom of this slide. How would a court rate the steps you've taken to protect yourself?

Slide 166

How to enforce trade secrets and know-how rights

Unlawful acquisition, use and disclosure of trade secrets

Member States shall ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in the proposed Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of their trade secret.

The acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful, whenever carried out by:

- a) unauthorised access to, appropriation of, or copying of any documents, objects, materials, substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;
- b) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions:

- a) having acquired the trade secret unlawfully;
- b) being in breach of a confidentiality agreement or any other duty not to disclose the trade secret;
- c) being in breach of a contractual or any other duty to limit the use of the trade secret.

The acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully.

The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully.

Exceptions

Member States shall ensure that an application for the measures, procedures and remedies provided for the Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

- a) for exercising the right to freedom of expression and information, including respect for the freedom and pluralism of the media;
- b) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;
- c) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise;
- d) for the purpose of protecting a legitimate interest recognised by Union or national law.

HOW TO ENFORCE TRADE SECRETS AND KNOW-HOW RIGHTS

Intellectual Property Teaching Kit

166

Turning your trade secrets or know-how into intellectual property rights is one thing. Enforcing your rights may be quite another. Let's now look at how it can be done.

Slide 167

Contracts are EVERYTHING

Contracts are intended to be helpful as well as prohibitive. They detail the confidential information to be protected, who is entitled to use the information, for what purposes and in what circumstances, and what legal obligations are placed on the signatories.

Contracts should be written in clear, plain but nonetheless legally binding language and must meet the high standards required by a court. It would therefore be advisable to have contracts drawn up by legal and IP professionals.

Contracts are EVERYTHING

- Private agreements between two or more parties:
 - define the exact scope of protection
 - put everything in writing
 - are legally enforceable
- Types of contract include:
 - restrictive covenants
 - non-disclosure agreements (NDAs)

It all leads to contracts that stand up in court – which means it's false economy not to have your contracts written by legal or IP professionals. This could be your biggest cost, but don't begrudge it.

Slide 168

Restrictive covenants

An employer with valuable trade secrets should require all employees with access to them to enter into a non-disclosure agreement. A point to stress is that the **same** contract – the same **duty of confidentiality** – must apply to **all** employees for whom a restrictive covenant is deemed appropriate. If the details of a contract change over time, they must also change – if legally possible – in existing contracts.

Another point to stress is that contracts should not be so restrictive that they amount to a **restraint of trade** on employees who leave the company.

For example, it might be reasonable to prevent an ex-employee from working for a competitor for (say) a year, but not to prevent him or her from **ever** working for a competitor.

Restrictive covenants

- Prohibit behaviour specified as not in the employer's interest
- Help protect business interests, which can specifically include trade secrets and know-how
- Cover time periods before, during and after employment

A restrictive covenant is a contract between – most usually – an employee and employer. It prohibits behaviour specified as not in the employer's interest.

Restrictive covenants are justifiable if they protect something of high value to the business. But they also restrict the freedom of people whose talent and goodwill the business depends on. For that reason, it is essential to get appropriate professional advice on the framing and writing of the covenant.

Slide 169

Typical protection clauses in restrictive covenants

In trade secrets lawsuits, the court evaluates how restrictive the covenant is (see slide 168). Courts will not look kindly on a contract that tries to bar ex-employees from using their skills and experience to make a living. This will be regarded as an inappropriate restraint of trade.

Typical protection clauses in restrictive covenants

- All IP created in the course of employment belongs to the employer
- Restraint of trade or non-competition clauses
- Non-solicitation/non-dealing clauses
- Non-disclosure agreement clause

Intellectual Property Teaching Kit

169

A typical clause in restrictive covenants states that all IP created in the course of employment belongs to the employer. 'Created in the course of employment' can include private projects apparently unrelated to employment but making use of an employer's resources – which may include confidential information. This can be a highly contentious area so be careful to define it clearly.

Under restraint of trade or non-competition clauses, an ex-employee may not work in a specified geographical area, or for a competitor, for a specified period of time.

Non-solicitation or non-dealing causes stipulate that former employees may not contact customers of their former employer for a specified period of time.

And non-disclosure agreement clauses state that employees may not disclose or use confidential information belonging to the employer except with the employer's prior knowledge and permission.

It is advisable to take appropriate professional advice on the framing and writing of restrictive covenants.

Slide 170

Non-disclosure agreements (NDAs)

NDAs are also known as **confidentiality agreements (CAs)** or **confidentiality disclosure agreements (CDAs)**. It is fair to say, though, that NDA is a much more widely known and used term.

NDAs are normally used with third parties such as suppliers, consultants, designers, subcontractors, component manufacturers and – importantly – potential licensees of proprietary technology.

The wording of individual NDAs may differ to some extent, but the rigour must be the same for all. For example, you should not be strict about confidentiality with one component manufacturer and more lenient with another.

You also cannot reasonably require one party to sign an NDA but exempt another in similar circumstances. Any evidence of inconsistent use of NDAs could weaken or destroy your case if a court has to decide whether information is confidential or not.

If a reminder is needed: NDAs are legally binding documents and so should ideally be drawn up by legal or IP professionals. Failure to do so could be false economy with potentially disastrous consequences for the owner of the trade secret or know-how.

Non-disclosure agreements (NDAs)

- Balance need to protect IP with need to obtain a third party's co-operation, so are usually less onerous than restrictive covenants
- Make it clear that any IP disclosed belongs to disclosing party
- Should include:
 - indication of confidential information being disclosed
 - definition of exactly who is (and is not) allowed access to the confidential information
 - duration of period of confidentiality
 - each party's obligations and the circumstances in which they may be terminated
 - applicable laws and legal jurisdictions

NDAs are often stand-alone documents, but their provisions are typically included in restrictive covenants.

They balance the need to protect IP with the need to obtain a third party's co-operation, so are usually less onerous than restrictive covenants. They make it clear that any IP disclosed belongs to the disclosing party, and they should include, among other things, an indication of the information being disclosed, a definition of exactly who is and is not allowed access to it, and the duration of the period of confidentiality.

There are many freely available models of NDA on the internet, but professional advice is best. If you write your own, at least get it scrutinised by a professional.

Because NDAs are legally binding, often for several years, people outside the business may be reluctant to sign. Therefore use them only when absolutely necessary, and keep them clear and reasonably short.

Slide 171

Enforceability – reliance on contracts

Patents by definition disclose information, which means that a court can consider a case of alleged infringement knowing exactly what IP is in dispute. This is very different from a case involving a trade secret or know-how. Here, a court must first establish that confidential information – and thus an IP right – actually exists. Only then can it consider the question of violation of that IP right.

Everything will hinge on whether or not there was a breach of confidentiality resulting in misappropriation (unlawful or unauthorised use) of the confidential information.

The defendant will try to claim that no duty of confidentiality existed – perhaps because the information was not genuinely confidential – or that any contract entered into was invalid, or that the contract actually allowed the use of information in the way that is now disputed.

The court will examine in great detail the wording and substance of the contract to see who has the stronger argument.

It is therefore essential that anyone who wants to enforce their ownership of an IP right in confidential information has a legally watertight contract. The court must be satisfied that it is legally valid and binding on the parties who sign it.

The court must also be satisfied that real economic damage or loss has been caused, or will inevitably be caused, by the misappropriation of the confidential information. (Even though, as a result of misappropriation, the information can no longer be considered confidential.)

There are therefore two legal tests:

- Was the information obtained improperly?
- Did the misappropriation of the information cause economic damage to its rightful owner?

It may be asked: why sue for breach of contract when the actual misdemeanour was breach of confidentiality?

The simple and practical answer is that it is more convenient. Courts find it easier to judge breaches of contract because such cases are common and there is a great deal of case law to use as guidance. By contrast, judging breach of confidentiality is often much more complex, has fewer precedents, and so has less predictable or reliable outcomes.

It is important to note that enforceability of a contract of confidentiality has limits. For example: if your (former) trade secret enters the public domain as a consequence of person A's breach of confidentiality, and it is used for gain by person B, who has no contractual relationship to you whatsoever, there is nothing you can legally do to stop person B.

Enforceability – reliance on contracts

- The law of contracts applies to both restrictive covenants and NDAs. They are **private** agreements that are **legally binding** on both parties
- If a breach of confidentiality is alleged, any legal judgment may depend entirely on the exact wording of the contract
- It is therefore vital to ensure that the contract (covenant or NDA) is of sufficient quality to meet legal requirements

It's no good waiting until your day in court to find that your restrictive covenant or NDA has enormous holes in it.

If a breach of confidentiality is alleged, any legal judgment may depend entirely on the exact wording of the contract, so spend time – and some money – on the **QUALITY** of your contracts before you get anyone to sign anything.

Slide 172

Know your IP rights

A vital preliminary to taking legal action in a different jurisdiction from your own is to ground yourself thoroughly in what that jurisdiction requires in the way of evidence, and what remedies are available. In many cases that will be best left to a qualified legal representative.

Article 39 of the WTO Agreement on Trade-Related Aspects of Intellectual Property Rights – commonly known as TRIPS – is reproduced here in full:

1. In the course of ensuring effective protection against unfair competition as provided in Article 10bis of the Paris Convention (1967), Members shall protect undisclosed information in accordance with paragraph 2 and data submitted to governments or governmental agencies in accordance with paragraph 3.
2. 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 practices (10) 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.
3. Members, when requiring, as a condition of approving the marketing of pharmaceutical or of agricultural chemical products which utilize new chemical entities, the submission of undisclosed test or other data, the origination of which involves a considerable effort, shall protect such data against unfair commercial use.

In addition, Members shall protect such data against disclosure, except where necessary to protect the public, or unless steps are taken to ensure that the data are protected against unfair commercial use.

Moreover, the Directive on Trade Secrets lays down rules on the protection against the unlawful acquisition, disclosure and use of Trade Secrets.

Member States shall ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in the Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of a trade secret.

Those measures, procedures and remedies shall:

- a. Be fair and equitable;
- b. Not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays;
- c. Be effective and dissuasive.

Furthermore, those measures, procedures and remedies shall be applied by the competent judicial authorities in a manner that:

- a. Is proportionate;
- b. Avoids the creation of barriers to legitimate trade in the internal market;
- c. Provides for safeguards against their abuse.

Know your IP rights

- Article 39 of the World Trade Organisation (WTO) Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) covers **proprietary information**
- Proprietary information is confidential information not protected by patent, registered design or copyright
- While Article 39 does not specifically mention trade secrets and know-how, their inclusion can be inferred

Intellectual Property Teaching Kit

172

Ideally, you need to avoid having to seek a legal remedy, because that means something has already gone badly wrong. Focus more on continuously maintaining and improving the security of your trade secrets and know-how.

Article 39 of the TRIPS Agreement recognises that you have a right to protect your ‘proprietary information’ – which by inference covers trade secrets and know-how.

With the ratification of the WTO treaties there is an expectation that each country will make appropriate provisions in its own laws. This is the case with EU member states, so you can be confident that your trade secrets and know-how can be protected in Europe (and in practice in many other countries).

