

Study on Trade Secrets and Parasitic Copying (Look-alikes)
MARKT/2010/20/D

Report on Trade Secrets for the European Commission

Hogan Lovells International LLP



CONTENTS

SECTION	PAGE
OBJECTIVE AND SCOPE OF STUDY	1
EXECUTIVE SUMMARY	1
Overview of the current system	1
What types of information can be protected?	2
Against whom can action be taken?	2
Employees	2
Third parties	2
Defences	3
Effectiveness of legal procedures	3
MAIN REPORT	5
THE IMPORTANCE OF TRADE SECRETS	5
CONDUCT OF THE STUDY	7
The initial questionnaire	7
The second questionnaire	8
The literature review	9
Discussions with interest groups	9
INTERNATIONAL BASIS FOR TRADE SECRET PROTECTION (TRIPS)	9
OVERVIEW OF PROTECTION OF TRADE SECRETS ACROSS THE EU	10
Austria	10
Belgium	11
Bulgaria	13
Cyprus	14
Czech Republic	14
Denmark	15
Estonia	15
Finland	16
France	17
Germany	18
Greece	19
Hungary	20
Republic of Ireland	20
Italy	21
Latvia	22
Lithuania	23

Luxembourg	24
Malta	24
The Netherlands	25
Poland	25
Portugal	26
Romania	28
Slovak Republic	29
Slovenia	30
Spain	30
Sweden	32
The United Kingdom	33
GENERAL FEATURES OF TRADE SECRETS PROTECTION IN THE EU	35
Information capable of protection	35
Basis of legal protection	36
Trade secrets as intellectual property rights?	38
Applicability of the Enforcement Directive	39
Employees	39
Remedies	40
Search orders	40
NUMBERS OF TRADE SECRET ACTIONS	41
THE EFFECTIVENESS OF COURT PROCEDURES IN TRADE SECRETS ACTIONS	41
GENERAL OBSERVATIONS AND CONCLUSIONS	43

OBJECTIVE AND SCOPE OF STUDY

1. In March 2011, the European Commission appointed Hogan Lovells to carry out a study aimed at providing clarification on the legal framework and practices, in the 27 Member States of the European Union, of trade secret protection and protection against parasitic copying (look-alikes) (the "Study").
2. The objective of the Study is to carry out a comparative law assessment of the legal protection against trade secret infringement and parasitic copying in the different Member States, and to provide the Commission with an overall view of the legal regimes and practical operation of the systems of law governing these matters throughout the European Union.
3. This report considers the protection of trade secrets. (See our separate report on the protection available against parasitic copying). One of the aims of the Study is to identify the main features of the different legal frameworks in the EU Member States for the protection of trade secrets. In this report we have considered the nature of the rights conferred, the judicial procedures and remedies available, perceived inadequacies in the current law and best practice. Our report focuses on the civil law but given that the criminal law is an important means of protection of trade secrets in some Member States we have included some commentary on the criminal law.

EXECUTIVE SUMMARY

OVERVIEW OF THE CURRENT SYSTEM

4. There is no harmonised system for the protection of trade secrets within the EU. All Member States offer some form of protection although in one or two Member States protection is extremely limited. The manner of protection varies from State to State and the law and procedure in some States is uncertain. It should be noted that the absence or existence of specific legislation dealing with trade secrets is not necessarily an indication of whether effective action can be taken in a country. Common law countries, such as the UK and the Republic of Ireland, have effective trade secret protection despite having no specific trade secret legislation.
5. Although trade secrets are not generally viewed as intellectual property rights¹ and most Member States' legislation does not treat rights in trade secrets as intellectual property rights, there is, at the very least, a close relationship between them. Some Member States regulate protection of trade secrets by statute in a similar manner to "traditional" intellectual property rights such as patents, trade marks and copyright. One Member State (Sweden) has an Act on the Protection of Trade Secrets. Other Member States (such as Germany) have trade secret provisions in legislation aimed at, for example, unfair competition, labour laws and criminal law. Other Member States, notably the UK and the Republic of Ireland, have no statutory form of protection for trade secrets and use the law of confidence to protect them. In yet further jurisdictions (such as the Netherlands) general tortious liability extends to trade secret infringement. Contractual liability is used to protect trade secrets, in particular in relation to employees, in most Member States. In one Member State (Malta) protection arises solely from the law of contract so there is no means of protection where no contractual relationship exists.

¹ This is a subject of academic and judicial debate (see below).

What types of information can be protected?

6. There is no uniform definition of "trade secrets" within the EU. Some States (for example, the Czech Republic) appear to apply (formally or informally) the definition of "undisclosed information" provided in Articles 39(1) and (2) of TRIPS².
7. What is protectable varies from State to State. In common law countries the law of confidence potentially protects all types of confidential and secret information whether it is commercial, industrial or personal. In some other countries, for example, Belgium and France, there is specific statutory protection against disclosure by employees and former employees of manufacturing or process information but different protection for commercial information.

Against whom can action be taken?

8. There is a lack of consistency between States as to the individuals against whom action can be taken. In some countries action may be taken against anyone who has received confidential information; in others against only those with whom some contractual relationship exists. Possible defendants may include, current and ex-employees, actual and potential licensees, competitors, independent third parties receiving information (sometimes accidentally and/or innocently) and those involved in industrial espionage. Public authorities also have responsibilities in relation to information coming into their possession³.

Employees

9. Most jurisdictions provide for contracts of employment to be enforced against employees during the term of their employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment.

Third parties

10. Often information will be disclosed to a party with whom the "owner"⁴ of the information has no contractual relationship. One example is where information is disclosed during contractual negotiations but no contract is concluded. Another is where a company has received information perhaps via a disaffected employee or a dishonest person. In some countries, such as Italy (if the recipient was aware of the misappropriation), the competitor will be open to an action for unfair competition and in the UK a duty of confidence may be implied by the circumstances; in some others (or if the recipient acquires the information in good faith) no action can be taken. The absence of a remedy in such circumstances can be particularly serious.
11. A special case is where a person receives information quite innocently – perhaps as a result of a mistake such as a wrongly addressed email. In a number of countries no action can be taken. For example, in Sweden, the Act provides that a recipient of information will be liable to compensate the owner if he wilfully or negligently reveals a trade secret which he understood, or ought to have understood, to have been revealed contrary to the statutory provisions. However, there are no remedies if a person receives a trade secret in good faith. In common law countries it will be possible in many cases to

² Agreement on Trade-Related Aspects of Intellectual Property Rights (Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.)

³ See paragraph 18 below.

⁴ In most Member States trade secrets are not regarded as property and so cannot be "owned" as such, but we will use the term "owner" for convenience.

obtain an injunction against an innocent but uncooperative recipient and an order for delivery up of any documents but no damages. In many countries nothing can be done.

Defences

12. The main defences available are generally similar⁵; primarily that the necessary ingredients of the claim are absent. (For example, the information is not a trade secret; there was no misappropriation; or the information was independently developed.) The fact that the responsibilities of third party recipients and ex-employees vary from State to State will, in itself, generate some differences in the defences available.

Effectiveness of legal procedures

13. Of course there has to be a suitable legal basis of protection. However, whether or not the law is of any real assistance in practice depends as much on whether there are effective procedural tools in place and how the courts implement them. Problems that have been noted are:

- (a) The local legal procedure is not always helpful in ensuring continual protection of the trade secret. For example, although in some jurisdictions (e.g. England) applications can be made for certain parts of the case to be heard in private to preserve the secrecy of the trade secret, in others the public can only be excluded from some hearings for reasons relating to security, public order or decency (e.g. Italy). In most countries, while pleadings are public documents, the trade secret itself can be kept confidential. This appears to be in line with TRIPS (see below). However, in Belgium in order to pursue a case, it is necessary to plead in writing the information that is alleged to be secret. These pleadings can be open to public inspection as can the submissions and evidence at the trial. Accordingly, unless the information has already become generally known, it may not be worthwhile to pursue a case.
- (b) There can be considerable difficulties in obtaining sufficient evidence of misuse.^{6,7} By their special nature dealings in trade secrets are unlikely to be publicly disclosed. Moreover, people dealing in other people's secret information are frequently dishonest; thus when accused of a trade secret violation they will conceal and/or destroy documents and computer files. This can be a serious obstacle to substantiating the claim and taking effective action.

In common law jurisdictions this problem has to some extent been dealt with by the use of ex parte search orders. These will be granted where there is a strong prima facie case and there is evidence that the proposed defendant will conceal or destroy materials if given advance notice. In common law jurisdictions these procedures have been very effective in dealing quickly and effectively with dishonest activity and can bring matters to an early conclusion. The Enforcement Directive⁸ provides for seizure of materials on an ex parte basis in appropriate cases in relation to intellectual property⁹. However, most Member States do not view trade secret rights as intellectual property and have not applied the

⁵ In the 6 countries that were the subject of a more detailed analysis, viz: Belgium, Bulgaria, Germany, Italy, Sweden and the UK.

⁶ These problems and proposed solutions are discussed in the Commission Staff Working Document SEC (2010) 1589 final (Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States).

⁷ Similar issues arise in relation to products suspected of infringing process patents. An attempt to deal with it has been made by reversing the burden of proof in certain circumstances. (TRIPS Article 34.)

⁸ Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States.

⁹ Article 7 (Measures for preserving evidence).

Enforcement Directive to trade secret cases. As the Commission has already observed in its evaluation of the working of the Directive, the existing provisions are:

"Understood in different ways in the different Member States and have given rise to different interpretations and applications in practice¹⁰."

So, even if the Enforcement Directive were to be applied specifically to trade secrets, it is not clear how the Member States would apply the provisions in Article 7 relating to the preservation of evidence, and, in particular, the "optional" provisions relating to "physical seizure". For the reasons explained above these provisions have even more relevance to trade secret violations than other types of intellectual property. Moreover, the Enforcement Directive stops short of providing for specific powers of search.

In some countries where the courts already have such powers they seem reluctant to use them. Others allow the defendant to avoid answering questions or providing any document that may incriminate him¹¹. However, in many countries where civil search and seizure orders are, in theory, available they appear to be of limited effectiveness, for one or more of the following reasons:

- (i) the burden of proof is very high and in practice cannot be overcome;
 - (ii) a search order can only be obtained on an inter partes basis;
 - (iii) the search can only be conducted by court officials without the assistance of the plaintiff's representatives. This means that it may be difficult to identify relevant materials and there may not be the necessary persistence. This is a particular problem where the subject matter is technically complex and/or where the activities are on a large scale.
- (c) There are evidentiary problems in proving the loss incurred (see Finland for example).
- (d) It is very important in many cases to determine who has access to or possession of information. A useful tool to prevent further misuse is an order that those from whom information has been unlawfully obtained and those to whom it has been given are identified. The law in some States does not permit or provide for procedures of this type which means that there cannot be any assurance that the "leak" has been sealed.
- (e) In some countries there is no, or no clear, power to grant "permanent" injunctions. In Belgium, for example, "permanent" injunctions¹² will not be granted at all. In Denmark, the courts appear unwilling to grant a final injunction for longer than two to three years even if the information is still secret at the end of that period. This means that whilst damages may be available there is no power to stop continued abuse.

¹⁰ See Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights, COM (2010) 779 final at page 4 and Staff Working Document, SEC (2010) 1589 final.

¹¹ But any such right should not extend to the production of pre-existing documents. It is also doubtful that Article 8 ECHR can be relied on to any real extent in relation to business premises. *Case C301/04 P Commission v SGL Carbon* [2006] ECR I-5915.