Moreover, the European Union Directive on Trade Secrets lays down rules on the protection against the unlawful acquisition, disclosure and use of Trade Secrets. It ensures that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in the Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of a trade secret.

Slide 173

How to extract value from trade secrets and know-how

HOW TO EXTRACT VALUE FROM TRADE SECRETS AND KNOW-HOW

Intellectual Property Teaching Kit

173

Intellectual property doesn't exist for its own sake. It's there to help you make a profit – so let's now look at how that's done.

Slide 174

Patents or trade secrets?

It is often difficult to make clear-cut decisions about which IP right(s) to use. Too much is at stake to rely on guesswork, so advice should routinely be sought from qualified IP law professionals.

A combination of IP rights will often offer the widest protection, so it is common for technology to be protected by both a patent **and** trade secrets or know-how.

High-tech technology transfer in particular is often a combination of patents and know-how. The technology may become redundant before the know-how, or vice versa.

A good use of know-how may be to protect a new or improved process. The normal assumption is that if you patent a technology, the process you use is the one described or implied in the patent.

But let's say you later discover a different way of working the technology that gives it a significantly greater competitive advantage. Patenting the new process may not be appropriate, because (a) it will eventually be published and so disclosed, and (b) without physical access to a competitor's premises it can be extremely difficult to prove infringement of a process. It may be much better all round to treat that process as a trade secret or know-how.

Example drawback of trade secrets:

- The owner of a trade secret must initiate often lengthy, uncertain and expensive breach of contract proceedings before any legal remedy for misuse of trade secrets is possible.

Example drawback of patents:

- There is a risk that after publication of a patent application a patent will not be granted. The applicant may then have made a completely unprotected disclosure of trade secrets.

Patents or trade secrets?

- A patent may (possibly) be better if a technology:
 - can be reverse engineered
 - might be developed independently by competitors
 - might have relatively short-lived commercial value
- A trade secret may (possibly) be used instead or in addition if:
 - the technology or product may have a 20+ year life span
 - there is nothing patentable in the technology
 - enforcing a patent is likely to be difficult

Which is better – patent protection or trade secret protection?

A patent may be better if a technology can be reverse engineered or developed independently by competitors or have a relatively short-lived commercial value.

A trade secret may be used instead or in addition if the technology or product has a 20+ year life span, if there is nothing patentable in the technology or if enforcing a patent is likely to be difficult.

These are only very rough guidelines. The best protection for a business, its products and its technologies usually comes from a COMBINATION of different forms of IP right. What that combination should be will vary from case to case. Again, you will need to seek professional advice to get it right.

Slide 175

Ways of 'working' trade secrets and know-how

When licensing, know-how can be bundled up with other IP rights such as a patent. A well-written licensing agreement will however stipulate separate royalties for each form of IP. This may help ensure that if one IP right becomes invalid, another might continue to provide income.

The potential importance (and thus value) of know-how should not be underestimated. In many instances a patent may be difficult to operate advantageously without process know-how that may not be evident in the patent or deducible from the technology.

Ways of 'working' trade secrets and know-how

- **Market advantage:** Use them to beat competitors in the market-place
- **Licensing:** They are licensable, so include them in licensing agreements alongside registered IP rights
- **Assignment or sale:** They can also be assigned or sold in the same way as registered IP rights
- **Spin-offs or start-up:** They can help improve the prospects of a new business

Intellectual Property Teaching Kit

175

Intellectual property is just that – property. It can be bought, sold, stolen, damaged, copied – just like physical property. The fact that trade secrets or know-how may spend most of their time locked inside someone’s head doesn’t alter that fact.

The slide shows different ways of “working” trade secrets and know-how. You can use them to beat competitors in the market-place. They are licensable, so you can include them in licensing agreements alongside registered IP rights. They can be assigned or sold in the same way as registered IP rights. And they can help improve the prospects of a new business.

Slide 176

All IP – registrable or non-registrable – has value (I)

All IP – registrable or non-registrable – has value (I)

- **Registrable IP** (particularly a patent) has higher perceived status but:
 - It is documented and so in the public domain for all to see
 - By defining the technology it may leave too much **unprotected**
 - Protection is limited by time and territory
 - Enforcing the IP right may be prohibitively expensive

Registrable IP – particularly patents – has a higher perceived status, but it is in the public domain for all to see.

But there may be more value in having your IP kept out of the public domain. The less others know what you've got, the better.

Slide 177

All IP – registrable or non-registrable – has value (II)

Stress that there are different forms of IP right for a reason. Each has its own strengths and weaknesses. But in a strategic combination appropriate to the IP that needs protecting, the whole of an IP portfolio will often be stronger than the sum of its parts.

For instance, contrary to patents, trade secrets are protected without registration, that is, trade secrets are protected without any procedural formalities. Consequently, a trade secret can be protected for an unlimited period of time.

All IP – registrable or non-registrable – has value (II)

- **Non-registrable IP** – including trade secrets and know-how – is lesser known but:
 - It can be kept private and unseen and yet still be IP
 - Ownership is not restricted by time or territory
 - Controlled access can help achieve business goals
 - It usually costs little to keep trade secrets and know-how secure

By now you know that trade secrets and know-how have real value. One thing to guard against is that, if you make your employees aware of its importance – as you should – then one or two of them might start to think ‘I’ll have some of that.’ So yet again, make sure you always do your utmost to keep confidential information genuinely confidential and in your control. It usually costs little, and can help you achieve your business goals.

Slide 178

Common to all IP

Stress again the importance of a **combination** of IP rights. The precise make-up of that combination, and the way you use it, may depend on your business strategy or objectives.

However, it is probably reasonable to say that identifying potential trade secrets and know-how should be an early priority.

The next priority should be to use rigorous, legally valid NDAs and restrictive covenants to protect all your confidential information.

This can include information that you might later decide to incorporate in a patent application. Keeping **all** technical information confidential as a matter of routine will help reduce the risk of inadvertent disclosures that might prevent you from obtaining a patent.

Common to all IP

- No IP right – registrable or non-registrable – is self-enforcing
- It is 100 per cent **your** responsibility to detect and take action against infringement of any of your IP rights
- That includes breaches of confidentiality

Whatever forms of IP you use, you're entirely on your own when it comes to policing them. No IP right – registrable or non-registrable – is self-enforcing. That's not always understood.

Gathering hard evidence that confidentiality has been breached can be very difficult – so make every effort to avoid getting in that position in the first place. It is entirely your responsibility to detect and take action against the infringement of ANY of your IP rights, including breaches of confidentiality.

Slide 179

Is any one form of IP right more important than another?

Is any one form of IP right more important than another?

- The short answer is no
- The longer answer is that in specific circumstances, one form of IP right may be more effective or valuable than another
- Do not to dismiss an IP right just because it is less well known
- If you do want a trade secret or know-how as an IP right, make sure to secure that right correctly

The short answer to this question is no. The longer answer is that depending on the circumstances, one form of IP right may be more effective or valuable than another.

Do not dismiss an IP right just because it is less well known. There are many instances of trade secrets or know-how proving more useful than patents.

Intellectual property is an area where things can quickly get complicated. Before saying, 'I want this information to be MY trade secret or MY know-how', make sure you know exactly what you're doing and why you're doing it. If in doubt, seek professional advice – it'll be money well spent.

Slide 180

Facts of enforcement in Europe

In any civil court the burden of proof is always on the plaintiff to prove that the defendant is at fault, and that his or her actions directly caused economic loss or damage to the plaintiff. A balance of probabilities, or a weak defence, will not be enough to sway a judgment in the plaintiff's favour.

The civil courts of each EU member state treat trade secrets differently. A good reference work is:

Report on Trade secrets for the European Commission compiled by Hogan Lovells International LLP. It can be downloaded free from:
http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/120113_study_en.pdf

For example:

Germany has a few provisions in its criminal Act Against Unfair Competition that can help enforce trade secrets.

Sweden is the only EU country that has a law specifically protecting trade secrets – yet it does not consider trade secrets to be intellectual property!

France regards 'manufacturing secrets' as IP rights but only in civil law and therefore only enforceable between private parties.

Facts of enforcement in Europe

- In a court of law the burden of proving a breach of confidentiality is always on the owner of the trade secret or know-how
- He or she must be able to prove that:
 - A wrong was committed and harm caused
 - Contracts and protection measures were fit for purpose
- Directive 2016/943 seeks to approximate the laws of the Member States so as to ensure that there is a sufficient and consistent level of civil redress in the internal market in the event of unlawful acquisition, use or disclosure of a trade secret.

Trade secrets were separately regulated across Europe. Hence, the European Parliament and the Council adopted the Directive 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, which harmonises the protection of trade secrets all across the European Union in three main areas, namely:

- The definition of what is a “trade secret” and how they will be protected;
- The remedies available to trade secrets holders in the event of misuse or misappropriation of their trade secrets; and
- The measures the Court can use to prevent the disclosure of trade secrets during legal proceedings.

Trade secret infringements by third parties are generally considered as torts.

Trade secret lawsuits require the plaintiff to prove the existence of a trade secret and that he or she has ownership rights to it.

Therefore in most cases, the only way to deal with that is to hire a patent attorney or some other suitable IP law specialist.

8 Trade secrets and know-how case study

Trade secrets and know-how case study

List of slides

Slide 181	Trade secrets and know-how case study
Slide 182	Contents
Slide 183	Who are Facit Homes?
Slide 184	How is a Facit house constructed?
Slide 185	How are the components manufactured?
Slide 186	Facit Homes' know-how
Slide 187	Initial IP strategy (I)
Slide 188	Initial IP strategy (II) (optional)
Slide 189	First-mover advantage
Slide 190	How do Facit Homes protect their trade secrets?
Slide 191	How can trade secrets be enforced?
Slide 192	Using IP strategy to expand the business

Slide 181

Trade secrets and know-how case study

TRADE SECRETS AND KNOW-HOW CASE STUDY

Intellectual Property Teaching Kit

181

This presentation consists of a case study on the use of trade secrets and know-how.

Slide 182
Contents

Contents

- Who are Facit Homes?
- Facit Homes' trade secrets
- Initial IP strategy
 - Identification of IP rights
 - Advantages of protecting a trade secret vs patent/utility model
 - First-mover advantage
- Protection and enforcement of trade secrets
 - Contracts and agreements
 - Enforcement of contracts and agreements
- Growing the business

In this presentation we will look at a company called Facit Homes and how they came to use trade secrets to protect their IP. We will remind ourselves of the advantages and disadvantages of trade secrets over patents and trade marks, as well as the ways in which trade secrets can be protected and enforced.

Slide 183

Who are Facit Homes?

The slide shows a technical drawing representing one view of a computer model illustrating the various timber elements required to build a house in London for a customer called Nick Garwolinski.

Facit Homes developed many new components specific to this project. In all, there are 200 components, each containing 10-15 parts, with 3 000 parts in total. All of these components were designed and cut out by a computer program developed by Facit Homes using an off-the-shelf CAD program. Using this software, the Facit team is able to design and build houses quickly. The components can be manufactured on site with little waste material.