¹² In reality few injunctions are truly "permanent". They will only last while confidentiality is preserved. In any event if the information is being exploited fairly there seems no reason why it should not be protected. It should also be noted that trade secret rights do not create a monopoly (unlike patents); there is no restriction on others generating the necessary information through their own effort.

MAIN REPORT

THE IMPORTANCE OF TRADE SECRETS

14. Trade secrets are very important to industry. Technical know-how and commercial information can be the result of considerable investment, skill and labour. Some features may be patentable or protected to some extent by other "traditional" intellectual property rights such as copyright or design rights but in the main such protection provides very limited protection in practice. This may be because the information may simply not be patentable – for example it may be a mass of information as to designs and specifications or detailed process information, which may not contain any invention but which, nonetheless, may be very valuable.
15. By creating a right to protect information, some argue that trade secrets law acts as an incentive for investment in technological development. Trade secrets law gives the means to exclude third parties from misusing valuable knowledge and thus increases competitive advantage and the expected returns of innovation. It also provides a basis for technology transfer. Some commentators, however, argue that due to the possibility of keeping trade secrets confidential indefinitely, their protection actually hinders competition (unlike patents which require publication of the invention in return for a limited monopoly right). This argument is only persuasive up to a point; there are fundamental differences in the type of protection afforded by patents and rights in trade secrets. A patent provides a monopoly in relation to the exploitation of the invention during the term of the patent; confidentiality does not. Whilst independent development is generally no defence to an action for patent infringement¹³ it is in relation to an infringement of trade secret rights. Patents protect the features of innovative products even after the product is put on the market; trade secrecy is limited in that in general it can only protect information as long as it is not made public. If the protected features (or the protected combination of features) are apparent from the marketed product the protection is at an end.¹⁴
16. Businesses in Europe tend to employ a combination of patent and know-how protection to protect their technology. Secret know-how concerning, say, the best mode of practice of a patented invention is often licensed together with the related patents, indicating the close relationship between patents and trade secrets or know-how. Some inventions may not be patentable, while others may warrant protection beyond the standard twenty year term of a patent. In both cases, the law of trade secrets can provide valuable protection for such inventions. Trade secrets in that respect are a very flexible form of protection.
17. Commercial information such as pricing or costing information, lists of customers or suppliers and business plans can also be extremely valuable. Naturally, the acquisition of such information without the need to make the required investment is advantageous to existing competitors or companies seeking to enter the market.
18. The importance of trade secrets is also recognised in the public sector. Public bodies receiving information have a general duty to adhere to Article 1 of the European Convention on Human Rights.¹⁵ Express obligations to respect trade secrets also arise in various specific circumstances such as competition investigations and in relation to public procurement contracts. The 2004 Public Procurement Directive¹⁶ provides:

¹³ Prior secret use provides a limited defence in some cases.

¹⁴ Note that the English Courts have granted injunctions for limited periods even though the information has become public in order to compensate for the head start gained by the wrongdoer.

¹⁵ "Every natural or legal person is entitled to the peaceful enjoyment of his possessions."

¹⁶ Directive 2004/18/EC of the European Parliament and the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts.

"Confidentiality

Without prejudice to the provisions of this Directive, in particular those concerning the obligations relating to the advertising of awarded contracts and to the information to candidates and tenderers ... the contracting authority shall not disclose information forwarded to it by economic operators which they have designated as confidential; such information includes, in particular technical or trade secrets and the confidential aspects of tenders." (Article 6)

The underlying rationale was explained by an English Court of Appeal judge as follows:

"...it is plain that there is a strong public interest in the maintenance of valuable commercial confidential information ... If the penalty for contracting with public authorities were to be the potential loss of such confidential information, then public authorities and the public interest would be the losers, and the result would be potentially anti-competitive^{17, 18}."

19. The need for effective protection has increased in recent years for a number of reasons. There has been a growth in the "information economy" in developed countries. Also, in order to compete effectively there has been a growth in the outsourcing of manufacture¹⁹. This has substantially increased the risks of manufacturing and design information being misused or "stolen". Another factor is the ease with which large quantities of documents and data can be downloaded, stored and transmitted. Until relatively recently the "stealing" of secret documents was a very risky and time consuming process – documents would have to be photocopied and removed as hard copies or photographed and prints made. Now documents are increasingly stored electronically and it is relatively quick and easy to download them. Large amounts of information, for example, can be stored on a memory stick that can be dropped in a pocket. The answer to this is not simply in ensuring the law is in place but also providing practical means which enable activity of this type to be detected, "stolen" documents to be located and seized, and the perpetrators identified.
20. The seriousness of this has been recognised in the United States where there have been a number of criminal cases involving attempts to expropriate trade secrets, in many cases to export trade secrets abroad. The types of information varied in these cases and included Windows source code, Microprocessor design technology, Coca-Cola marketing information, fire-proofing ingredients, process technology for manufacturing the anti-cancer drug Taxol and military aircraft training software. Not only has the US introduced dedicated criminal sanctions but also specific legislative measures to encourage an acceptable level of protection under the civil law.
21. The number of trade secret cases commenced in Europe appears to be increasing rapidly, in particular, in the UK.²⁰ This may be due to an increasing awareness of the importance of trade secrets.
22. Trade secrets are extremely important to certain industries. The pharmaceutical and biotech industries rely heavily on rights in know-how (either as a complement to or alternative to patent protection). For example, one of the largest European biotech trade secrets disputes in recent years involved a strain of bacterium used in the manufacture of

¹⁷ *Veolia v Nottinghamshire CC [2010] EWCA 1214 per Rix LJ.*

¹⁸ *See Varec v Belgium [2008] 2CHLR 24* where the Court (citing Article 287 of The EC Treaty and Article 41 of the Charter of Fundamental Human Rights) stated that the right to protection of business secrets was recognised by Community law.

¹⁹ *See Intellectual Property in Global Sourcing, Baldia, S 38 Geo. J. Intl. L. 499.*

²⁰ *See UK Ministry of Justice Statistics, 2010 (although these statistics may include some privacy cases).*

an antibiotic. The dispute was of major importance to both companies involved given that the antibiotic had annual sales of over US \$1 billion.²¹

23. Trade secrets are very important to the software industry too. Copyright protects object code but a third party having access to source code can use it to produce software with the same functionality as the original software but different enough to avoid infringing the copyright. Therefore, source code is usually kept secret.
24. The food industry also uses trade secrets. The most often cited example of a trade secret is the formula of Coca Cola.

CONDUCT OF THE STUDY

25. Research for the Study has included three main elements:
 - (a) a questionnaire based survey of the 27 Member States;
 - (b) a more detailed follow up questionnaire directed to six Member States selected on the basis of geographical diversity and for the legal systems available; and
 - (c) a literature review. We have also reviewed materials supplied by the Commission and the Trade Secrets and Innovation Coalition interest group.

The initial questionnaire

26. Questionnaires were sent to intellectual property law practitioners in each Member State to assess the structure and operation of the trade secret laws in their respective countries, including relevant aspects of procedure. A list of the practitioners to whom questionnaires were sent is set out at Appendix 1 of this report.
27. Their responses to the initial questionnaire are set out in Appendix 2. The following questions were asked:
 - (a) Does the legislation of your Member State provide specific provisions on the protection of trade secrets? (Where so, practitioners were asked to provide the text of the relevant provisions and the context and field of law in which protection derives.)
 - (b) Where your Member State does not provide specific legislation on the protection of trade secrets, indicate the legal provisions that can be used in order to secure protection against trade secrets infringement. Again the context and field of law for each provision were requested.
 - (c) Are trade secrets considered to be intellectual property and protected as an intellectual property right? Is the legislation that implemented the Enforcement Directive applicable to the protection of trade secrets in your Member State?
 - (d) What elements must be established in order to be able to launch a legal action against trade secret infringement?
 - (e) What remedies are available for infringement?
 - (f) Are ex-parte search orders available?

²¹ Keeping the strain secret was the only practical means of protection. In such a case the strain could be the result of many years' development.

The second questionnaire

28. A second questionnaire was sent to the same intellectual property law practitioners in six selected Member States to provide a more detailed analysis of the law and practice in those jurisdictions. Their responses are set out in Appendix 3.
29. The six Member States were selected in order to be as representative as possible of the EU, taking into account the different approaches revealed by the answers to the first questionnaire. The chosen States were:
- (a) Belgium
 - (b) Bulgaria
 - (c) Germany
 - (d) Italy
 - (e) Sweden
 - (a) The UK
30. The following questions were asked in the second questionnaire:
- (a) What difficulties have plaintiffs encountered in civil proceedings in enforcing trade secret protection? In this regard the following were considered:
 - (i) What forms of interim relief, if any, are available?
 - (ii) Are final injunctions time limited?
 - (iii) What is the average duration of proceedings from initiating the claim to final judgment?
 - (iv) Are cases involving technical trade secrets heard by specialist judges?
 - (v) What measures are put in place to protect the secrecy of information during the proceedings?
 - (vi) Approximately how many trade secret actions are heard by the civil courts each year?
 - (b) Can action be taken against innocent recipients of trade secrets and if so, in what circumstances? What remedies are available?
 - (c) What defences are available?
 - (d) Which different types of trade secrets are recognised?
 - (e) In taking action for misuse of secret information does the court or legislation consider the importance of the information in determining whether or how it can be protected?
 - (f) To what extent can an employer prevent an employee misusing or disclosing its trade secrets during employment and once the employee has left? Examples of contractual clauses for contracts of employment to address employees and former employees misusing or disclosing trade secrets were requested.
 - (g) Perceived inadequacies of the law on trade secrets and suggested improvements.

- (h) A list of leading case law to demonstrate the ways in which trade secrets are protected was also requested.
- 31. Examples of clauses for contracts of employment designed to address use of confidential information during and after employment can be found at section 6 of each response at Appendix 3.
- 32. The responses to both questionnaires have been summarised by Hogan Lovells in tabular form at Appendices 4 and 5 of this report.

The literature review

- 33. In addition to the questionnaires we were asked to carry out a review of relevant literature in the English language from the last five years, in particular seeking out literature which provides a comparative study between different jurisdictions. A list of the relevant literature identified is set out at Appendix 6 to this report.
- 34. Recent English language literature on the protection of trade secrets in Europe is limited; in particular there are few comparative law analyses. Confidential information is often referred to as a "Cinderella" of IP rights and so this lack of literature is not surprising. Much more literature exists in the US where the protection of trade secrets has a higher profile. We have included some literature on the US system.

Discussions with interest groups

- 35. We were contacted by the Trade Secrets and Innovation Coalition (TSIC). The TSIC is a recently formed coalition of European businesses from different industries formed to highlight the importance of trade secrets in the context of innovation.

INTERNATIONAL BASIS FOR TRADE SECRET PROTECTION (TRIPS)

- 36. The international basis for the protection of trade secrets is set out in Article 39 of the World Trade Organisation's 1994 TRIPS Agreement (Agreement on Trade-Related Aspects of Intellectual Property Rights). The TRIPS Agreement sets out minimum levels of protection for intellectual property rights of WTO Members. There are 153 Members of the World Trade Organisation including all 27 EU Member States.
- 37. Article 39 (Protection of undisclosed information) provides:
 - 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 utilise 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.*
38. Footnote 10 of the TRIPS Agreement states that "a manner contrary to honest commercial practices" shall mean "at least practices such as breach of contract, breach of confidence and inducement to breach, and includes the acquisition of undisclosed information by third parties who knew, or were grossly negligent in failing to know, that such practices were involved in the acquisition."
39. Article 10bis of the Paris Convention (unfair competition) provides:
- (a) *The countries of the Union are bound to assure to nationals of such countries effective protection against unfair competition.*
- (b) *Any act of competition contrary to honest practices in industrial or commercial matters constitutes an act of unfair competition.*
- (c) *The following in particular shall be prohibited:*
- (i) *all acts of such a nature as to create confusion by any means whatever with the establishment, the goods, or the industrial or commercial activities, of a competitor;*
- (ii) *false allegations in the course of trade of such a nature as to discredit the establishment, the goods, or the industrial or commercial activities, of a competitor;*
- (iii) *indications or allegations the use of which in the course of trade is liable to mislead the public as to the nature, the manufacturing process, the characteristics, the suitability for their purpose, or the quantity, of the goods.*
40. Article 39 of the TRIPS Agreement provides a relatively flexible framework of trade secret protection and Member States have enjoyed a certain freedom with respect to how they should implement these provisions.

OVERVIEW OF PROTECTION OF TRADE SECRETS ACROSS THE EU

Austria

41. Austria's Unfair Competition Act provides civil and criminal sanctions against trade or business secret misuse by employees and those who exploit such information without consent for the purposes of competition. Other legislation such as the Patents Act and the Criminal Code also provides legal remedies in particular circumstances, such as disclosure of inventions by employees or in cases of industrial espionage. In addition, the Austrian courts have held that obtaining trade or business secrets by breach of confidence (in the course of contractual negotiations) falls within the Unfair Competition Act.

42. There exists no statutory definition of "trade or business secrets" in Austria but the judiciary and legal scholars have devised a definition. This definition applies to all types of information, such as manufacturing, product technology, business information (such as customer and supplier lists) and know-how.
43. Austrian law does not contain a definition of intellectual property as such. The Enforcement Directive has not been implemented insofar as trade secrets are concerned.
44. To commence legal proceedings for trade secret infringement in Austria it is necessary to establish:
 - (a) the existence of the trade or business secret;
 - (b) the misappropriation of that secret by the infringer;
 - (c) the infringer's imminent intent to use or disclose such secret; and
 - (d) that the owner has a reasonable interest in its secrecy.
45. Civil remedies available in Austria are an injunction (interim injunctions are also available) and damages. A claim for damages requires fault on the part of the defendant (but a claim for cease and desist may be brought against an innocent infringer). A claim for damages can include loss of profits. Although there is no ability to obtain an account of the infringer's profits under the Unfair Competition Act, the Austrian Supreme Court has granted an account in cases of passing off by analogous application of Section 151 of the Patents Act.
46. Under the Austrian Code of Civil Procedure it is possible to preserve evidence in civil proceedings but only by the hearing of witnesses, evidence by inspection (typically inspection of production facilities and machines) and court expert evidence. Preservation of evidence may only be ordered by the court if the plaintiff can show that without the grant of the order he will lose the ability to bring evidence. In case of imminent danger, the court may order ex parte preservation of evidence.
47. The Code of Enforcement provides that the court may grant interim injunctions to prevent the frustration of a claim and to secure evidence if there is a danger that the defendant might destroy evidence.
48. There are very few criminal convictions for trade secret violations in Austria. Such infringement is punishable by imprisonment or a fine. Prosecution only takes place at the injured party's request. The injured party may file a criminal action but the preliminary investigation is not open to him.

Belgium

49. There is no one piece of legislation on the protection of trade secrets as such in Belgium but there are several provisions of Belgian law which can be used against the misuse or disclosure of trade secrets. Trade secret owners generally rely on the general law of tort, unfair competition and specific provisions in Belgian criminal and labour law.
50. The Belgian Criminal Code protects manufacturing secrets (technical data including plans, drawings, materials or manufacturing processes). Individuals working or having worked in a factory may not disclose manufacturing secrets to third parties. Disclosure is punishable by imprisonment or a fine.
51. The Labour Law also prevents an employee from disclosing, during or after his employment, trade secrets belonging to his employer. The general law of tort (see Article

1382 of the Belgian Civil Code) can also be invoked to compensate trade secret misuse. Undertakings can also rely on the Unfair Competition Law to prevent misappropriation and use by another undertaking of trade secrets where such misappropriation or use could cause prejudice. However, as explained below, it is difficult or impossible in practice to get an injunction against the use of a misappropriated trade secret.

52. Trade secrets are not considered to be intellectual property in Belgium. As a result, the Enforcement Directive is not applicable to trade secrets in Belgium.
53. How to commence legal proceedings for trade secret infringement depends on the legal basis of such proceedings. In order to start an action against a company or an individual (not an employee) for unauthorised use or disclosure of trade secrets (based on the general law of torts), the plaintiff must prove:
 - (a) the defendant has committed a civil wrong i.e. has behaved in a way which is not consistent with the behaviour of a normal, careful person placed in the same circumstances;
 - (b) the defendant's behaviour has caused prejudice to the plaintiff; and
 - (c) there is a causal link between the behaviour and the prejudice.
54. In order to start an action against an undertaking for unfair practices under the Unfair Competition Law, the plaintiff must prove:
 - (a) the plaintiff and defendant are undertakings within the meaning of the legislation;
 - (b) the defendant committed an act contrary to fair market practices (misuse or disclosure of the trade secrets of another is usually considered by the courts to be such an act); and
 - (c) the misuse or disclosure has caused or threatens to cause prejudice to the plaintiff.
55. Preliminary injunctions are available and in cases of extreme urgency an ex parte application may be made. If an action is brought under the Unfair Competition Law, it is also possible to expedite the main action provided the claim is not based on a breach of contract.
56. In an action on the merits, the plaintiff can seek an injunction and damages. However, the Belgian court has refused to grant orders prohibiting the use of misappropriated trade secrets on the basis that this would grant the holder of a trade secret potentially broader protection than a traditional IP right as the prohibition could last forever. Damages are compensatory and are not based on the infringer's profits. However, the plaintiff can ask for the infringer's profits to be taken into account to demonstrate the plaintiff's lost profits.
57. Although laws are in place to protect trade secrets, plaintiffs in Belgium face serious problems in enforcement. The plaintiff must usually describe his trade secret in his pleadings and can be forced by the court to file documents describing the trade secret. Court hearings (and decisions) are public, again leading to possible further disclosure of the trade secret. The court must also describe the trade secret in its judgment when it issues a cease and desist order (injunction). Although the court can decide that some confidential information should not be disclosed in the decision in order to limit public disclosure²², this is not the usual practice and cannot be relied upon. The enforcement

²² See, for example, Brussels Court of Appeal, 20 June 2008, ICIP 2008, p.566 where the serotypes of GSK's vaccine were blanked out.

system in Belgium does appear to work against the interests of the holder of a trade secret and may discourage litigation. Preventing further disclosure of the trade secret is usually the plaintiff's main aim in litigation as damages may not be an adequate remedy. A system which requires further disclosure of the trade secret to bring a successful claim cannot be attractive to most plaintiffs.

58. Ex parte orders to search premises and computer systems for misappropriated data and to require the defendant to provide information are not available in Belgium. Such ex parte orders are only available to IP rights holders.

Bulgaria

59. There is no specific legislation on trade secrets in Bulgaria but various laws including the Law on Protection of Competition and the Law on Access to Public Information contain general provisions which may be used to protect trade secrets. In fact, there are over 60 such statutory and non-statutory provisions (including criminal liability under the Criminal Code).
60. Trade secrets are not considered to be intellectual property in Bulgaria. Thus the Enforcement Directive is not applicable to trade secrets.
61. In order to claim compensation in tort in civil proceedings for trade secret misuse, the plaintiff must demonstrate that the defendant has breached a statutory duty not to disclose a trade secret. Fault is presumed to exist until otherwise proven. In contract, damages are available on proof of breach. Other elements to be established depend on the contents of the contract.
62. Proceedings under the Law on Protection of Competition may be brought by any person affected by a breach of the statutory non-disclosure obligation in that law. In particular, the acquisition, use or disclosure of trade secrets other than in good faith is prohibited. The Commission on Protection of Competition (CPC) who will hear the case cannot award compensation to the plaintiff but a claim for compensation can be made before the court.
63. The CPC can impose interim measures such as cessation of commercial malpractice. The plaintiff may also seek interim relief in proceedings before the court. Final injunctions, as such, are not provided for under Bulgarian law although interim injunctions, save in limited circumstances before the CPC, are not subject to specific time limits.
64. Damages are the most common remedy sought in Bulgaria. If the claim is brought in tort, damages are compensatory and can include non-pecuniary losses. In contract, further remedies are available. Generally, contractual damages are limited to compensation of direct and proximate material losses which were foreseeable at the time of entering the contract. However, if the defendant has acted in bad faith he should be liable for all direct and proximate losses.
65. In civil proceedings, the court may order (and execute) an inspection of property in order to collect and verify evidence. Parties may also request evidence be secured where there is a danger that such evidence may be lost. The Civil Procedure Code does not specify the method of collection. There is also no specific provision on the presence of the plaintiff's representatives, so they may be permitted to attend. In proceedings before the CPC, the CPC itself may conduct onsite inspections and seizure of evidence. Inspections are authorised by a court order issued by the administrative court in Sofia at the request of the chair of the CPC.

Cyprus

66. Overall, protection for trade secrets in Cyprus is very limited. There is no specific legislation governing trade secret misuse in Cyprus but there are a number of different laws which mention trade, business and professional secrets. For example, the Commercial Descriptions Law, the General Product Safety Law and the Competition Law. However, liability is criminal; there is no civil liability for trade secret misuse.
67. Trade secrets are not considered to be intellectual property in Cyprus and the Enforcement Directive is not applicable to the protection of trade secrets.
68. While it is technically possible to obtain ex parte orders to search premises and computer systems for misappropriated data or information, in practice the courts are very reluctant to grant such orders.

Czech Republic

69. The Czech Commercial Code defines a trade secret and provides remedies for trade secret infringement. The TRIPS Agreement is directly applicable in Czech law and thus the definition of a trade secret under Article 39(2) of the TRIPS Agreement also applies in Czech law. The basis of trade secret protection in the Czech Commercial Code, however, is the civil law of unfair competition.
70. As in most EU States, trade secrets are not considered to be intellectual property and so the Enforcement Directive is not applicable.
71. In order to prove trade secret misuse, the plaintiff must demonstrate that:
 - (a) the information (commercial, manufacturing or technical) has actual or potential value;
 - (b) is not commonly available in the relevant business circles;
 - (c) has been maintained in secrecy; and
 - (d) the plaintiff has adequately ensured its secrecy.

In practice, the plaintiff will need to show that appropriate measures were in place to ensure the secrecy of the information.

72. The civil remedies available in the Czech Republic are an injunction, damages, recovery of unjustified enrichment (an account of the infringer's profits), satisfaction of immaterial injury (such as an apology) and an order to remove the infringing goods.
73. Trade secret violation is also a criminal offence punishable by imprisonment or payment of a fine.
74. Although the Czech Civil Procedure Code includes a general provision to secure evidence before commencement of proceedings, this provision is very rarely used. In practice, no ex parte order to search the premises and computer systems or to require the defendant to provide information as to the whereabouts of documents is available in civil

proceedings. However, the police may carry out a search of premises in criminal proceedings.