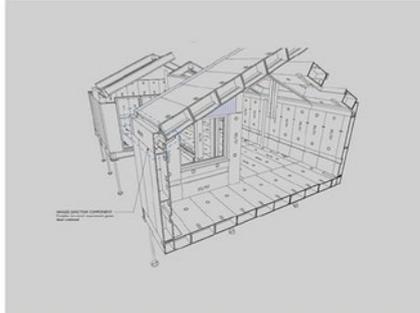
The process developed by Facit Homes to convert the computer models to the instructions required to cut out the components is known as the D-Process.

See for more information:

www.facit-homes.com/clients/nick-garwolinski

Who are Facit Homes?

Facit Homes are a firm of architects who not only design houses but also manufacture the components needed to build them



Intellectual Property Teaching Kit

183

Unlike many other architecture practices, Facit Homes not only design houses but also manufacture the components needed to build them.

What makes the company unique is its innovative on-site manufacturing process.

It is one of the first companies in the world to digitally fabricate and manufacture an entire house on-site. The company's patented D-Process uses a compact, high-tech machine to turn a 3-D computer model into exact physical components that can be joined together.

The slide shows the various timber elements required to build a house the company designed for a client in London.

Slide 184

How is a Facit house constructed?

Read more about the construction of Nick Garwolinski's house in the case study published on Facit Homes' website at www.facit-homes.com/clients/nick-garwolinski

How is a Facit house constructed?



Intellectual Property Teaching Kit

184

During construction of the house, the manufactured timber components are placed into a timber sole plate. The timber sole plate, which is the base of the house, and each component are cut by a computerised machine with a high degree of accuracy and little wastage.

Slide 185

How are the components manufactured?

For more information on Facit Homes' D-Process and how it was developed watch Own-it's interview with Bruce Bell at <http://vimeo.com/59581274>

How are the components manufactured?



Intellectual Property Teaching Kit

185

The components are made using the D-Process™ mobile production facility, which is located on the building site itself. It transforms computer models into the physical components to be used in the building. The components are produced on demand, which helps keep costs down and eradicate lead times.

Now we have seen the manufacturing process, let's have a look at how the company protects its innovations.

Slide 186

Facit Homes' know-how

Facit Homes chose to protect their most valuable asset by keeping confidential information such as the source code within the company.

What exactly is a trade secret?

According to the Directive 2016/943 on Trade Secrets, 'trade secret' means information which meets all of the following requirements:

- 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; it has commercial value because it is secret;
- it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

Such definition should be constructed so as to cover know-how, business information and technological information where there is both a legitimate interest in keeping them confidential and a legitimate expectation that such confidentiality will be preserved.

Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) lists three requirements:

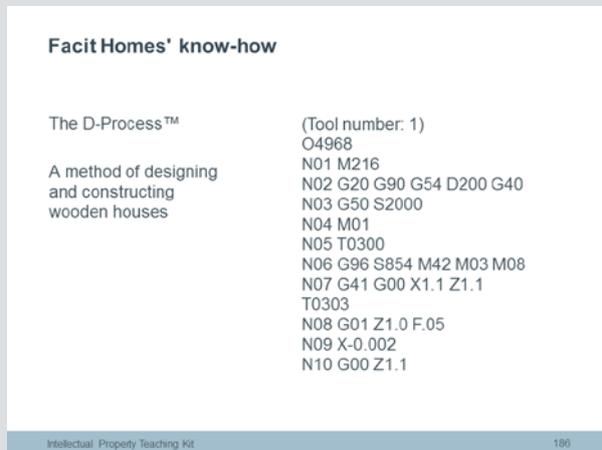
- The information must be secret (i.e. not generally known among, or readily accessible to, circles that normally deal with the kind of information in question).
- It must have commercial value because it is a secret.
- It must have been subject to reasonable steps by the rightful holder of the information to keep it secret (e.g. through confidentiality agreements).

In terms of factors which can distinguish trade secrets from know-how, the following explanation may be useful. It is based on UK case law. The situation may be different in other European countries.

Know-how is considered 'subjective' knowledge which an employee learns during the course of his employment and which becomes part of his own knowledge, skills and experience. Employees have a duty to keep such knowledge confidential while employed if the employer asks them to keep it confidential or if it is obvious that it is confidential. In general, there is no restriction on employees using such know-how once they leave to work for another employer.

Trade secrets, on the other hand, are confidential to the extent that they cannot be disclosed by the employee after they have left the employment even though they are part of their learned knowledge.

In practice it is very difficult to distinguish between know-how and trade secrets. This is important as only trade secrets can be made the subject of a so-called "restrictive covenant" (which we shall explain later in the presentation).



In order for the manufacturing unit to produce the pre-fabricated timber elements, the computer must be programmed with a machine code which provides the machine with the exact instructions to control the technical process with the necessary precision. As you can see from the extract on the slide, there is no “code” as such. It is more like a list or direction.

The code used by Facit Homes is called G-Code. Widely used in the manufacturing industry, it is a very simple standard language giving co-ordinates and type of cut. As with any language, the programmer has to have the skill and experience to use it in the way that best suits the task. In this case, it means translating the 3D drawings generated by a CAD programme into G-Code to instruct the machine.

Facit Homes identified this know-how as the company’s most valuable asset, which, if disclosed, would seriously harm its business interests. The most effective way to protect his kind of know-how is to keep it secret, since the IP framework does not provide for any other method of protection.

Slide 187

Initial IP strategy (I)

It is crucial to identify all types of IP created in your business and consider your business strategy and objectives before developing an appropriate IP strategy. The first thing that many people think about is patents. However, it is often better to rely on a mix of assets, such as design rights, trade marks and copyright, as well as trade secrets. Trade secrets can be particularly valuable if the 'secret' is such that the information cannot be easily discovered by examining the final product or by "reverse engineering", i.e. tearing apart the product and investigating how it works.

In our case, the machine code doesn't reveal the underlying source code or a particular method of translating the computer model into the timber building elements to be manufactured by the machine.

Information about all types of IP can be found on the websites of the EPO (www.epo.org/learning-events.html), the EUIPO (European Union Intellectual Property Office (<https://euipo.europa.eu/knowledge/>)) and many of the national IP offices.

It is always advisable to consult a solicitor or patent/trade mark attorney, who will help you to identify your intellectual assets and make informed decisions about the best IP strategy for your business.

Initial IP strategy (I)

- **Copyright:** architecture plans, buildings, software
- **Patents:** computer implementation of design (possible in some countries), the way in which the components are put together
- **Design rights:** appearance of components
- **Trade marks:** FACIT Homes (brand name), logo
- **Trade secrets:** Conversion of designs into manufactured components



Intellectual Property Teaching Kit 187

When Bruce Bell, the founder of Facit Homes, started out, he thought that certain aspects of his components might be patentable, for example how to put them together. He discussed the possibility with a patent attorney and they reviewed the advantages and disadvantages of patent protection. Utility model protection was not an option, as the company is based in the UK, where there are no utility models.

The attorney was able to identify other IP in the business, such as copyright in the computer program, the design drawings and the design of the building itself, trade marks in the company's name and logo, and confidential information.

It turned out that the company's most valuable asset was its confidential information – or trade secrets.

Of course, Bruce Bell could have tried to obtain a patent for his system of assembling the timber components in addition to keeping his technical innovation secret. He could also have tried to register a design, although this would not have been easy since functional elements of designs are excluded from registration.

Slide 188

Initial IP strategy (II) (optional)

This slide considers the advantages of trade secrets over patents and utility models. As it is not crucial to the presentation of the case study you may want to hide it and use it as background information.

Advantages of trade secrets

- Trade secrets can be protected “forever”, if the company manages to keep the information in the trade secret confidential. We will discuss methods of protection in a later slide.
- Protection is mainly based on contracts. Companies need to instruct attorneys to help them identify their trade secrets correctly and draft appropriate contracts. This can be cheaper than drafting a patent application and liaising with examiners at the patent office.
- Trade secrets exist as soon as they can be treated as such and the company establishes appropriate measures to protect them.
- It can take 2-5 years to obtain a patent from initial application to grant. Patent applications are published after 18 months and can be read by competitors. Once the information is published, neither the applicant nor any competitor can file another patent application based on the same invention in another country, since it would fail the prior art test as the invention would no longer be new. And if the patent application is refused, the inventor will have disclosed the invention, but have got no protection in return. This means that anybody has the right to use the published information without the need to obtain permission. You should therefore consider whether a patent is actually the most appropriate way forward or whether it would be better to keep the invention secret. Filed patent applications can be withdrawn before they are published.
- Protection by patents and utility models is restricted to the country in which the patent/utility model application is filed. European patents provide protection in the contracting states, while US patents provide protection in the United States only.
- Everything has the potential to be a trade secret. A trade secret is know-how that has not – or not yet – been registered as an industrial property right but that is actually or potentially valuable to its owner and not generally known or readily ascertainable by the public, and which the owner has made a reasonable effort to keep secret.

Disadvantages of trade secrets

- Protection is only as robust as the contractual and procedural arrangements in place to keep the information secret. It relies on people to keep the information secret.
- Enforcement may fail if agreements are poorly drafted or procedures inadequate.
- To prove that information has been leaked, you have to identify the source of the leak and/or the person who leaked the confidential information. If you don't know who did it, then it is almost impossible to prove.
- The burden is on you to prove that the information was a trade secret. In the case of registered IP rights, no such proof is needed.
- If a competitor obtained the information through reverse engineering or through independent discovery, then you don't have a claim. You cannot stop the competitor using this independently developed information.
- As soon as a trade secret is leaked, the information is considered to be in the public domain and anybody who receives it in good faith can use it. You can only claim damages from the person who leaked the information and who is in breach of confidence or contract.
- If this person was not bound by any agreement or duty to keep the information confidential, you don't have a claim.

Initial IP strategy (II) (optional)

Advantages of trade secrets vs patents/utility models

Trade secrets	Patents/utility models
<ul style="list-style-type: none">– potentially forever– relatively cheap– immediate effect– no restriction on territory– no restriction on subject-matter	<ul style="list-style-type: none">– time-limited protection– patents expensive to obtain– utility models cheaper than patents but not available in all member states– patents take up to 4½ years to process– utility models can be processed within 6 months– restricted to territory– strict regulations regarding subject-matter

Trade secrets have a number of advantages over patents and utility models.

Trade secrets can potentially be protected forever, whereas patent protection is limited in time.

They are also cheaper to obtain, and their effect is immediate. The patent grant process, on the other hand, can take anything from two to five years.

Patent and utility model protection is restricted to the country in which they were applied for, while there is no restriction on territory for trade secrets.

On the down side, the protection of trade secrets is only as robust as the contractual arrangements in place to keep the information

secret. It relies on people keeping the information secret. If there is an information leak, the burden is on the owner to prove that it has been leaked and to identify the source. With patents, no such proof is needed.