Denmark

75. In Denmark there is no statutory definition of trade secrets; however case law has clarified the types of information that are protectable to include both technical and commercial information. Several statutes, both civil and criminal, are used to protect the rights of trade secret owners as well as legal principles derived from contract law, competition law, employment law and unfair competition law. Most notably, the Criminal Code and the Marketing Practices Act contain provisions protecting trade secrets.
76. Trade secrets are not considered to be intellectual property under Danish law and so the Enforcement Directive is not directly applicable to trade secrets in Denmark.
77. In order to succeed in a civil claim for trade secret infringement in Denmark, the plaintiff must establish that:
 - (a) the information constitutes a "trade secret" (i.e. information about the trader's internal matters which could comprise technical or commercial information);
 - (b) the plaintiff is authorised to bring the claim i.e. that he is the "owner" of the trade secret or is authorised by the owner to take legal action; and
 - (c) the defendant has committed a violation of the Marketing Practices Act.
78. It is possible to obtain an interim injunction. Permanent injunctions are also available but their value is limited since they are normally limited in time to two to three years from the commencement of the infringement. Damages are also available. The infringer's profits may be taken into consideration when assessing the plaintiff's loss. However, the courts are quite strict when considering damages and the damages awarded often do not amount to the plaintiff's full loss.
79. In addition, the plaintiff can be granted an order for the infringer to deliver up or destroy the infringing products. The defendant may also be required to publish a statement on the infringement on its website, for example.
80. Trade secret violation is also a criminal offence under the Criminal Code and the Marketing Practices Act. The maximum penalty is six years imprisonment (for industrial espionage).
81. In civil proceedings, the plaintiff cannot obtain an ex parte search order - these only apply to IP rights. However, if the trade secret violation is subject to a criminal investigation, the police may carry out a search and seizure exercise.

Estonia

82. Estonian legislation provides specific provisions on the protection of trade secrets, most notably in the Competition Act, the Commercial Code, the Employment Contracts Act and the Penal Code. The Competition Act includes an illustrative list of information considered to constitute trade secrets. The Supreme Court has also held that in addition to this definition, the definition of trade secrets provided in the TRIPS Agreement can also be used to interpret the term "trade secrets" under Estonian law.
83. Trade secrets are not generally considered to be intellectual property under Estonian law. However, there is no case law on this point. The legislation implementing the

Enforcement Directive relates only to copyright and industrial property and is not applicable to the protection of trade secrets in Estonia.

84. In order to commence legal proceedings for trade secret misuse, where there is no contract, the elements which must be established are:
 - (a) misuse of trade secrets incurring damage to the plaintiff;
 - (b) the misuse of trade secrets was unjustified; and
 - (c) the culpability of the infringer (through carelessness, gross negligence or intent).
85. If the confidentiality obligation arises from a contract, the plaintiff must show:
 - (a) a valid contractual obligation to maintain the trade secret;
 - (b) the obligation is in force; and
 - (c) breach of the contractual obligation.
86. For non-contractual liability the plaintiff may seek compensatory damages and demand that the damaging behaviour be ceased. For contractual liability, the plaintiff may seek performance of the obligation or withhold performance of the obligation (as appropriate); compensatory damages; termination of the contract; and a penalty (if the parties have agreed on a penalty for breach).
87. Under the Penal Code there is criminal liability for trade secret violation but this is limited to cases where the person misusing the secret becomes aware of the secret in connection with his or her professional or official duties and the unlawful act was committed for commercial purposes or with the aim to cause damage.
88. The Civil Code does not expressly provide for ex parte orders to search premises but such searches may be performed during criminal proceedings by the investigating body.

Finland

89. There are a number of Acts which include provisions for the protection of trade secrets, most importantly the Unfair Business Practices Act, the Employment Contracts Act and the Criminal Code. Unlike its neighbour, Sweden, Finland does not have one piece of legislation directed specifically to the protection of trade secrets.
90. The Criminal Code defines the concept of "business secret". None of the other Finnish Acts contains a definition of business or trade secret. However, a review of the statutes and the (limited) case law makes it clear that trade secrets can be divided into two categories – financial secrets and technical secrets. Both forms are given equal protection by the courts.
91. Although trade secrets are not considered to be typical intellectual property rights, the broad definition of intellectual property rights under Finnish law encompasses their protection under the Unfair Business Practices Act. So, the Enforcement Directive is applicable insofar as the provisions on precautionary measures in the Act on the Safeguarding of the Presentation of Evidence in Disputes concerning Copyright and Industrial Property Rights apply to claims of trade secret infringement under the Unfair Business Practices Act.
92. In order to bring a claim under the Unfair Business Practices Act, the plaintiff must show that the defendant unjustifiably:

- (a) has obtained or attempted to obtain information regarding a business secret or has used or revealed information obtained in an unjustified manner;
 - (b) has used or revealed a business secret he obtained while in the service of the plaintiff in order to benefit himself, another or in order to harm another;
 - (c) has revealed a business secret that he obtained while carrying out a task on behalf of the plaintiff or for other business purposes; or
 - (d) has used or revealed a business secret of the plaintiff, which the defendant has been given by another, knowing that the informant obtained the information unjustifiably.
93. If the owner of the trade secret considers the infringing conduct to amount to an offence under the Criminal Code, the owner may ask the police to initiate an investigation. Attempted industrial espionage and trade secret violation are also criminal offences. Punishment is a fine or up to two years imprisonment.
94. Under the civil law, remedies may be sought under the Unfair Business Practices Act and the Employment Contracts Act. Damages are available and the plaintiff may also seek an injunction under the Unfair Business Practices Act, the Act on the Safeguarding of the Presentation of Evidence in Disputes concerning Copyright and Industrial Property Rights, or the Code of Judicial Procedure. Interim injunctions are also available. If damages are assessed pursuant to the Tort Liability Act, the claimed damages should correspond to the plaintiff's actual loss. The infringer's profits can be taken into account although the plaintiff cannot recover damages in excess of the loss suffered. Damages based on a contractual penalty clause may, however, amount to compensation greater than the loss suffered.
95. The court may seize data that is expected to be relevant under the Act on the Safeguarding of the Presentation of Evidence in Disputes concerning Copyright and Industrial Property Rights. The applicant must show that it is likely that he is the proprietor of a business secret and that his rights are being infringed or infringement is imminent. In addition, the applicant must show that there is a danger that the defendant may hide or destroy the evidence. Ex parte orders are available if the purpose of the precautionary measure would be endangered by the defendant being given notice of the hearing. Such orders securing preservation of evidence are enforced by a bailiff (possibly with the assistance of the police or the applicant (acting as an expert)). More extensive searches of the premises and computer systems, however, are generally only conducted in connection with criminal investigations.

France

96. The only specific trade secrets legislation in French law is that protecting "manufacturing secrets". Other provisions of civil and criminal law protect trade secrets more generally. Three general categories of trade secrets are protected under French law: manufacturing secrets, confidential business information and know-how.
97. Protection for manufacturing secrets is found in the Intellectual Property Code (IPC). Protection under the IPC for manufacturing secrets is limited:
- (a) only manufacturing secrets and not all undisclosed information is protectable;
 - (b) the person committing the act must be an employee or a former employee; and
 - (c) the act complained of must be a disclosure or an attempted disclosure and not a use.

98. Some provisions of the Criminal Code and the Civil Code have been used by the courts to protect other types of information. The Labour Code also provides criminal liability for trade secret violations by employees or former employees. When parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.
99. "Manufacturing secrets" are understood to be intellectual property rights. However, the Enforcement Directive does not apply to their protection under French law.
100. To be liable under the civil (tort) law, three elements must be present: fault (including negligence); damage; and a causal link between the fault and the damage.
101. Compensatory damages (in tort) are available. The evidenced loss of the plaintiff is used as a basis for awarding damages. The infringer's profits are not taken into account. Where there is breach of a contractual obligation, the plaintiff may obtain damages specified in the agreement or in the Civil Code and possibly termination of the contract. An employee who discloses confidential information may also be held to be in violation of his duty of loyalty. The employer may seek damages and termination of the employment contract. Injunctions are also available (both interim and final) in all civil cases.
102. In France, criminal liability for trade secret violation is most often viewed as theft (if documents containing the information are stolen too) and breach of trust. Different penalties apply depending on whether the information is a manufacturing or other secret.
103. Trade secret owners can use the general provisions of the French Code of Civil Procedure to try and secure evidence of trade secret infringement either in ex parte or inter partes proceedings. The Code provides that if there is a legitimate reason to preserve or establish evidence, legally permissible preparatory inquiries may be ordered by the court.

Germany

104. There are a number of provisions in German legislation protecting trade secrets. The most important statutory provisions for the protection of trade secrets are found in the Act against Unfair Competition. These provisions apply to employees and to third parties.
105. Many of the statutes protecting trade secrets under the criminal law also have civil law provisions. These provisions allow for damages and injunctive relief if one of the relevant criminal law provisions is violated.
106. Civil law remedies are also available under the Civil Code (tort law). German contract law also provides effective protection where there is a contractual obligation to maintain the secrecy of trade secrets.
107. During employment, disclosure by an employee of a trade or business secret to a third party is subject to criminal charges. Use of the secret for any purpose unrelated to the employer is also unlawful. After termination of the employment contract the situation is more complex. The general rule is that the former employee is free to use the skill and knowledge gained during employment to further his career. However, any information recorded on paper or otherwise or that the employee deliberately memorised during employment for use after termination cannot be lawfully used.
108. The Act against unfair competition provides against disclosure of trade secrets by employees or third parties for the purposes of competition, personal gain, for the benefit of another or with the intent to cause damage. The Act provides that a particularly serious case usually exists when the perpetrator acts on a commercial basis; knows at the time of

the communication that the secret is to be used abroad; or he effects use abroad without authorisation.

109. Although trade secrets are not regarded in Germany as intellectual property the rules for their protection are to some extent similar to those for the protection of intellectual property rights. However, the Enforcement Directive has not been applied to trade secrets in Germany.
110. In civil proceedings the plaintiff must identify the trade secret precisely in his pleading. This may prove to be difficult, as may proving that unlawful use or misappropriation of the trade secret has taken place. In criminal proceedings it is not necessary to provide full evidence of the unauthorised use. The prosecution authorities must gather all evidence and come to their own conclusion on that basis. The results of the prosecutor's investigations can be used in civil proceedings. For this reason, many cases concerning the misappropriation of trade secrets start with a criminal prosecution.
111. The following civil remedies are available:
 - (a) cease and desist claims (preliminary and permanent injunctions);
 - (b) damages (which may be awarded on the basis of tortious principles or unjust enrichment);
 - (c) delivery up of protected information; and
 - (d) claims to render account (for the purpose of calculating damages).

Greece

112. Greek Unfair Competition Law provides specific provisions on the protection of trade secrets. The Greek Penal Code also provides criminal liability for misuse or disclosure of state, scientific, professional or business secrets. More general protection is found in the Greek Civil Code which includes general tort provisions.
113. Trade secrets are not considered to be intellectual property in Greece and as such the Enforcement Directive is not applicable to the protection of trade secrets.
114. If an employee discloses secrets during the term of his employment, his employer may commence legal proceedings if he can show the existence of a secret which has come to the attention of the employee. There must be a causal link between his employment and his obtaining knowledge of the secret. Secondly, the employer must show disclosure of the secret during the term of the employee's employment to a third party without authorisation. Intention must also be shown - either to compete with the employer or to damage the owner.
115. More generally, the Greek Law of Unfair Competition can also be used to bring proceedings against any person for unauthorised use or disclosure of secrets if the plaintiff can show:
 - (a) the existence of a secret of which the offender has knowledge, either through disclosure by an employee or through his own illegal or unfair act;
 - (b) the unauthorised use or disclosure of the secret to a third party; and
 - (c) intention on behalf of the offender to compete with the owner.
116. The remedies provided under civil law are:

- (a) a cease and desist order (interim injunctions are also available);
 - (b) damages. Under the Greek Civil Code, the plaintiff is entitled to recover his full loss; and
 - (c) unjust enrichment. Under Greek law the plaintiff is entitled to seek the infringer's profits as well as damages.
117. Criminal liability is punishable as a misdemeanour by imprisonment of up to five years and/or a fine.
118. A plaintiff may obtain an ex parte order to search premises for misappropriated data. However, in practice it is difficult to obtain such an order as the plaintiff must prove extreme urgency. A more effective way is for the plaintiff to file a criminal complaint and ask the police to conduct searches for evidence.

Hungary

119. Hungarian law provides specific provisions on the protection of trade secrets. The Civil Code and Unfair Competition Act in particular provide specific protection. The Civil Code defines trade secrets, focusing on information which would, if disclosed, imperil the financial, economic or market interests of the owner. Provisions also exist in the Labour Code and in various financial/banking laws. There is criminal liability under the Penal Code in relation to financial secrets.
120. Trade secrets are not considered to be intellectual property and, as such, the Enforcement Directive is not applicable.
121. As in many other jurisdictions, the trade secret owner faces difficulties in proving infringement and the extent of the damage suffered.
122. Under civil law, the owner can seek:
- (a) a declaration of infringement;
 - (b) a cease and desist order;
 - (c) restoration of the previous state (i.e. any action to put the plaintiff in the position he was in before infringement); and
 - (d) punitive damages in accordance with the liability regulations under civil law (rare in practice). The Court can also further penalise the infringer by ordering him to pay a fine to be used for public purposes.
123. It is possible to search premises and computer systems for misappropriated data under the criminal, administrative and competition law. However, such an investigation is not possible under civil law. If the plaintiff can identify a particular document, the court may call for its production but this procedure is of limited use in practice.

Republic of Ireland

124. There is no specific legislation in Ireland directed to the protection of trade secrets. However, proceedings may be brought under laws relating to breach of confidence, data protection, criminal damage and specific sectorial pieces of legislation.
125. As in England, Irish law has the equitable principle that a person who has received information in confidence cannot take unfair advantage of it. Generally, Irish law imposes a duty of confidentiality in both non-employment cases and employment cases. In both

situations, there must be an obligation of confidence and once it is established that such an obligation exists then the person to whom the information is given has a duty to act in good faith and only use the information for the intended purpose. Again, as in England, an obligation to keep information confidential may either be imposed by contract; implied because of the circumstances of the disclosure or implied because of the special relationship between the parties.

126. Leading commentators in Ireland have stated that trade secrets should not be considered as intellectual property.
127. As in England, three elements are generally required for a successful civil claim in breach of confidence:
 - (a) the information should have the necessary quality of confidence;
 - (b) it should be imparted in confidence; and
 - (c) the person who received the information must have misused it.
128. Civil remedies vary depending on the facts of the case. In general the remedies available are an injunction to restrain further infringement; damages or an account of profits; and delivery up or destruction of the information. Damages and an account of profits are mutually exclusive remedies. There is no criminal liability for trade secret violations in Ireland.
129. Plaintiffs may seek an Anton Piller order giving the right to search premises without prior warning to prevent the destruction of evidence. As in the UK, the party seeking an Anton Piller order has to show that there is an extremely strong prima facie case and very clear evidence that the defendant has in its possession incriminating documents or materials which would be destroyed if the defendant were forewarned.

Italy

130. Specific provisions on the protection of trade secrets are contained in the Italian Code of Industrial Property (IPC). Secret information may only be protected if the requirements set out in the IPC are met. Most business information and technical/industrial expertise is protectable provided the information is secret, has economic value due to its being secret, and has been subject to adequate measures to keep it secret. There are also general tortious obligations and unfair competition provisions in the Civil Code which can be employed to compensate for trade secrets misuse.
131. Trade secrets meeting the requirements set out in the IPC are regarded as intellectual property in Italy. As such, they benefit from the enhanced enforcement measures provided by the law implementing the Enforcement Directive.
132. As regards employees, during employment they will be subject to a general duty of loyalty to their employer under the Civil Code. This includes not disclosing the employer's trade secrets to a competitor. After employment ends, however, the employee is free to use information which has become part of the employee's general skill and knowledge, but he may not use copies of documents or trade secrets in his new job.
133. Since they are considered to be intellectual property rights, trade secrets enjoy all the remedies contemplated under Italian intellectual property law including injunctions, compensatory damages, removal of the infringing products from the market and seizure. Destruction of the infringing goods or assignment of them to the rights holder may also be sought.

134. The Italian Criminal Code contains provisions that may be applied to protect trade secrets. Punishment includes imprisonment (up to three years) and a fine (up to about €1,000).
135. The main difficulty encountered by plaintiffs in civil law trade secret cases is proving misappropriation. However, the Italian courts may presume misappropriation based on the circumstances of the case (such as where customised products are manufactured by the defendant in such a way that only access to the plaintiff's trade secret would allow) and prima facie evidence of infringement.
136. Preliminary search orders under the IPC may be obtained in trade secret cases. Such orders may be granted ex parte to prevent removal or destruction of evidence. The search order allows the applicant to access the defendant's premises together with a bailiff and an expert to collect evidence of the infringement and damages caused.

Latvia

137. Latvia has a number of pieces of legislation which provide specific provisions on the protection of commercial secrets. The Commercial Law is the main Act regulating commercial activities. It defines "commercial secrets" and provides express protection for them. The definition of commercial secret includes economic and technical or scientific information both written and oral which complies with the specific conditions set out in the Commercial Law.
138. The Labour Law also includes provisions regarding use of commercial secrets by employees. Employees have a statutory duty not to disclose any information brought to their attention which is a commercial secret of their employer. Employers must indicate in writing what information is to be regarded as a commercial secret.
139. Latvia also has an Unfair Competition Act which expressly provides that the acquisition, use or disclosure of commercial secrets of another competitor without their consent is a form of unfair competition.
140. Latvia's criminal law imposes criminal liability for illegal acquisition or disclosure of commercial secrets. Punishment includes imprisonment (up to eight years), community service or a fine (up to 150 times the minimum monthly wage). These are amongst the most severe criminal penalties in the EU for trade secret violation.
141. Trade secrets are generally understood in Latvia to be intellectual property and to that extent the Enforcement Directive applies. However, the definition of intellectual property rights in the Civil Procedure Law does not expressly refer to trade secrets and so it is unclear whether the remedies provided in the Civil Procedure Law apply to trade secrets (see below).
142. In order to launch a successful civil action for trade secret misuse, the plaintiff must show that the secret is of an economic, technical or scientific nature, and complies with the following features:
 - (a) the information is contained in the company or is directly related to it;
 - (b) the information is not generally accessible to the public;
 - (c) the information has actual or potential value;
 - (d) the information coming into the hands of another person may cause loss to the company; and

- (e) the company has taken reasonable measures to preserve its secrecy.
143. In this respect, any kind of classification of information and limited access rights within the company will be taken into account.
144. There is no case law regarding whether the remedies (preliminary orders) provided in the Civil Procedure Law apply to trade secrets. If they do apply, provided the conditions of Civil Procedure Law are met, the plaintiff may seek the securing of evidence and the securing of a claim as preliminary measures. Other provisional measures available under the Civil Procedure Law for intellectual property right infringement namely seizure of infringing goods; recall of goods alleged to infringe and an injunction (an order to refrain from performing certain acts) may also be available. However, due to the lack of case law it is not clear whether these remedies are available for trade secret infringement. There is also no case law on the availability of search orders in Latvia although the Civil Procedure Law does provide for the securing of evidence if there is reason to believe that it may be difficult to produce that evidence later in the proceedings.
145. Damages are available under the Civil Law. These are designed to be compensatory. In order to claim damages the plaintiff must prove the particular violation, that the defendant was at fault and the causal link. The amount of loss suffered must also be shown.

Lithuania

146. Lithuanian legislation provides specific provisions on the protection of trade secrets, most importantly in the Civil Code, the Law on Competition, the Labour Code and the Criminal Code.
147. Under the Civil Code, information is considered to be a commercial (industrial) secret if its value results from its secrecy and the owner has made reasonable efforts to preserve its confidentiality. Anyone unlawfully acquiring a commercial secret is liable to compensate the owner for the damage caused. The Code goes on to give examples of the type of damage suffered by the owner of the secret including the costs of its creation, development and use and the income of which the owner has been deprived. Any income received from the unlawful use of the commercial secret is considered to be unjust enrichment and can be included in the damages claim. There are also express provisions in the Labour Code regarding disclosure by employees who disclose a commercial secret in breach of their employment contract.
148. It is unclear from the law in Lithuania whether trade secrets are intellectual property. The Paris Convention is usually invoked in arguments that trade secrets do fall within the scope of intellectual property. However, the Enforcement Directive has not led to enactment of any specific provisions on the protection of trade secrets in Lithuanian law.
149. The usual civil remedy in Lithuania is damages. The plaintiff may also request an injunction against threatened future infringement which is generally not limited in time but can be amended or revoked upon the respondent's application if circumstances change. Delivery up or destruction of the secret information may also be requested.
150. There is criminal liability under Lithuanian law for commercial espionage and for disclosure of a commercial secret causing substantial damage. The maximum punishment is two years imprisonment. More likely is a lesser punishment such a fine and a prohibition against engaging in certain activities or holding office.
151. A plaintiff may request the court to issue an order to secure evidence in civil proceedings. If such an order is granted, the respondent's premises may be searched and the evidence indicated in the court order seized by a bailiff. Usually representatives of the plaintiff and

the respondent are allowed to be present. The respondent may also be ordered to disclose the whereabouts of documents and files containing relevant information. The order to secure evidence may be issued ex parte in urgent circumstances.

Luxembourg

152. There are no specific legal provisions protecting trade secrets in Luxembourg. However, trade secrets can be protected by unfair competition law, criminal law, tort law and contractual law.
153. Use of trade secrets obtained through employees is also subject to criminal liability, punishable by imprisonment of up to three years and a fine of up to €12,500.
154. Trade secrets are not protected as intellectual property in Luxembourg. Thus the Enforcement Directive does not apply to trade secrets in Luxembourg.
155. In order to bring a civil claim for trade secret infringement a plaintiff has to prove the existence of a trade secret and its infringement. Under the current case law, trade secrets are considered to be information known only to a limited circle of people who have an interest in keeping the information secret, the information is related to a commercial or industrial enterprise and disclosure of the information is likely to cause damage to that enterprise.
156. Injunctions and damages are available (but see below). Preliminary injunctions are available for all types of claims provided evidence of infringement is clear.
157. The judge granting the injunction cannot award damages. A claim for damages has to be brought before the District Court and based in tort or contract law.
158. Ex parte measures to search premises are available in criminal proceedings and should in theory also be available under the new Code of Civil Procedure for civil proceedings. However, there is no case law on this point.