Slide 189

First-mover advantage

You can read about House 1 and view the full episode of Grand Designs broadcast on Channel 4 here:

www.the-self-build-guide.co.uk/facit-homes.html

You can watch the full episode on Vimeo at

<http://vimeo.com/53932758>

Gizmag has an interesting article available at

www.gizmag.com/digitally-fabricated-homes-facit/23844/

It is interesting to read that commentators consider either that the process is not new or that the materials are not appropriate for certain areas, or they are too complex and too expensive for a one-off design. The challenge is therefore to manufacture houses on a larger scale. Bruce Bell fully agrees. The article and comments on the article are a good example of the problems faced by first-movers in the marketplace. First movers need to convince the public and potential clients that their new product or service is innovative and is a good idea, because it solves an existing problem. They have to address problems that only come to light once the innovation starts being used by a larger number of clients. At this point, another company may step in using a similar idea, but, having learnt from the first mover, it can implement the idea with more effective technology or material, on a larger scale and/or with the provision of better customer service. If this happens, the first mover has to make space for the second mover.

Examples

- Atari (first mover) and Nintendo (second mover)
- Charles Stack Online Bookstore (the first to set up an online bookstore but now largely forgotten) and Amazon (second mover, now an international corporation and a market leader)

Source: http://en.wikipedia.org/wiki/First-mover_advantage

First-mover advantage

- "The advantage gained by the initial ("first-moving") significant occupant of a market segment" (Wikipedia)
- Facit Homes is the first company worldwide to use industrial design manufacturing technology to build houses on-site. In doing so it eradicates lead times and avoids waste material

First-mover advantage is, according to Wikipedia, the advantage gained by the initial or first-moving significant occupant of a market segment.

Bruce Bell had a unique opportunity to demonstrate his new technology to the public when he was asked by the producers of Grand Designs, a popular TV programme on the UK's Channel 4, to build a simple structure in front of the cameras in two days. The company did not have any registered intellectual property rights at this stage, but Bruce went ahead anyway as he did not want to miss the opportunity to publicise his business.

However, first-movers cannot always fully exploit their technological advantage once their innovative ideas – if not their trade secrets – have been clearly exposed. Other companies,

with better marketing techniques, more investment and better connections, may follow. In fact, quite often, it is not the first mover who is the most successful company, but the second or even third company in the business. These later arrivals can avoid mistakes and may make or develop more effective technology based on the original ideas of the first mover.

Slide 190

How do Facit Homes protect their trade secrets?

Employees have certain obligations to their employer while they are employed. One of these is the duty not to disclose to other parties (e.g. customers or competitors) information which the employer considers confidential. Such confidentiality clauses therefore just state what is implied in the law, namely that there is a duty of fidelity between the employee and the employer (in Germany, *Treuepflicht*; in France, *devoir de loyauté*). In order to enforce such a general clause, employers must introduce systems and procedures to keep the information confidential and ensure that employees know what is considered to be confidential information. Contracts should include clauses which state that any IP developed during the course of employment belongs to the employer. Copyright in software is harmonised throughout Europe and belongs to the employer under the Software Directive. However, ownership of the copyright in designs or publications is not harmonised and depends on national laws.

According to the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreement, trade secrets are proprietary information and as such can be construed as the intellectual property of the employer.

Restrictive covenants can include promises to not compete with the current employer after the employee leaves employment, e.g. not to work for a competitor for a certain period of time or not to work for a certain period of time in the same area, or not to disclose the trade secret to third parties. They can also include the obligation not to contact clients or lure away employees who are still employed by the former employer.

Employers also need to be aware that only trade secrets can be protected beyond the termination of the employment, since it is not in the public interest to restrict employers from using the skills and experience acquired in the course of their career to the advantage of their new employers.

Therefore, the scope of the trade secret must be defined carefully in the restrictive covenant in order to balance the interests of the employer against those of the employee, especially the right to earn money and the freedom to move to other employment.

Additionally, companies should consider if a one-way **confidentiality agreement** is appropriate or if the other party will also disclose confidential information during the course of the project. In this case, a two-way confidentiality agreement should be signed. Again, it is a good idea to have such non-disclosure agreements (NDAs) or confidential disclosure agreements (CDAs) drawn up by an attorney in order to maximise the ability to enforce the agreement in court if necessary. Note that the terms NDA and CDA are synonymous.

Employers should be aware that a clear definition of the scope of the confidential information is required in any confidentiality agreement. If the definition is too broad, it may contain information which is already in the public domain and therefore cannot be the subject of an NDA. If it is described too narrowly, it may not cover all matters that are considered confidential. An added problem is where partners develop a project whose output they consider confidential. Due to the nature of the development, this cannot yet be described. Therefore, the contracts need to be updated during the research/development project in order to record and agree what they consider to be confidential information and therefore subject to non-disclosure.

Employers should also be aware that having NDAs in place with a large number of people covering the same information can weaken their position in court, since the more people that know about the information the more likely it is that the information will be deemed to be public or not confidential. It also becomes more difficult to enforce an NDA if it is not clear who leaked the information.

How do Facit Homes protect their trade secrets?

- Restricted access to sensitive documents
- Confidentiality clauses in employment contract
- Ownership by employer of IP developed in the course of employment
- Restrictive "covenants" (clauses) in employment contracts
- Non-disclosure agreements with third parties
- Appropriate staff training

Intellectual Property Teaching Kit

190

Facit Homes use machine security settings to restrict access to sensitive information in their mobile production facility. Security settings allow authorised users to set a password for opening files and prevent others from printing, saving, screen grabbing, copying text and so on.

Their employees have confidentiality clauses in their contracts of employment. These confidentiality clauses are very common, as employees normally have a duty to act loyally towards their employer.

The company uses non-disclosure or confidential disclosure agreements or clauses when dealing with their European partner, with whom it needs to share confidential information or trade secrets. Such agreements are signed before the confidential information is disclosed.

They offer appropriate training so that employees are aware of their duty of fidelity and to use the systems provided to keep information confidential. The stricter such measures are, the more likely an employer will be able to identify the source of a leak and enforce the obligation to keep information confidential.

For Facit Homes, this means that employees are generally aware of which information is sensitive, use encryption technology when sending such information, and keep records of who the information was sent to.

Slide 191

How can trade secrets be enforced?

For a comprehensive study on trade secrets and how they are enforced in the various EU member states see the 'Study on Trade Secrets and Confidential Business Information in the Internal Market' (published in April 2013 by the European Commission):

http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/130711_final-study_en.pdf

Moreover, on 8 June 2016 following a proposal from the European Commission, the European Parliament and the Council adopted a Directive that standardises the national laws in EU countries against the unlawful acquisition, disclosure and use of trade secrets (Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure). Said Directive harmonises the protection of trade secrets all across the European Union in three main areas, including the remedies available to trade secrets holders in the event of misuse or misappropriation of their trade secrets and the measures the Court can use to prevent the disclosure of trade secrets during legal proceedings.

Following the approval of the Parliament, the Council should formally adopt the Directive at its next sitting on the end of May or beginning of June 2016.

How can trade secrets be enforced?

- Contract law
- Civil law: "tort"
- Criminal law

Intellectual Property Teaching Kit

191

Facit Homes have so far not had any reason to enforce contracts relating to trade secrets, and so we can only discuss enforcement in theory. We have already seen that the method of protecting trade secrets is through contracts. Contracts are private agreements between two or more parties and are enforced in civil courts. Certain obligations are implied in the employment contract, even if they are not expressly stated in the written contract. These obligations are either based on common law, as in the UK, on statutes or written law, or on both. For example, it would be wrong – a “tort” – of an employee to breach his duty of confidentiality even when the duty is not expressly stated in the contract.

The onus is on the claimant or plaintiff to prove that a trade secret or the duty of fidelity or confidentiality existed and that there was a breach of contract. In most countries,

the claimant must be able to show that ‘on the balance of probabilities’ confidential information existed and has been misused.

A civil court can order “remedies” if it decides that the defendant has breached their obligations to keep information confidential. These remedies can include injunctions, which are instructions issued by the court to not do something or to stop doing something. In most cases, this is already too late when the information is leaked. They can also include the award of damages for the losses suffered.

In some countries and in certain circumstances, the theft of trade secrets or dealing in illegally obtained confidential information can be a criminal offence and may be subject to serious penalties.



With the aim of harmonising the protection of trade secrets all across the European Union, the Directive 2016/943 on the protection of undisclosed know-how and business information (*Trade Secrets) against their unlawful acquisition, use and disclosure should be transposed by 9 June 2018 was adopted. The Directive establishes the measures, procedures and remedies that should be made available to the holder of a trade secret in case of unlawful acquisition, use or disclosure of that trade secret by a third party

It sets the general principles applicable to the civil enforcement instruments in order to prevent and repress acts of trade secret misappropriation, notably effectiveness, fairness and proportionality and safeguards to prevent abusive litigation. Moreover, it establishes a period of limitation that shall not exceed 6 years and requires that Member States provide judicial authorities with

mechanisms to preserve the confidentiality of trade secrets disclosed in court for the purpose of litigation.

Moreover, it provides for provisional and precautionary measures in the form of interlocutory injunctions or precautionary seizure of infringement goods. Furthermore, it establishes safeguards to ensure the equity and proportionality of those provisional and precautionary measures.

Finally, the Proposal provides for measures that may be ordered with the decision of the merits of the case, namely:

- Provides for the prohibition of use or disclosure of the trade secret, the prohibition to make, offer, place on the market or use infringing goods (or import or store infringing goods for those purposes) and corrective



measures. The corrective measures request, inter alia, the infringer to destroy or deliver to the original trade secret holder all the information he or she holds with regard to the unlawfully acquired, used or disclosed trade secret.

- Provides safeguards to ensure equity and proportionality of the measures provided for in the Directive.
- The awarding of damages for the prejudice suffered by the trade secret holder as a consequence of the unlawful acquisition, use or disclosure of his/her trade secrets is contained in the text.
- It empowers the competent judicial authorities to adopt publicity measures at the request of the plaintiff, provided that the trade secret is not disclosed and after considering the proportionality of the measure.

All these measures are laid down by the Directive with the aim of guaranteeing the protection against the unlawful acquisition, disclosure and use of trade secrets.

Among the corrective measures, Member States may provide that, when ordering the withdrawal of the infringing goods from the market, their competent judicial authorities may order, at the request of the trade secret holder, that the goods be delivered up to the holder or to charitable organisations.

Slide 192

Using IP strategy to expand the business

Licensing the software to a third party might reveal the underlying functionality of the program, which is the subject of their trade secret. Although the trade secret could be protected by a confidentiality agreement, the risk remains that somebody might leak the confidential information, which would destroy their most valuable asset. Any damages awarded would be unlikely to compensate for the loss to the companies.

Another option would be to expand the business through franchising, which means licensing the business model to other parties who would then trade under the Facit Homes brand, using Facit's technical innovations and any other know-how or IP rights in the business.

If the trade secret is the subject of the licensing contract, its scope must be described accurately in order to be enforceable. Additionally, the licensing agreement must include an obligation to keep confidential information secret. However, any franchising model comes with an inherent risk of losing control and therefore an increased risk of disclosure of confidential information to third parties.