Malta

159. There is no specific legislation on the protection of trade secrets in Malta. Trade secrets may be protected contractually, by express or implied terms, and, an employee is presumed to be under an obligation not to disclose confidential information. There are also some criminal sanctions for misuse (see below).
160. Trade secrets are not considered to be intellectual property in Malta and as such the Enforcement Directive does not apply.
161. Protection for trade secrets in Malta is among the most limited in the EU; if no contract exists there will be no civil law right to protect a trade secret. The remedies available are an injunction and damages for breach of contract.
162. The wording of the Criminal Code appears to be wide enough to cover cases of violation of trade secrets. Criminal liability may be found if the violation amounts to the crime of misappropriation or unlawful access to or use of information. Penalties include imprisonment of up to four years and/or a fine (up to €23,293.73). For employees, the penalties are greater (imprisonment of up to ten years and/or a fine of up to €116,468.67).
163. The Criminal Code grants the police powers of entry, search and seizure provided they have a warrant. Having lawfully entered the premises the police also have the right to seize and retain documents and information.

The Netherlands

164. There are no specific provisions on the protection of trade secrets in Dutch legislation. In the Netherlands, the protection of trade secrets is based on the general principle of tort law i.e. an unlawful act. In 1919, the Dutch Supreme Court held that the provision in the Dutch Civil Code on unlawful acts could be used to secure protection against trade secret infringement. Contract law also provides some protection in contractual relationships if there are confidentiality obligations in the contract.
165. There is also a criminal law relating to disclosure of confidential information by people in particular offices or capacities, for example an advocate disclosing confidential client information. The Dutch Penal Code also includes provisions against intentional disclosure by employees of confidential information that may harm their employer. This provision does not extend to use of the confidential information by third parties. Penalties for trade secrets crimes are low in the Netherlands – maximum imprisonment tends to be one year and fines of a few thousand Euros.
166. Additional protection of trade secrets is found in the Dutch Labour Law which permits an employer to terminate a contract of employment where an employee discloses confidential information of the business. Most of the Dutch case law on trade secrets relates to employees and former employees.
167. The Dutch implementation of the Enforcement Directive does not apply to trade secrets. Trade secrets are not considered to be intellectual property in the Netherlands.
168. The protection of trade secrets under Dutch civil law is in general limited to those cases where either the acquisition, use or disclosure of the trade secret constitutes an unlawful act under the Dutch Civil Code. It is deemed unlawful if the secret information is obtained in a manner which is not in accordance with the normal standards of decency, for example, by industrial espionage, theft or the bribery of employees. The simple use of trade secrets by third parties is allowed provided improper methods have not been used to acquire the secrets.
169. Under Dutch law it is possible to obtain a preliminary or permanent injunction restraining disclosure and/or use of trade secrets. The injured party may also claim damages. There are no established guidelines for calculating damages in trade secrets cases so it is considered difficult to assess such damages. The injured party may claim the actual damages it has suffered, taking into account the infringer's profits.
170. Ex parte orders to search premises only apply to the infringement of intellectual property rights and so such orders are probably not available for trade secret infringement. However, ex parte search orders have been obtained where the claim is for misuse of trade secrets and infringement of (other) intellectual property rights.

Poland

171. There are specific provisions on the protection of trade secrets in Polish legislation, notably in the Unfair Competition Act. A number of other Acts mention trade secrets, for example, the Civil Code, the Labour Code, the Act on Competition and Consumer Protection, the Code of Commercial Companies and Partnerships etc.
172. The Labour Code includes express provisions requiring employees to maintain the confidentiality of information the disclosure of which could cause damage to their employer.

173. Generally speaking, trade secrets are not considered to be intellectual property in Poland and the Enforcement Directive is not applicable to the protection of trade secrets.
174. To commence legal proceedings for trade secret infringement under unfair competition law the plaintiff must establish that:
- (a) the plaintiff and the defendant are both enterprises (or in the case of the defendant an employee or someone who worked for the plaintiff);
 - (b) the act complained of constitutes a breach of law or an activity contrary to good practice;
 - (c) the act consists of one of the following:
 - (i) transfer;
 - (ii) disclosure;
 - (iii) use; or
 - (iv) receipt from an unauthorised person;
 - (d) the act concerns a business trade secret;
 - (e) the act threatens or violates the plaintiff's interests; and
 - (f) the defendant has acted in bad faith (for example, if the defendant acquired the trade secret from an unauthorised person for payment).
175. The following civil remedies are available: injunction against continuance of the prohibited acts; removing the effects of the infringement; damages and an account of the infringer's profits (unjustified benefits). The plaintiff can also seek that the defendant makes a public statement relating to the infringement and makes a payment to a Polish cultural or national heritage body. In addition, the court may order destruction of the infringing goods or include them in an account of damages. All the remedies are cumulative save that the plaintiff cannot recover damages and an account of profits exceeding the damage suffered.
176. There is criminal liability for trade secrets violation in Poland which can lead to a fine, limitation of liberty or imprisonment of up to two years.
177. It is possible to obtain a preliminary injunction ex parte which may lead, for example, to seizure of data or goods by a bailiff upon the court's order. The plaintiff's representatives may be present during the seizure.

Portugal

178. The Portuguese Industrial Property Code has specific provisions relating to the protection of trade secrets. The Industrial Property Code is directed towards unlawful acts against competitors. A violation is punished, not as a crime, but as a misdemeanour.
179. The Portuguese Criminal Code also has provisions relating to the disclosure of trade secrets by someone as a result of their employment or position. Unauthorised disclosure or misappropriation of a trade secret under the Criminal Code is a crime punishable by imprisonment of up to one year or a fine of up to 240 days. These penalties can be increased to a maximum of sixteen months imprisonment or 320 days of fine if the unauthorised disclosure was carried out:

- (a) to obtain reward or enrichment to oneself or to another, or to cause damage to another person or to the State; or
 - (b) through the media.
180. The Labour Code also contains provisions which stipulate that an employee may not disclose information, while employed, relating to his employer's organisation, production methods and company business. An employee is not forbidden from using general know-how he has acquired whilst working for other employers but he is prohibited from disclosing a previous employer's trade secrets (both during and after employment).
181. Trade secrets are not considered to be intellectual property in Portugal. However, the Enforcement Directive was implemented by amendment to the Portuguese Industrial Property Code and so some provisions of the Enforcement Directive are applicable to the protection of trade secrets.
182. Under the Industrial Property Code the protection of trade secrets depends on three requirements:
- (a) the confidential or secret nature of the information;
 - (b) the commercial value of the information; and
 - (c) the objective/will of the owner of the trade secret to keep it confidential.
183. The violation of a trade secret is seen to be an illicit act under Portuguese law and so the injured party can file a request for damages based on the civil responsibility for illicit acts (tort law). Simultaneously, the injured party can file a request for damages in the civil court and if a claim is brought under the Criminal Code, the injured party can file a request for damages in criminal proceedings.
184. Under the Industrial Property Code, when a trade secret has a connection with an intellectual property right, the injured party can also request a preliminary injunction to:
- (a) prohibit any imminent infringement;
 - (b) prohibit continuing infringement;
 - (c) provisionally detain suspected goods or information; and
 - (d) provisionally secure assets from the infringing party to safeguard the payment of damages.
- If the trade secret has no connection with an intellectual property right, the injured party can only request a preliminary injunction under the Civil Procedure Code.
185. Final injunctions may also be sought to:
- (a) temporarily restrict the infringing party or any intermediaries from engaging in exercising certain activities or professions;
 - (b) deprive the infringing party or its intermediaries from participating in fairs or markets; and
 - (c) ensure temporary or permanent closure of a commercial establishment.

186. The injured party can also request preliminary injunctions of the same scope under the Civil Procedure Code, if the trade secret is not directly or clearly related to a specific intellectual property right.
187. Searches may be ordered under the criminal law and the court must supervise the search. However, it is not possible to require the defendant to provide information about the whereabouts of documents.

Romania

188. There is specific legislation in Romania on the protection of trade secrets. Provisions regulating protection of trade secrets have been included in the Law for the Prevention of Unfair Competition ("Law on Unfair Competition") and specify that the unfair use of a competitor's trade secrets is regarded as contrary to honest commercial practices. Trade secrets are defined in the legislation as:
 - (a) information that is not generally known by or easily accessible to those in the environment that usually deals with such information;
 - (b) the information is valuable by reason of it being secret; and
 - (c) the holder of the information took reasonable steps to preserve its secrecy.
189. Under the Law of Unfair Competition, the protection of the trade secrets lasts for as long as these requirements are met.
190. Breach of the Law of Unfair Competition can result in civil or criminal liability. The punishment for criminal offences ranges from two years imprisonment to a fine of up to ROL 50 million (RON 5,000).
191. There are also provisions in the Penal Code against disclosure of professional secrets. Punishment ranges from a fine (ranging from RON 2,500 to RON 30,000) to imprisonment of up to seven years. (For civil remedies see below.)
192. Only know-how (product or process information) is considered to be intellectual property under Romanian Law. The Enforcement Directive has been implemented in Romanian law by the Copyright Law. Thus the Enforcement Directive is only relevant to those trade secrets which are also protected by Copyright Law.
193. In order to commence civil proceedings for misuse of trade secrets, the plaintiff must establish:
 - (a) information for which protection is sought is a trade secret, i.e. not generally known or easily accessible to persons in the environment who usually deal with such information, and the information has value by reason of it being secret. The plaintiff must also show that he has taken reasonable measures to keep the information confidential;
 - (b) the disclosure, acquisition or use of a trade secret by a third party; and
 - (c) the party disclosing, acquiring and/or using the information is aware or should have been aware that the information is a trade secret belonging to another.
194. In some cases, in order to successfully prosecute an individual, the prosecutor must also show that:
 - (a) the trade secret has been obtained through industrial espionage;

- (b) the trade secret has been disclosed and/or used by individuals employed by a public authority or by individuals authorised to represent the owner of the trade secret before a public authority; and
- (c) the trade secret has been disclosed by a person that obtained said information as a professional or in the course of his employment.

195. The following civil remedies can be granted:

- (a) an injunction against further use or disclosure of the trade secret;
- (b) destruction or delivery up of any documents containing the trade secret;
- (c) an order requiring the defendant to provide information about the trade secrets disclosed to third parties;
- (d) damages;
- (e) publication of the court decision in a newspaper; and
- (f) an injunction against the defendant using any goods resulting from use of the trade secret in the course of trade or an order to destroy such goods.

196. Under Romanian law, the owner of the trade secret has no right to ask the court for permission to search premises and computer systems for misappropriated data. Such proceedings can only be ordered by the prosecutor in criminal proceedings and must be approved by the judge.

Slovak Republic

197. Protection of trade secrets in the Slovak Republic is regulated by the Commercial Code and the Penal Code.

198. Trade secrets are defined in the Commercial Code which also specifies remedies for trade secret infringement. The relevant fields of protection are civil law, commercial law, intellectual property law, non-contractual liability and unfair competition law. The Penal Code includes penalties for unfair competition offences which include trade secret violations.

199. Trade secrets are generally considered to be intellectual property in the Slovak Republic. The Commercial Code implemented the Enforcement Directive and so the Enforcement Directive is applicable to trade secrets.

200. To bring civil proceedings for trade secret infringement the plaintiff has to show that the information falls within the scope of the definition of a trade secret and that such trade secrets have been disclosed or misused by the defendant. The available remedies are:

- (a) an injunction;
- (b) compensatory damages;
- (c) account of the infringer's profits (in addition to damages for the plaintiff's loss);
- (d) appropriate compensation (by apology and/or monetary compensation); and
- (e) removal of the consequences of the infringement.

201. Under the Penal Code there is criminal liability for trade secrets violations by way of unfair competition acts. Anyone who causes significant damage to a competitor or endangers his business shall be punished by imprisonment of up to three years. For large scale damage, imprisonment can be up to six years.
202. It is possible in the Slovak Republic to obtain ex parte orders in civil and criminal proceedings to search premises and computer systems for misappropriated data and to require the defendant to provide information as to the whereabouts of documents. Such orders are usually executed by the police.

Slovenia

203. Trade secrets are specifically protected in Slovenia by a number of pieces of legislation, in particular, the Companies Act, the Employment Relationship Act, the Protection of Competition Act, the Penal Code and the Code of Obligations.
204. The Companies Act sets out the type of information which is considered to be a trade secret rather subjectively; i.e. a business secret is deemed to be data so determined by the company in a written resolution.
205. The Enforcement Directive has been implemented into Slovenian legislation by the Copyright and Related Rights Act and the Industrial Property Act. Trade secrets enjoy the protection of these two statutes only in particular circumstances. Otherwise, the Enforcement Directive is not applicable.
206. In order to successfully bring a civil action against trade secret misuse the plaintiff must show that the person who used or disclosed the trade secret without his consent knew or ought to have known that the data was a business secret.
207. The remedies available for trade secret infringement depend on the position of the person in breach. If an employee is in breach, his actions constitute breach of his employment contract; for senior employees it may also constitute a breach of contract and for management the sanction may be their dismissal. In addition, the plaintiff may also seek damages accruing from the breach. A preliminary or final injunction may also be available. Usually these will last for as long as they are necessary to serve the purpose for which they were granted. Preliminary injunctions will last only until the final judgment or order. Temporary injunctions may be granted to last until their purpose is fulfilled or they are no longer necessary.
208. Proving that the infringer knew or ought to have known that the information was a business secret can be difficult, as can quantifying damage. In theory the plaintiff can seek loss of its profits and the infringer's profits.
209. No search orders are available without the defendant's consent in civil proceedings but the police may carry out searches in criminal proceedings.

Spain

210. Trade secrets are mainly protected in Spain under the Unfair Competition Act and the Criminal Code. The Act contains provisions specifically aimed at trade secrets. There are also other laws which deal with trade secret protection indirectly, for example, the laws establishing the obligations of directors and other employees.
211. Trade secrets are considered to be intellectual property in Spain at least formally (as stated by legal commentators in the absence of any case law) in light of Article 1.2 of TRIPS which defines intellectual property to include the protection of undisclosed information. However, the relevant provisions of Spanish law do not provide trade secrets

with the same protection granted to traditional IP rights. The Enforcement Directive was implemented in Spain by amendment to the Civil Procedure Act and various intellectual property acts but it did not directly affect the regulation of trade secrets.

212. In order to bring a civil claim for unauthorised use or disclosure of trade secrets, the following elements must be established:
- (a) the information must be secret, have commercial value and have been subject to reasonable steps by the person controlling it to keep it secret;
 - (b) the trade secret must be disclosed, used or appropriated without the owner's authorisation;
 - (c) either the trade secret is disclosed or used by someone who had legitimate access to it who was under an obligation to keep it confidential, or it is disclosed or used as a result of illegitimate access to it such as espionage, breach of contract or similar; and
 - (d) the trade secret violation must be carried out either to obtain an advantage directly or for a third party or to cause damage to the owner.
213. Under the Unfair Competition Act, the plaintiff can seek:
- (a) a declaration that the disclosure, use and/or misappropriation of the trade secret is unfair and therefore illegal;
 - (b) an injunction (including an order to cease the disclosure, use and/or misappropriation and a prohibition against future repetition);
 - (c) removal of all the consequences of the violation of the trade secret;
 - (d) compensation in the form of damages provided that the infringer was negligent or acted in bad faith;
 - (e) compensation for unfair enrichment obtained by the infringer provided that the trade secret violation harmed an exclusive legal position or similar; and
 - (f) publication of the decision.
214. All these remedies are cumulative. The trade secret owner may also seek a preliminary injunction under the general rules of the Civil Procedure Act and can launch pre-trial inspection proceedings to obtain the information necessary to prepare a claim on the merits (see below).
215. There is criminal liability for trade secret violation under the Criminal Code, punishable by imprisonment of up to seven years and fines of up to 24 months. (Fines are calculated in the Spanish criminal system using a "day-fine" ratio determining the economic value of a day on the basis of the circumstances of each offender.)
216. Ex parte orders to search premises are available but these are executed by court officials and experts (such as computer or accounting experts). The plaintiff is not entitled to participate in the inspection. The court will only provide the plaintiff with a copy of the documents that are necessary to file the proceedings on the merits.

Sweden

217. Sweden is the only country in the EU to have an Act specifically protecting trade secrets. The Act provides a definition of trade secrets, penalises trade secret espionage and contains provisions on civil liability.
218. Under the Act, a trade secret comprises three elements:
- (a) it must concern business or operating conditions of a business;
 - (b) it must be confidential; and
 - (c) a disclosure of the information must be detrimental to the competitiveness of the business in question.
219. Information covers information of any nature but it must be specific to the particular business.
220. Anyone who intentionally obtains unauthorised access to a trade secret can also be convicted of trade espionage. Interestingly, the mere transfer of information to a storage device is not considered trade espionage since the concept of "access" to a trade secret under Swedish law requires that the perpetrator obtains actual knowledge of the trade secret. Trade espionage for employees includes access to information that is clearly beyond what is required for the employee to perform his duties provided that the employee suspected the information was confidential. Unauthorised dealing with a trade secret is also a crime under the Act. Such acquisition must be made with intent to unlawfully use or disclose the trade secret. There is no requirement for payment.
221. Liability for damages under the Act varies depending on the type of potential infringer. Liability differs between business partners, employees, former employees and third parties. Anyone committing a criminal offence under the Act may be liable for the damage caused by the act and for any damage resulting from the subsequent unauthorised use or disclosure of the trade secret.
222. Other sections of the Act set out provisions for recovery of damages for breach of confidentiality obligations in a business relationship, breach of confidentiality obligations in employment contracts and damages for subsequent dealings with a trade secret by a third party. How to determine the amount of compensation under these provisions is included to ensure that the provisions on damages are effective. The Swedish legislature noted that in many cases it can be difficult to quantify the damage caused. It is possible to base the assessment of damages on circumstances other than purely economic circumstances. Compensation is set at a level so that unauthorised use of a trade secret is never financially more rewarding than acquiring the trade secret legitimately. The infringer's profits may also be taken into account.
223. Injunctive relief is available under the Act. Interim injunctions can be granted if the plaintiff can show probable cause that a trade secret has been subject to unauthorised use, access or disclosure and it can reasonably be assumed that such act will continue and diminish the trade secret's value. Delivery up or destruction of documents or objects containing the trade secret are further remedies available.
224. As well as the specific legislation for the protection of trade secrets, there are provisions outside the Act which can be used to protect trade secrets such as in the Swedish Penal Code, in particular, breach of faith, breach of professional duty of confidentiality and bribery.

225. Where parties are bound by a contractual obligation not to disclose secret information, an action lies for breach of contract.
226. While an employee is still employed, an employer can prevent him from disclosing its trade secrets under the Act, the principle of the general duty of loyalty of employees, the Employment Protection Act and a contractual confidentiality clause. The Act also provides for damages post-employment where there are "extraordinary reasons". According to the Swedish Courts "extraordinary reasons" would include an employee gathering information during employment with the intention to start a competing business once he has left. Post-termination restrictions can be included in contracts. On the whole, the legislation leans in favour of the ex-employee.
227. Trade secrets are not generally considered to be intellectual property in Sweden although it is acknowledged that there is a close relationship between the protection of trade secrets and intellectual property rights. The Enforcement Directive has not been implemented into Swedish legislation in relation to trade secrets.
228. It is possible to obtain ex parte orders to secure evidence in trade secret claims if giving the defendant an opportunity to respond would place the plaintiff's claim at risk. Measures are available to secure evidence under the Code of Judicial Procedure and under the criminal law. Searches may be carried out as part of a criminal investigation and requests for documentary evidence can be made under the Code of Judicial Procedure.

The United Kingdom

229. There is no legislation providing specific protection for trade secrets. Trade secrets are protected by contract and/or by the law of equity.
230. Technical trade secrets are treated as intellectual property for the purpose of the allocation of cases in the courts. In one case a judge in the Court of Appeal stated that it was "accepted" that technical trade secrets were intellectual property and were therefore covered by the Enforcement Directive²³. There seems to have been limited argument on this point and, therefore, it is open to challenge. However, the UK probably complies with the Enforcement Directive anyway in relation to trade secrets.
231. In order to commence civil proceedings it is necessary for the plaintiff to show that:
- (a) the relevant information has the quality of confidence in the sense of not being generally known and not being of a trivial nature;
 - (b) the information was disclosed to the defendant in circumstances of confidence; and
 - (c) the defendant has used or disclosed the information without permission or has threatened to do so (and possibly that such use or disclosure was or would be to the detriment of the plaintiff).
232. Whilst employed, an individual has a duty of good faith to his employer and will be bound to keep all confidential information secret. After employment ends the court will usually only offer protection to high-grade confidential information ("real trade secrets") and not day-to-day information which forms part of the employee's general skill and knowledge. The factors that the court will take into account in determining whether information should be protected after employment are:

²³ *Vestergaard Frandsen v Bestnet* [2011] EWCA Civ 424.

- (a) the nature of the employment;
 - (b) the nature of the information;
 - (c) whether the employer impressed upon the employee the confidentiality of the information; and
 - (d) whether the information can be easily isolated from other information that the employee is free to use.
233. None of these factors is conclusive. It may be possible to protect lower grade information after employment by imposing a suitable post-employment contractual restriction (known as a restrictive covenant).
234. There are three primary remedies in a claim for trade secret infringement:
- (a) an injunction to prevent further misuse or disclosure;
 - (b) compensatory damages; and
 - (c) an account of profits.
235. The plaintiff usually has to choose either damages or an account of the infringer's profits and cannot receive both. An injunction is usually available in addition to the award of damages/an account of profits. However, the grant of an injunction is discretionary and in some cases the court may decide that an injunction is inappropriate.
236. Information may become public knowledge as a result, for example, of an article being placed on the market. In some cases a competitor is able to get onto the market early by obtaining design information unlawfully. In such a case there would be a claim to damages but the court may also grant what is known as a "springboard" injunction for a period of time to neutralise the illegitimate advantage. Some judges have, however, questioned whether it is ever appropriate to grant an injunction in circumstances where the information has become public. This is still an open question.
237. Innocent infringers may also be enjoined from further use of the information but will not be liable for damages.
238. There is no criminal liability as such for misuse of trade secrets. However, if documents containing the information are physically removed then this may amount to theft. If no physical material is removed then the copying of secret information is not a criminal offence under English law although views have been expressed to the contrary.²⁴
239. It is possible to obtain ex parte court orders permitting the plaintiff's legal representatives to enter the defendant's premises without notice in order to search for materials containing misappropriated trade secrets. This requires strong evidence and the process is supervised by an independent lawyer who reports directly to the Court. It is also possible to obtain an order requiring a person to disclose the whereabouts of such materials.²⁵ The person subject to such an order may be the wrongdoer himself but can also be an innocent individual who has the necessary information.

²⁴ See Bugs, Spies and Paparazzi, Wadlow C., E.I.P.R. 2008.

²⁵ Originally and sometimes still referred to as "Anton Piller Orders". Two examples are set out below. In these cases it is extremely unlikely that any effective action could have been taken without the use of this procedure.