Using IP strategy to expand the business

Advantages and disadvantages

- Licensing agreements
 - What is the subject of the licence?
 - Protecting the trade secret?
- Franchising model
 - Licensing the business model, including trade marks, business methods, know-how, trade secrets, copyright, design rights

Facit Homes are currently considering expanding the business and are looking for suitable business partners. They are already collaborating with an architecture practice in Denmark called Eentilen. Eentilen design the houses and provide the digital 3D models to Facit Homes, who then translate the digital 3D design into the machine code to instruct the computerised machine in the mobile production facility on site in Denmark.

In this way, Facit Homes do not have to disclose their trade secrets to their partner.

The company has considered licensing the software or setting up a franchising model, which would mean less involvement in the job and scope for more rapid expansion and investment, but has so far not pursued either of these options.

9 Trade secrets and know-how exercises

Trade secrets and know-how exercises

List of slides

Slide 193	Trade secrets and know-how exercises
Slide 194	Contents
Slide 195	Confidential information: the essentials
Slide 196	Practical protection of confidential information
Slide 197	Employee awareness and training
Slide 198	Trade secrets and know-how in practice
Slide 199	Court case 1: Listerine (I)
Slide 200	Court case 1: Listerine (II)
Slide 201	Court case 1: Listerine (III)
Slide 202	Court case 2: Rockwell Graphics (I)
Slide 203	Court case 2: Rockwell Graphics (II)
Slide 204	Court case 2: Rockwell Graphics (II)
Slide 205	Court case 2: Rockwell Graphics (IV)
Slide 206	Court case 2: Rockwell Graphics (V)
Slide 207	Court case 3: Metallurgical Industries (I)
Slide 208	Court case 3: Metallurgical Industries (II)
Slide 209	Court case 3: Metallurgical Industries (III)
Slide 210	Court case 3: Metallurgical Industries (IV)
Slide 211	Court case 3: Metallurgical Industries (V)
Slide 212	Court case 4: Chicago Lock Company (I)
Slide 213	Court case 4: Chicago Lock Company (II)
Slide 214	Court case 4: Chicago Lock Company (III)
Slide 215	Court case 5: Kevlar (I) (optional)
Slide 216	Court case 5: Kevlar (II) (optional)
Slide 217	Court case 5: Kevlar (III) (optional)
Slide 218	Exercises
Slide 219	Exercise 1
Slide 220	Exercise 2
Slide 221	Exercise 3
Slide 222	Exercise 4
Slide 223	Conclusions

Slide 193

Trade secrets and know-how exercises

This presentation contains summaries of several real-life court cases which illustrate how the courts view trade secrets and know-how as valuable forms of intellectual property.

The court cases are followed by exercises for the students.

TRADE SECRETS AND KNOW-HOW EXERCISES

Intellectual Property Teaching Kit

193

Here we are going to recap briefly, then look at practical examples of how IP rights in trade secrets and know-how can be used to prevent unfair competition.

Slide 194

Contents

By the end of this presentation students should be able to analyse trade secrets and know-how from a legal point of view.

Contents

- 1. Confidentiality in practice (recap)**
- 2. Court cases**
- 3. Exercises**

This presentation starts with a recap of confidentiality in practice. We will then work through a number of court cases on various aspects of the topic. These are followed by a series of exercises for the students.

Slide 195

Confidential information: the essentials

A breach of confidentiality can cause serious loss or damage to a business and can potentially ruin it.

Maintaining confidentiality – potentially forever – is an increasing challenge. In part this is because, thanks to the internet, leaked information spreads further and faster than it ever did. In part it's because the culture of keeping secrets has changed. In mainstream media, leaking secrets is worth money, as 'cheque-book journalism' makes clear. In social media, money may not change hands but it is now almost a requirement that nothing shall be secret.

In wartime Britain, thousands of people spent years carrying out top-secret work at the Bletchley Park military intelligence centre. Its very existence remained unknown for many years after 1945, and even now, hardly any of the people who worked there has ever spoken about it. Simply put, they belonged to a generation brought up to respect the need for secrecy.

How conceivable is it that a modern Bletchley Park could remain unknown for longer than a few weeks? How secure could one ever consider its secrets to be?

As time goes on, keeping commercial secrets will become harder, not easier.

Confidential information: the essentials

- Confidential information disclosed or used without its owner's permission can seriously harm a business of any size
- The appropriate use of contracts imposes a **duty of non-disclosure** as a condition of sharing confidential information
- Anyone who breaches confidentiality – deliberately or by omission – may be sued for **breach of contract**
- But a court must first agree that the contract is legally valid and enforceable. So make sure that it is!

A breach of confidentiality can potentially ruin your business, so you need to take all reasonable steps to ensure that you have binding contracts in place to stop that happening.

At the same time, accusing someone of a breach of contract is an extremely serious matter, so a court is going to put the contract that binds them under a microscope.

So you have to be confident that your contracts meet the requirements not just of your business, but also those of a court.

Slide 196

Practical protection of confidential information

Confidentiality will never happen of its own accord. You have to make it happen.

Practical protection of confidential information

- **Label** it as confidential. Leave no one in any doubt
- As routine, **restrict access** to sensitive information – for example, supplier or customer databases. And lock things away!
- Don't be afraid to use **contracts** (restrictive covenants or NDAs) to impose a duty of non-disclosure on employees and third parties
- Seek **professional advice** to make your contracts legally robust

Intellectual Property Teaching Kit

196

The slide shows a list of the main things you actually DO to protect your confidential information. As you can see, there is nothing particularly difficult about any of it.

You should label the information as confidential, restrict access to it, use contracts to impose non-disclosure on employees and others, and seek professional advice to make your contracts legally robust.

The hardest part is probably paying for professional advice, but it will almost certainly be a very false economy if you do without it.

Slide 197

Employee awareness and training

One way of making it happen is to incorporate it into staff training or induction procedures.

The key things to impress on staff are:

- They have a **duty of confidentiality** comparable to that of doctors and solicitors.
- There are sound reasons for taking that duty of confidentiality seriously – and one of them is self-interest. If they want to remain employed, the business has to remain competitive.
- Breaching confidence is not a minor matter. If the consequences for the business are serious, then so too are the consequences for anyone found guilty of causing the breach.

Employee awareness and training

- **Get employees on side** by explaining why it's important – and in their own interests – to keep all work-related information confidential
- Make it clear that all the information they work with **belongs to their employer** – even if it's been created by employees
- Give employees basic **training in IP** generally. Most people simply don't know what IP is and why it's important

Employee awareness and training in IP matters is often overlooked, but could make maintaining confidentiality in the long term much easier.

If you do not want your trade secrets becoming public knowledge, you have to explain to your employees why they should keep work-related information confidential and the potential consequences to employee interests of breaching confidentiality – loss of business, loss of jobs, loss of bonuses, loss of promotion opportunities, and so on.

Slide 198

Trade secrets and know-how in practice

TRADE SECRETS AND KNOW-HOW IN PRACTICE

Intellectual Property Teaching Kit

198

Let us now look at what happened when five cases involving trade secrets and know-how came to court.

Slide 199

Court case 1: Listerine (I)

This is a 1960 US court case relating to a trade secrets contract drawn up in 1880.

STRESS: That fact alone illustrates how long trade secret IP rights can last. By comparison, a patent granted in 1880 would have expired in 1900.

Court case 1: Listerine (I)

- A trade secret licensed to a company is no longer confidential. Is the licensing agreement still valid?



In the interests of accuracy I must point out that the bottles of Listerine you are looking at here are marketed by Johnson & Johnson. It is no longer a Warner-Lambert product.

Slide 200

Court case 1: Listerine (II)

John J. Reynolds was the licensor, and from his point of view it was an extremely good contract. Warner-Lambert and its successors had to pay Reynolds royalties more or less forever.

Even after the formula was published by an independent researcher in 1931, it took almost another 30 years before Warner-Lambert tried to escape from the contract.

Court case 1: Listerine (II)

- 1880: Warner-Lambert Pharmaceutical Co acquired license from John J Reynolds Inc. for the Listerine formula (a trade secret) in return for royalty payments from Warner-Lambert
- 1931: Listerine formula published in Journal of the American Medical Association
- By 1956: Warner-Lambert had paid a total of USD 22 million in royalties
- 1960: court considered Warner-Lambert's request to stop royalty payments

Intellectual Property Teaching Kit

200

In 1880, Warner-Lambert Pharmaceutical Co acquired a license from John J Reynolds Inc for the Listerine formula – a trade secret. In return, Reynolds would get royalty payments from Warner-Lambert.

In 1931 the Listerine formula was published in the Journal of the American Medical Association.

By 1956 Warner-Lambert had paid Reynolds a total of 22 million US dollars in royalties.

It was not until 1960, almost 30 years after the formula was published by an independent researcher, that Warner-Lambert went to court in an attempt to stop the royalty payments.

Slide 201

Court case 1: Listerine (III)

Perhaps against expectation, the court ruled that Warner-Lambert had either to keep on paying royalties or to renegotiate the contract, which had been freely entered into by both parties and had not foreseen the possibility that the Listerine formula might be disclosed independently.

DISCUSSION: What might their chances be of renegotiating the contract?

STRESS: No contract ever gives one party the right to decide unilaterally not to honour their side of the bargain. That would itself be an immediate breach of contract.

The solution is to build escape clauses and termination clauses into the contract – something Warner-Lambert failed to do, to their very substantial cost.

For more details on this case, see:

1. The court decision:

<http://law.justia.com/cases/federal/districtcourts/FSupp/178/655/1642490/>

2. Additional information:

Contracts. Construction. Duty to Pay Royalties for Use of Trade Secret under Contract Specifying No Termination Date Survives Public Disclosure of Secret. Warner-Lambert Pharm. Co. v. John J. Reynolds, Inc. (S. D. N. Y. 1959).

Harvard Law Review, Vol. 74, No. 2 (Dec. 1960), 409-412.

Court case 1: Listerine (III)

Decision

- Court found contract valid and enforceable, and so binding to the parties
- Warner-Lambert should continue to pay royalties, or negotiate a different contract

Lesson

- Make sure that contracts are valid – but also look ahead and consider 'what if?' scenarios
- If you're a Reynolds, the other party has to honour the contract even if the trade secret is no longer secret
- If you're a Warner-Lambert, insist on the inclusion in the contract of escape, limitation or termination clauses as appropriate

The court ruled that Warner-Lambert had to keep on paying royalties. It looked at the 1880 contract that had been freely entered into by both parties, and found no reason in law to stop the payments.

Evidently the 1880 contract had not allowed for the eventuality that the Listerine formula might one day be disclosed, that it might suddenly stop being a secret.

Were Warner-Lambert naive or incompetent? Did they not consider the possibility that the formula might not stay secret forever? Or were they so keen to get the formula that they agreed to everything Reynolds proposed?

We may never know the full story, but we do know the legal consequence. The court ruled that Warner-Lambert must carry on paying up, or renegotiate the contract. Little chance of renegotiation, one might imagine.

Slide 202

Court case 2: Rockwell Graphics (I)

The following court case on Rockwell Graphics goes into allegations of misappropriation of trade secrets in some detail.

Court case 2: Rockwell Graphics (I)

- What counts as misappropriation of trade secrets?
- What are 'reasonable methods' of protecting a trade secret?

In cases based on allegations of misappropriation of trade secrets, the courts have to decide:

- Whether misappropriation has actually taken place – and often that is not straight forward.
- Whether the trade secret was protected well enough in the first place.

Slide 203

Court case 2: Rockwell Graphics (II)

This case relates to Rockwell Graphics, a company which manufactures newspaper presses. Suppliers manufacturing replacement parts for these presses had to work in confidence from highly detailed and securely held piece part drawings. The piece part drawings were central to this case.

Rockwell press parts could not be reverse engineered without dismantling a whole press – hardly a cost-effective tactic – so without the drawings, contractors could not make parts. The manufacturers contracted to make these parts had to sign NDAs, and were given copies stamped 'Confidential'.

Court case 2: Rockwell Graphics (II)

- Rockwell required the return of the drawings – but did not enforce their return all the time
- Former Rockwell employees joined DEV Industries Inc. One of them had been fired for being in possession of piece part drawings

Intellectual Property Teaching Kit

203

Rockwell Graphics could have patented the piece part drawings, as they specified the materials, dimensions, tolerances and methods of manufacture. They considered this unnecessary, as parts could not be reverse engineered without completely dismantling a whole press. The assumption was that anyone who bought a Rockwell press would not see any point in doing that.

Rockwell kept all its piece part drawings in a vault in a building to which only a few authorised employees had access. So far so good – but manufacturers contracted to make parts also had to see the drawings.

The compromise was to make them sign NDAs, and give them copies stamped with words to the effect that each drawing was confidential. Given all that security, it seems unfortunate to say the least that Rockwell was haphazard about getting the copies of the drawings back.

Then a former Rockwell employee who had been fired for being in possession of piece part drawings, joined DEV Industries, a competing manufacturer.

Slide 204

Court case 2: Rockwell Graphics (III)

Unfortunately, Rockwell proved less than diligent about getting all copies of the drawings back.

So Rockwell went to some length to secure its trade secrets – but arguably not enough. And DEV clearly used Rockwell's drawings without permission.

DISCUSSION: But if Rockwell did not pay enough attention to retrieving all its drawings, could they really be regarded as confidential?

Court case 2: Rockwell Graphics (III)

- DEV started manufacturing presses similar to Rockwell products. Rockwell sued for **misappropriation** of trade secrets
- DEV claimed it obtained many Rockwell drawings from different contractors, but could not prove it obtained them lawfully
- Did DEV obtain drawings unlawfully? Former employees took drawings **without permission**
- Did Rockwell really protect its trade secrets? Was Rockwell negligent by not retrieving drawings from contractors?

DEV started manufacturing presses similar to Rockwell products. Rockwell sued for misappropriation of trade secrets. DEV then claimed that it had obtained many Rockwell drawings from different contractors, but could not prove it had obtained them lawfully.

So here are the two questions for the court. Did DEV obtain drawings unlawfully? And did Rockwell really protect its trade secrets, or was it negligent by not retrieving drawings from contractors?

Slide 205

Court case 2: Rockwell Graphics (IV)

The court decided that misappropriation had occurred. Rockwell had not been negligent about secrecy, despite being inconsistent about getting the copies of its drawings back.

Whenever Rockwell sells a printing press it gives the buyer assembly drawings as well. Rockwell does not claim that they contain trade secrets. It admits having supplied a few piece part drawings to customers, but they were piece part drawings of obsolete parts that Rockwell had no interest in manufacturing and of a safety device that was not part of the press as originally delivered.

Court case 2: Rockwell Graphics (IV)

Decision

- The court ruled that Rockwell took 'reasonable' measures to ensure secrecy
- Contractors were given drawings under confidentiality. Even though Rockwell did not enforce their return, this did not invalidate the confidentiality requirement
- Giving drawings to multiple contractors under confidentiality was not dissemination into the public domain

Was there misappropriation? Yes. The former employees removed and passed on drawings without authorisation and so broke their employment contracts.

Was Rockwell negligent by being inconsistent about the return of drawings? Apparently not. The court found that Rockwell had taken reasonable security measures. The drawings had not passed into the public domain because the contractors, having signed NDAs, were still bound by confidentiality.

A factor in Rockwell's favour was that it had a good record of keeping documents safely and restricting access.

Slide 206

Court case 2: Rockwell Graphics (V)

DISCUSSION: How, if Rockwell's physical safeguarding of its drawings was so good, did a disgruntled employee manage to be found with drawings in his possession, presumably **after** he had disclosed them to DEV?

For more information on this case see:

1. The decision: <http://law.justia.com/cases/federal/districtcourts/FSupp/730/171/1984734/>

2. Additional information:

<http://caselaw.findlaw.com/us-7th-circuit/1205525.html>

Court case 2: Rockwell Graphics (V)

Lesson

- The test for misappropriation in this case is:
 - Has the IP owner **maintained and protected** the trade secret?
 - Has the IP owner taken **'reasonable'** steps to ensure protection of the trade secret?
 - Has the other party **obtained the information lawfully or unlawfully**?

It might be argued that Rockwell got off lightly here, and there are certainly lessons in this case study about the need for total diligence. If you put security measures in place, don't let them lapse. You must maintain and protect your trade secrets or you may regret it and lose control of them. You must also take reasonable steps to ensure their protection.

Slide 207

Court case 3: Metallurgical Industries (I)

Based on the case of Metallurgical Industries v. Fourtek we will find out more about what can and cannot be considered a trade secret.

Court case 3: Metallurgical Industries (I)

- What qualifies as a trade secret?

This next case addresses a quite fundamental question: you have got some information – are you justified in calling it a trade secret?

Slide 208

Court case 3: Metallurgical Industries (II)

Metallurgical Industries used ThermoVac furnaces to process spent tungsten carbide and extract carbide for reuse. This required some modification to the furnaces, and the modifications were shown in detail to ThermoVac's representative, Irving Bielefeldt. They were disclosed to him under an NDA, so when he and some other ThermoVac employees set up Fourtek Inc. and began making modified furnaces, Metallurgical Instruments accused him of misappropriating its trade secrets.

Court case 3: Metallurgical Industries (II)

- Metallurgical Industries bought furnaces from ThermoVac Inc and modified them
- The modifications were disclosed to ThermoVac's representative Irving Bielefeldt under confidentiality as a trade secret
- Following ThermoVac's bankruptcy, Bielefeldt and other ThermoVac employees set up Fourtek Inc to make the modified furnaces
- Metallurgical Industries alleged that Fourtek had misappropriated trade secrets disclosed to Bielefeldt

Intellectual Property Teaching Kit

208

Some background is needed here.

Metallurgical Industries bought furnaces from ThermoVac to process spent tungsten carbide and extract carbide for reuse, and then modified them for their own use.

The modifications were shown in detail to ThermoVac's representative, Irving Bielefeldt. He was told that the modifications were trade secrets and that they were disclosed to him under confidentiality.

ThermoVac went bankrupt. Bielefeldt and other ThermoVac employees set up Fourtek Inc and began making the modified furnaces.

Metallurgical Industries alleged that Fourtek had misappropriated the trade secrets disclosed to Bielefeldt.

Slide 209

Court case 3: Metallurgical Industries (III)

Bielefeldt argued that Metallurgical Industries' disclosures to other parties vitiated the secrecy required to obtain legal protection as they had occurred before Bielefeldt allegedly misappropriated the knowledge of modifications. No trade secret in fact existed.

The court stated that “although the law requires secrecy, it need not be absolute. Public revelation would, of course, dispel all secrecy, but the holder of a secret need not remain totally silent: He may, without losing his protection, communicate to employees involved in its use. He may likewise communicate it to others pledged to secrecy Nevertheless, a substantial element of secrecy must exist, so that except by the use of improper means, there would be difficulty in acquiring the information.”

Court case 3: Metallurgical Industries (III)

- Fourtek countered that MI had disclosed the modifications to two other companies **before** speaking to Bielefeldt – so it was not a trade secret but public knowledge

- **Question for the court:** What makes something a trade secret?

Normally:

- Information **must** be a secret
- Reasonable effort must be made to **keep** it a secret
- Information must have **value** (actual or potential)

Bielefeldt could not use the argument that he did not know the drawings were confidential, as he had been told explicitly that they were.

Instead he used the defence that the drawings were already in the public domain, because two other companies saw them before him. He presumably hoped his case would be strengthened because Metallurgical Industries seemed to make little effort to take back all the copies.

In effect he was relying on the principle that, for something to be a trade secret, it must be actively and diligently KEPT a secret. Metallurgical Industries had failed in this regard, which meant that their drawings were not trade secrets but information in the public domain.

Slide 210

Court case 3: Metallurgical Industries (IV)

The court concluded in its decision that a trade secret holder may divulge information to a limited extent without destroying its status as a trade secret. To hold otherwise would greatly limit the holder's ability to profit from his secret. If disclosure to others is made to further the holder's economic interests, it should, in appropriate circumstances, be considered a limited disclosure that does not destroy the requisite secrecy.

The court stated that: "whether a disclosure is limited is an issue the resolution of which depends on weighing many facts. The inferences from those facts, construed favorably to Metallurgical, is that it wished only to profit from its secrets in its business dealings, not to reveal its secrets to the public."

Court case 3: Metallurgical Industries (IV)

The court also considered:

- Did MI incur a cost to maintain the trade secret?
- Did the disclosures to the two earlier companies – before talking to Bielefeldt – amount to public disclosure?
- Did MI disclose their trade secrets themselves, destroying the secret status?

The Metallurgical Industries response:

- MI used NDAs to reveal the trade secret, making it **in effect** a secret, even if not an absolute secret
- The trade secret had value in reclaiming carbide
- The total value of all the modification made up the trade secret
- MI incurred cost in producing the modifications

Intellectual Property Teaching Kit

210

Here is the situation the court had to consider.

Irving Bielefeldt was relying, more or less, on the court deciding that Metallurgical Industries had been neglectful of their own trade secrets, which were now open industry knowledge – so why should he be bound any longer by confidentiality?

Metallurgical Industries claimed that the drawings met all the main trade secrets criteria:

- the drawings had independent economic value
- taken together they added up to a very substantial commercial asset, and
- they were protected by stringent security and an NDA that Bielefeldt had signed.

What do you think?

If you were the judge, would you accept the drawings as trade secrets, or would you accept Irving Bielefeldt's argument that they might have been trade secrets once but no longer were?

Slide 211

Court case 3: Metallurgical Industries (V)

The Metallurgical Industries arguments were affirmed by court.

For more details on this case see:

http://biotech.law.lsu.edu/cases/IP/ts/Metallurgical_v_Fourtek.htm

<http://gozips.uakron.edu/~dratler/2008tradesecc/materials/metal.htm>

Court case 3: Metallurgical Industries (V)

Decision

- The reasons for disclosure to the two earlier companies were **for economic interest** and were **as confidential matter**
- Secrecy does not need to be absolute
- So yes, the drawings were still trade secrets when Metallurgical Industries spoke to Bielefeldt

The court additionally considered the two companies that Bielefeldt claimed had seen the drawings before him.

It concluded that in both instances, Metallurgical Industries had disclosed under confidentiality and had done so to further the company's economic interest – a legitimate use of trade secrets.

One of the companies was going to build furnaces for Metallurgical Industries, while the other was a prospective licensee of the technology including the modifications.

So Bielefeldt and his company Fourtek lost the case comprehensively.

Slide 212

Court case 4: Chicago Lock Company (I)

The following case focuses on another issue connected with trade secrets: reverse engineering.

Court case 4: Chicago Lock Company (I)

- Do trade secrets protect against independent invention or reverse engineering?

What happens when you have protected your know-how or trade secret and it is giving you a definite competitive advantage, and then along comes someone who finds a way round your secret by their own independent effort?

Suddenly your secret is much less valuable. Your new competitor has reverse engineered your product, or has independently invented an alternative that many consumers prefer to yours.

To what extent can you use your trade secret as an IP right to prevent others from taking business away from you?

Slide 213

Court case 4: Chicago Lock Company (II)

The Chicago Lock Company, a manufacturer of “tubular” locks, brought suit against Morris and Victor Fanberg, locksmiths and publishers of specialised trade books, to “enjoin the unauthorised dissemination of key codes for the company’s “Ace” line of tubular locks” (see decision of 6/5/1982, United States Court of Appeals, Ninth Circuit, No. 80-5000, *Chicago Lock Co. v. Fanberg*, para. 1).

Court case 4: Chicago Lock Company (II)

- Chicago Lock Company sold locks with keys that were hard to duplicate. Customers needing a replacement key had to call the company and provide proof of identity
- A faster option (though more expensive) was to call a locksmith to pick the lock to find the tumbler combination
- Morris and Victor Fanberg contacted locksmiths who had noted the tumbler combinations for most lock serial numbers. They then published a directory that allowed anyone to find the right tumbler combination needed to make a key

Intellectual Property Teaching Kit

213

The Chicago Lock Company sold locks with keys that were hard to duplicate. They were clever locks. The company kept the serial numbers and tumbler combinations secret, so anyone needing a replacement key had to call the company, give them the serial number on the lock, then wait to be sent a new key.

Understandably, many customers did not want to wait. They would simply summon a locksmith to pick the lock and get the tumbler combinations. The locksmith could then cut a key immediately.

Defendants Morris and Victor Fanberg had the bright idea of contacting locksmiths, collecting all the serial numbers and tumbler combinations they had found and publishing them as a directory. Locksmiths then did not need to bother picking the locks.

The whole operation cost the customer less and was faster. It brought locksmiths more work, so both customers and locksmiths benefited from the directory.

Slide 214

Court case 4: Chicago Lock Company (III)

In this case the Court of Appeals reversed the District Court decision stating that “the key codes for the Company’s tubular locks were improperly acquired trade secrets” and enjoining distribution of the Fanbergs’ compilation of those codes and order that judgment be entered in favor of the Fanbergs (see decision of 6/5/1982, United States Court of Appeals, Ninth Circuit, No. 80-5000, Chicago Lock Co. v. Fanberg, para. 2).

For more details on this case see:

1. The decision:

<http://files.grimmelman.net/cases/ChicagoLock.pdf>

2. Additional information:

<https://law.resource.org/pub/us/case/reporter/F2/676/676.F2d.400.80-5000.html>

Court case 4: Chicago Lock Company (III)

Question for the court

- Did the Fanbergs obtain the information in their directory improperly or did they discover it independently?

Decision

- The Fanbergs had no case to answer
 - They spent time and effort – amounting to independent discovery – compiling the directory
 - They did not steal the information from Chicago Lock Co.
 - Their compilation of the directory was a 'fair and honest' means of discovery

Lesson

- Trade secrets do not offer protection against independent invention and reverse engineering

Intellectual Property Teaching Kit

214

Based on what you should know by now, it's fairly easy to see why the court decision went the way it did.

The Fanbergs had no relationship with the Chicago Lock Company and had not entered into any contract of confidentiality. Nor did they compete with the Chicago Lock Company in selling identical or similar locks. They didn't in fact sell locks or hardware at all. Everything they did was entirely independent and the outcome of their own entrepreneurialism.

Nor did the locksmiths have any contract of confidentiality with the Chicago Lock Company. They too were free and independent agents. Their primary duty of care was to the customers who paid them for their services.

It's clear therefore that the Fanbergs didn't misappropriate information belonging to the Chicago Lock Company. Nor did the locksmiths.

The Fanbergs acquired information from the locksmiths, who in turn acquired it as a necessary step in doing the perfectly legitimate job the customer was paying them to do.

Another lesson, perhaps, is that companies that try to use trade secrets to control the market too tightly will eventually come unstuck — because others will look for clever ways to beat them at their own game.

Slide 215

Court case 5: Kevlar (I) (optional)

The following case looks at a US Federal Appeals Court decision to award DuPont Co. 919.9 million dollars in compensation for the theft of trade secrets relating to a fibre used to make Kevlar bulletproof vests.

Court case 5: Kevlar (I) (optional)

- How trade secrets can protect an invention even after patent protection lapses



This court case relates to Kevlar, a product made by DuPont. Kevlar is the subject of many patents. Its inventor, Stephanie Kwolek, was a DuPont employee and so the invention belonged to DuPont.

All the original DuPont patents for Kevlar have now expired. Nonetheless, DuPont still dominates the Kevlar market. This case study gives some insight into how it does it.

Slide 216

Court case 5: Kevlar (II) (optional)

Could anything have been done with patents to stop this situation arising in the first place? Fundamentally, no. Once the main Kevlar patents had expired after 20 years, that was it.

Instead, DuPont made the strategic decision to keep the commercial manufacturing process a secret. That had the practical effect of enabling them to keep ownership of Kevlar IP long after the patents had expired.

Was that strategy anti-competitive in spirit?

DuPont legitimately used trade secrets as an IP right, and breach of contract as a deterrent to misappropriation of those secrets. It enabled a company that had spent a fortune on developing Kevlar to prevent an unscrupulous competitor from stepping in and taking much of the economic benefit away from them.

Court case 5: Kevlar (II) (optional)

- DuPont owned several patents relating to Kevlar. Even after the patents expired, DuPont continued to dominate the Kevlar market
- This was possible because DuPont treated most of its technical information about the commercial manufacture of Kevlar as trade secrets or know-how
- Competitor company Kolon sought those secrets by recruiting current and former employees of DuPont
- Kolon was eventually caught holding a huge number of DuPont documents without DuPont's permission

Korean company Kolon Industries tried to take business away from DuPont by hiring former senior DuPont employees who were familiar with the DuPont know-how.

When Kolon's strategy became evident, DuPont took them to court. The complaint was that the former DuPont employees still had a duty of confidentiality to DuPont, and so were guilty of breach of contract, while Kolon was guilty of misappropriating trade secrets.

The court case related to a particular Kolon product called Heracron. One former DuPont employee, Michael Mitchell, pleaded guilty and was sentenced to 18 months imprisonment. DuPont came away with a 919.9 million dollar award against Kolon and a 20-year injunction to stop Kolon selling Heracron and other Kevlartype products.

Slide 217

Court case 5: Kevlar (III) (optional)

The US court decided that trade secrets had indeed been misappropriated and that the actions of Kolon were wilful and malicious.

In 2014 the judgment against Kolon was subsequently appealed and a retrial was pending. (See the chronology at www.scotusblog.com/case-files/cases/kolon-industries-incorporated-v-e-i-dupont-de-nemours-company/).

Date	Proceedings and Orders
Jun 20 2014	Application (13A1265) to extend the time to file a petition for a writ of certiorari from July 2, 2014 to July 23, 2014, submitted to The Chief Justice.
.....	
Oct 8 2014	DISTRIBUTED for Conference of October 31, 2014.
Nov 3 2014	Petition DENIED. Justice Alito and Justice Kagan took no part in the consideration or decision of this petition.)

For more details on this case see:

1. The decision: www.leagle.com/decision/In%20FCO%2020140403113.xml/KOLON%20INDUSTRIES%20INCORPORATED%20v.%20E.I.%20DuPONT%20DE%20NEMOURS%20&%20COMPANY
2. Additional information:
www.reuters.com/article/2014/04/03/us-dupont-kolon-lawsuit-idUSBREA321FB20140403

Court case 5: Kevlar (III) (optional)

Questions for the court

- Was there misappropriation of trade secrets?
- Were the actions of Kolon willful and malicious?

Decision

- Yes and yes
 - DuPont was awarded close to a USD billion in damages and a 20-year injunction preventing Kolon from making Heracron (though in 2014 a retrial was ordered and both sanctions put on hold)

Owing to a successful 2014 appeal that overturned the court's judgment and ordered a retrial, however, this case is far from over. Yet it still illustrates that even the largest companies need protection from predatory competitors – and trade secrets coupled with legally binding contracts can be powerful enough to do the job!

Slide 218

Exercises

The following four exercises are based on a fictional case. Feel free to make this scenario more relevant and interesting by adding details that will tailor it to your own area of technology/expertise.

Exercises

- Fictional description

Fictional description

You own a small research and development company. You have long known of a product called **ProNice**, made and sold by a company called **Fairdeal Ltd**. ProNice is a very successful product; it generates a great deal of sales revenue for Fairdeal.

You have developed the technology for a new product – **iBetter** – which you are confident is superior to ProNice. Trials of prototypes show it to be 40 per cent more efficient and much simpler to manufacture. The factory gate cost is predicted to be around half that of ProNice.

You are now keen to:

- Find a licensee for your iBetter technology.
- Recruit a researcher to help your company carry out further confidential R&D in this technology field.

Slide 219

Exercise 1

Key questions to address:

- Is the information exchanged during the conversation actually confidential?
- Is there any documentation to establish what was disclosed during the meeting?
- Can it reasonably be claimed that Fairdeal Ltd used the iBetter information gained by its employee in a manner that was unlawful or unauthorised?

A relevant real-life US case is *BondPro Corporation v. Siemens Westinghouse Power Generation*. BondPro specialised in bonding dissimilar materials. Siemens Westinghouse made electricity generators.

Siemens Westinghouse had a technical problem with attaching insulation material around a bowl-shaped component. Current practice was to use a slightly larger bowl to compress and harden the insulation material on to the component. The problem was that this often left creases in the insulation that were difficult to remove.

BondPro developed a method that used a vacuum bag rather than the larger bowl. Air pressure then compressed the material without creasing it.

BondPro explained and demonstrated the process to a materials engineer at Siemens Westinghouse. There were some negotiations in confidence and BondPro made it clear that the process was proprietary to them.

Siemens Westinghouse did not seek a licence for the BondPro technology (and never in fact used the technology). Instead they later filed a patent application for a process very similar to that shown to them by BondPro. They claimed that they had developed the solution independently. BondPro accused them of misappropriating a BondPro trade secret.

The court considered these questions: Was confidentiality breached? And if so, did it result in the disclosure of a trade secret?

The court ruled that confidentiality was clearly breached. But the crux of the case was whether the NDA detailed the process that needed protecting.

For it to be a trade secret, the confidential information would have to be rich in detail. This is because a process described in general terms will usually be familiar to someone 'skilled in the art' and will not therefore constitute a trade secret.

The court found that BondPro did not provide enough specifics of the process for the information to be considered a trade secret.

This case is also relevant to Exercise 2.

STRESS: Once information is disclosed, it can quickly seem obvious to the person receiving the information, especially if that person is 'skilled in the art'. With the passage of time it may become difficult to prove that the receiving party did not acquire some or all of the contested information independently.

A UK case – *Seager Ltd v Copydex Ltd, 1967* – established the principle that **even without a confidentiality agreement**, under equity law a person who receives information in confidence cannot take unfair advantage of it.

However, a formal contract of confidentiality is far preferable. It creates certainty and establishes a mutually understood contractual obligation. It sets out in detail the conduct that the disclosing party expects from the receiving party. It also simplifies enforcement by following a procedure that has been tried and tested in the courts many times.

STRESS: Safety first, always. Legally binding confidentiality agreements **must** be entered into **before** starting any commercial negotiations that might involve trade secrets. This applies no matter how friendly and trusting the two parties may have been previously.

Exercise 1

- Scenario
 - You tell a friend who works for Fairdeal Ltd. about iBetter as you hope to get first-hand information from him about the market for ProNice
 - You tell him that your conversation needs to be confidential. But after several months you read a news release from Fairdeal announcing that they will soon be launching a product that is iBetter in all but name
- Question
 - Do you have any legal remedy against Fairdeal?

Let's assume you have a friend who now works for Fairdeal Ltd. You have not seen him since university, but you arrange a meeting. You hope to get first-hand information from him about the market for ProNice, as this may help you get iBetter into the same market.

You tell him that your conversation needs to be confidential. He agrees and seems interested. Encouraged, you tell him about iBetter in considerable detail.

It's essentially an informal conversation, so you do not ask your friend to sign a non-disclosure agreement (NDA).

Several months go by. Finding a licensee for iBetter is taking longer than you expected. Then, to your dismay, you read a news release from Fairdeal. They are soon to launch a

product that is iBetter in all but name.

You have applied for a patent for the iBetter technology – but you filed it **after** you spoke to your friend.

Do you have any legal remedy against Fairdeal?

Slide 220

Exercise 2

Key questions to address:

Did the confidentiality agreement detail (normally in an annexe) what was to be disclosed?

Without such detail it may be difficult to prove that Fairdeal's own independent R&D efforts did not lead them to the iBetter technology.

STRESS: The devil is in the detail, and so the detail in the annexe to the NDA needs to be written very thoroughly and carefully. Too often, courts find that NDAs drafted and relied upon by owners of confidential information are deficient. Detail is unclear, or incomplete, or missing altogether, or in other ways unhelpful.

The more specific, detailed and unambiguous the information written into the confidentiality agreement, the easier it is for a court to agree that a duty of confidence was breached.

A court will also consider the commercial purpose that justified the disclosure as a factor in decisions about wrongfulness.

Exercise 2

- Scenario
 - You negotiate a licensing deal with Fairdeal and sign Fairdeal's NDA, disclosing detailed information about iBetter and how it could be manufactured
 - You have not so far applied for a patent for the iBetter technology
 - Then you discover that Fairdeal has filed a patent application for the iBetter technology
- Question
 - Do you have any legal remedy against Fairdeal?

In the hope of negotiating a licensing deal with Fairdeal – surely iBetter will be just what they're looking for? – you ask for, and are granted, a meeting with a Fairdeal product manager.

You sign Fairdeal's NDA. (They don't want to put their own R&D secrets at risk by talking to you except in strict confidence.)

You have not so far applied for a patent for the iBetter technology.

At the meeting you disclose detailed information about iBetter and how it could be manufactured.

A few months go by. You hear nothing from Fairdeal.

Then you discover that Fairdeal has filed a patent application for the iBetter technology.

Do you have any legal remedy against Fairdeal?

Slide 221

Exercise 3

Key questions to address:

Did Dr Righton obtain the information wrongfully or unlawfully?

At first glance the answer is no. It was sent unsolicited. If the e-mail contained words to the effect that the information was addressed to Dr Right and meant only for the eyes of Dr Right, then it ought to be clear to Dr Righton that the information he received was not intended for him. But will the court take that view?

A 2010 report on trade secrets for the European Commission (report [MARKT/2010/20/D](#)) asked the questions: Can action be taken against innocent recipients of trade secrets? If so, in what circumstances? And what remedies are available?

In Bulgaria, for example, the acquisition, use or disclosure of trade secrets other than in good faith is prohibited. Compensation might be justified, but for a claim to proceed there must be proof of consequential damage or loss.

Germany has unfair competition laws, but Dr Righton would first need to use the information commercially. There would also have to be proof that he knew all along that he was using a secret and acting without authorisation.

In Eire and the UK the key question would be: Did Dr Righton have a duty of confidence – a duty not to disclose or use information?

In this case, on the one hand the e-mail was clearly intended solely for Dr Right, and so it might be argued that there was an implied duty on Dr Righton not to use the information. But, on the other hand, it is equally clear that there was no intended duty of confidence on Dr Righton.

Whatever the answer to that question, there would also have to be proof of actual or imminent damage or loss arising from the misappropriation of the confidential information.

Exercise 3

- Scenario
 - You want to recruit a researcher for another iBetter project: Dr Right
 - By mistake you send the e-mail with technical information and an NDA to someone with a similar name – Dr Righton – who even more unfortunately works for a company that competes with yours
- Question
 - Can Dr Righton now use your research data without your permission?

You want to recruit a researcher for another iBetter project. Dr Right looks promising. She signs your NDA and you then e-mail her the technical information she needs to understand the project.

Unfortunately, by mistake, you send the e-mail to someone with a similar name — a Dr Righton — who even more unfortunately works for a company that competes with yours.

Can Dr Righton now use your research data without your permission?

Slide 222

Exercise 4

Key questions to address:

Is the information claimed as confidential actually confidential?

STRESS: Remember that it is never enough to claim that something is confidential. It must actually be **kept** confidential.

Giving confidential information to friends at a restaurant table is disclosure. If no one was told that the information about iBetter needed to be kept confidential, and no one was asked to sign an NDA — not a popular request, one might surmise — then a reasonable conclusion is that the information disclosed was not actually confidential and so was not a secret.

A US patent case is relevant to the question of whether a disclosure of confidential matter is a public disclosure.

In 1979 someone applied for a patent based on a dissertation published at a German university and archived in its library. Information already disclosed cannot be patented, so could the patent application proceed? It was ruled that it could not. The question the court considered most relevant was not, did somebody read the dissertation, but did the public have access to the dissertation? Yes, they did — so the dissertation was public disclosure.

How many people does the relevant 'public' include?

The US Supreme Court answered this question long ago, and the same principle applies in Europe. In 1855 a Mr Barnes invented improved corset springs and gave a Mrs Cuiger his invention to wear. In 1866, when he wanted to apply for a patent, the court asked:

1. Can the single use of an invention constitute public use? Answer: Yes. Though use by several people would strengthen the evidence of use, a single person will do!
2. Can a use be public even if the invention is hidden from view (as in the case of a corset)? Answer: Yes.

Exercise 4

- Scenario
 - You want to recruit a researcher (Dr Smith) for another iBetter project. You send her an NDA with details of the iBetter technology
 - A few days she signs the NDA, you reveal key details of the iBetter technology to some friends over lunch. It's broadly the same information you sent to Dr Smith
- Questions
 - Can the information you sent Dr Smith be considered confidential?
 - Is the NDA Dr Smith signed legally binding?

You want to recruit a researcher for another iBetter project. You send a NDA to Dr Smith, your preferred candidate. She signs it and you then send her details of the iBetter technology.

A few days before she signs the NDA, you have a meal out with friends. During conversation you casually reveal key details of the iBetter technology. It's broadly the same information you sent Dr Smith. It's spoken rather than written, but some of your friends have enough technical knowledge to understand what you're talking about.

Can the information you sent Dr Smith be considered confidential? Is the NDA Dr Smith signed legally binding?

Slide 223

Conclusions

STRESS: Never overlook the potential of trade secrets and know-how to protect your business and improve its prospects. In many circumstances confidential information can be much more valuable than a patent.

Conclusions

- Guard your trade secrets and know-how:
 - covenants and NDAs
 - restricted access to and use of confidential information
- Be alert to independent discovery or reverse engineering
- Investigate to see if the springboard doctrine might apply
- Be aware that some commercial information may have greater value as a trade secret than as a patent

Never overlook the potential of trade secrets and know-how to protect your business and improve its prospects.

Guard your trade secrets and know-how by having appropriate contracts of confidentiality, including covenants and NDAs, and by being diligent in restricting access to and use of confidential information.

Be alert to independent discovery or reverse engineering that might destroy your trade secrets.

Terms of use

The IP Teaching Kit has been produced by the EPO in co-operation with the EUIPO.

The content provided in this IPTK is for training and information purposes only. The Information is of a general nature only and not intended to address the specific circumstances of any particular case, individual or entity.

It cannot be guaranteed by the EPO and the EUIPO that the information is always comprehensive, complete, accurate and up-to-date. Consequently, no responsibility for any loss or damage that may arise from reliance on the information is accepted by the EPO and the EUIPO.

The information in no case constitutes professional or legal advice.

Users may modify or translate the IPTK and any of its parts on condition that the EPO and EUIPO is credited as the provider of the original and that it is clearly stated that changes have been made to the original material, that the modified or translated version has not been authorised by the EPO and EUIPO, and that the EPO and EUIPO shall not be responsible for the correctness of any such modified or translated version. Any other reference to the EPO and the EUIPO, and in particular their official logo, shall be removed from any such version.

Users shall give the EPO and EUIPO free of charge an electronic copy of the modifications or translations together with the right to further distribute them, if it so wishes, as part of the IPTK, as an additional version or an alternative language version. In such cases, the EPO and EUIPO shall mention the author of the modifications or translations if requested to do so.

The IPTK and any of its parts, as well as any modification or translation thereof, may be used for non-commercial teaching and training purposes only.

For online access to the extensive IPTK collection, plus updates and further learning opportunities, go to www.epo.org/learning-events/materials/kit.html where you will also find a tutorial for teachers and lecturers.

Imprint

Produced by

European Patent Office (EPO) and
European Union Intellectual Property Office (EUIPO)

Published by

EPO Munich
2nd edition
ISBN 978-3-89605-156-1

Concept and co-ordination

European Patent Academy

Content provided by

EPO
EUIPO
Community Plant Variety Office
ip4inno project (www.ip4inno.eu)

Individual modules were produced and/or edited by

Graham Barker
Silvia Baumgart
Robert Harrison
Anu Idicula
Ingrida Karina-Berzina
John Mc Manus
Sérgio Maravilhas Lopes
Anna Yotova

Final editing

EPO Language Service

Design

EPO Graphic Design Munich

Photos

Cover: Thinkstock

IPTK can be downloaded free of charge from the EPO website
at www.epo.org/learning-events/materials/kit.html
and from the EUIPO website
at <https://euipo.europa.eu>

© EPO 2018

European Patent Office
www.epo.org

European Union Intellectual Property Office
www.euipo.eu