(a) In one case in the UK an ex parte search order was obtained against a manufacturer of competitive spare parts for industrial machinery. The claimant had some information that the defendant was making use of substantial numbers of the claimant's drawings. The search order was executed by the claimant's lawyers and an independent supervising lawyer appointed by the court. The possession of the drawings was denied. In fact the

240. It should be noted that the United Kingdom contains three distinct jurisdictions:
- (a) England and Wales;
 - (b) Scotland; and
 - (c) Northern Ireland.
241. England, Wales and Northern Ireland are common law jurisdictions and the law in Northern Ireland is generally similar to that in England and Wales. Scotland, however, is a mixed jurisdiction where the law has both common law and Roman law origins. Scots law relating to trade secrets is less developed than English law although the judicial view is that the law is similar. However, there is still some doubt as to the extent to which information in the hands of an ex parte innocent recipient may be protected in Scotland. Remedies are similar to England and search orders may be granted by the Scottish courts in an appropriate case.

GENERAL FEATURES OF TRADE SECRETS PROTECTION IN THE EU

242. Although the legal bases differ, the responses received indicate that all Member States provide some protection for trade secrets. It is possible to distil some basic principles.

Information capable of protection

243. Several different types of information have been considered to be capable of protection as a trade secret in cases in Member States. For example:
- (a) customer or supplier lists (the more information the list contains, such as which are the most valuable customers, the more likely it is considered to be a trade secret);
 - (b) technical designs, drawings, blue prints and maps;
 - (c) information about business strategies, methods of doing business etc;
 - (d) costing and price information;
 - (e) R&D information;
 - (f) source code for computer software;
 - (g) manufacturing technology;
 - (h) negative information (such as technical processes that have been discovered not to work);
 - (i) prototypes;

defendant had several thousand drawings hidden in hard copy in the roof space and in an electronic form on a remote server abroad. The links to the server were sabotaged during the search and it was only persistent searching and questioning over several days and the assistance of forensic computer specialists that enabled these to be found. It was discovered that the drawings had been obtained by bribing an employee to access the claimant's computer system. The company's illegal business was then closed down within 2-3 months. This would not have been possible without an ex parte search order.

- (b) In another case the identity of an ex-employee scientist who had been offering documents relating to a new secret process for sale was tracked down using search orders. This individual also denied having any secret documents until these were found in the loft at the individual's home. Without this procedure the identity of the "mole" would not have been discovered leaving other honest employees under suspicion.

- (j) formulae or recipes; and
- (k) genetic material.

Not all States protect all of these.

244. Although several countries include definitions of trade secrets in their legislation, many do not.
245. However, even where no definition exists, a trade secret is often accepted to be (in broad terms) any information, including, but not limited to, technical or non-technical data, patterns, compilations, programs, devices, methods, techniques, financial data, lists of customers or suppliers that:
- (a) is sufficiently secret to have economic value in that such information is not generally known to third parties who could obtain economic value from its use or disclosure; and
 - (b) whose secrecy is achieved due to the owner's reasonable efforts.
246. The confidentiality of the information and in many cases the owner's efforts to keep it secret are generally considered to be the key elements of a trade secret.
247. Where no formal definition of trade secrets exists, the courts often consider a number of factors to determine whether information is a trade secret. Such factors include:
- (a) the extent to which the information is known outside the owner's business;
 - (b) the extent to which the information is known by employees and others involved in the owner's business;
 - (c) the measures taken by the owner to guard the secrecy of the information;
 - (d) the value of the information to the owner and to its competitors;
 - (e) the amount of effort or money contributed by the owner to develop the information; and
 - (f) the ease or difficulty with which the information could be acquired or duplicated by others.

Basis of legal protection

General

248. Only one country (Sweden) has an Act wholly directed to the protection of trade secrets. Some countries have specific legislative provisions protecting trade secrets while others have more general legislation which, while it does not mention trade secrets expressly, can be used to protect trade secrets.
249. Several jurisdictions protect trade secrets using the law of unfair competition and/or through the criminal code. There are also generally provisions in labour laws to prevent employees divulging their employer's trade secrets at least while they are employed. Misappropriation of trade secrets by employees is a common problem throughout Europe.
250. As well as statutory provisions on the protection of trade secrets, confidentiality obligations may also be created contractually or in the absence of an agreement, under

tort law. Appendix 4 sets out a summary of the different bases for protection in each of the 27 Member States. Some examples of the different approaches are given below.

Unfair competition

251. The key provisions of the German trade secrets law are found in the law of unfair competition. The situation is similar in Austria and Poland. Most of the civil law countries have some form of unfair competition law which applies to trade secrets.
252. Other States with unfair competition laws include Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, Hungary, Latvia, Lithuania, Romania, Slovenia and Spain.

Tort law

253. Most notable of the States relying on tort law for protection is The Netherlands. Portugal, Belgium and Greece also rely on tort law.

Criminal law

254. Most States have criminal sanctions against trade secret infringement. Punishment is usually a fine or imprisonment. Some countries recognise the severity of industrial espionage and impose long prison sentences. However, some think there may be a need for even longer sentences to act as a deterrent to serious trade secret misuse. Some countries such as Germany, Cyprus and Greece rely heavily on the criminal law to protect against trade secret misuse.
255. While most countries do have criminal liability for trade secret "theft", maximum terms of imprisonment and fines vary considerably from State to State. Also very few criminal prosecutions appear to be brought which raises questions as to the effectiveness of the law in practice.
256. Unlike most of the civil law States, the common law jurisdictions of England and the Republic of Ireland do not have criminal liability for infringement of trade secrets. In 1997, the English Law Commission issued a report recommending the criminalisation of trade secret "theft" but no steps have as yet been taken to create such a law.

Breach of confidence action

257. In the UK and the Republic of Ireland there is no legislation to protect trade secrets and the breach of confidence action is the principal means of trade secret protection. To prove breach of confidence, the plaintiff must show that the information has the necessary quality of confidence, that it was imparted in circumstances of confidence and there has been (or is threatened) misuse or disclosure of the information. It may also be necessary to prove that the misuse or disclosure has caused (or will cause) damage to the plaintiff. There is no definition of "trade secrets" under English or Irish law but this is not an issue because subject to certain limited specific exclusions, all types of confidential information are capable of being protected and the courts decide on a case by case basis whether or not the information has the necessary quality of confidence.

Contractual claims

258. Most, if not all, States provide for the protection of trade secrets by contractual obligations. However, in Malta, civil protection of trade secrets appears to be solely limited to contractual claims - one of the most limited forms of protection in the EU.

Trade secrets as intellectual property rights?

259. The question as to whether trade secrets are "intellectual property" has no clear answer. The TRIPS Agreement²⁶ treats "undisclosed information"²⁷ as a form of intellectual property. Notwithstanding this, most Member States do not treat trade secrets as intellectual property. Exceptions to this rule can be found in a few Member States such as Italy and to some extent England, Finland, France, Latvia, Romania, Slovenia and the Slovak Republic. For example, the English Courts classify technical trade secrets as intellectual property for the purpose of allocating cases to the Court list. The English Court of Appeal also accepted in one case that trade secrets are a form of intellectual property and thereby subject to the Enforcement Directive.²⁸ Furthermore, in an English case dealing with the rights of co-owners of information in the form of an unpatented invention the rules regulating the ownership of patents were applied by analogy.²⁹

260. One academic commentator comes down firmly with the view that trade secrets are intellectual property:

*"Trade secrets are IP rights. They serve the same purpose as patent and copyright law – they encourage innovation and the disclosure and dissemination of that innovation, though they sometimes serve those purposes in surprising ways"*³⁰

On the other hand, the English, Canadian, US and Australian courts have also expressed views that the right of action to protect trade secrets does not depend on a proprietary right but a duty of good faith.³¹ But the point is still open.

261. As to "property" in a more general European context, Article 1 of the European Convention on Human Rights provides that

"Every natural or legal person is entitled to the peaceful enjoyment of his possessions.."

The English Court of Appeal commented on this as follows:

" The concept of 'possessions' is broad and covers a wide range of things which have significant economic value. It extends to business goodwill and to various forms of intellectual property, including copyright, although there is apparently no case which expressly covers confidential information..."

*Although the parties were unable to cite any Strasbourg authority which expressly covers confidential information as a form of 'possessions, no case was cited against that proposition. I can see no reason, in the light of the Strasbourg jurisprudence which does exist, why valuable commercial information... cannot fall within the concept of 'possessions'."*³²

262. Despite the difference in classification, Member States often provide similar protection to trade secrets as to intellectual property although the means for protection varies considerably from State to State.

²⁶ Agreement on Trade-Related Aspects of Intellectual Property Rights (Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, signed in Marrakesh, Morocco on 15 April 1994.)

²⁷ Information which is secret, of commercial value and which has been the subject of reasonable steps to keep it secret Article 39(2) of TRIPS

²⁸ Rules of Civil Procedure, Part 63 and Practice Direction 63 at paragraph 16.1 (11)

²⁸ *Vestergaard Frandsen SA & Ors v Bestnet Europe & Ors* [2011] EWCA Civ 424

²⁹ *Heyl-Dia v Edmunds* (1899) 81 LT 579

³⁰ *The Surprising Virtues of Treating Trade Secrets as IP Rights* Lemley, 61 Stan. L. Rev. 311 2008 - 2009

³¹ The Canadian case *Cadbury Schweppes v FBI Foods* [2000] FSR 491 contains a useful discussion of common law cases on this point.

³² *Veolia v Nottinghamshire CC* [2010] EWCA Civ 1214

263. Some countries regulate protection of trade secrets by statute in a similar manner to "traditional" intellectual property rights such as patents, trade marks and copyright. One Member State (Sweden) has an Act on the Protection of Trade Secrets. Other Member States (such as Germany) have trade secret provisions in legislation aimed at, for example, unfair competition, labour laws and criminal law. Common law countries, notably the UK and the Republic of Ireland, have no statutory form of protection for trade secrets and use the law of confidence to protect them. In yet further jurisdictions (such as the Netherlands) general tortious liability extends to trade secret infringement. Contractual liability is used to protect trade secrets, in particular in relation to employees, in most Member States. In one Member State (Malta) protection arises solely from the law of contract so there is no means of protection where no contractual relationship exists.

Applicability of the Enforcement Directive

264. As most countries do not consider rights in trade secrets to be intellectual property rights, they have not applied the Enforcement Directive to trade secrets. (This is consistent with the 2005 Statement by the Commission³³ which listed the intellectual property rights which the Commission considered to be covered by the Enforcement Directive. Trade secrets were not included in that list.)

Employees

265. Most jurisdictions provide for contracts of employment to be enforced against employees during the term of their employment. However, the position differs as to what can be done in relation to an ex-employee who uses or discloses secrets after leaving employment. In Italy, as in many Member States, non-compete agreements are used to prevent use or disclosure after the contract of employment ceases, albeit offering more limited restrictions than those which exist during the period of employment. In Sweden, damages for breach of confidentiality obligations after termination of employment are only available where there are "extraordinary reasons".

266. Clearly disaffected ex-employees who have access to very important information, such as research scientists, are in a position to cause serious economic damage. On the other hand, the threat of a breach of confidence action can be used in order to make it unjustifiably difficult for an employee to obtain work in a similar area elsewhere. There is some variation between States as to how a balance between the interests of the employer and the employee is achieved.

267. In Germany, after termination of employment the general rule is that the former employee is free to use the skill and knowledge gained during employment. However, any information that the employee deliberately memorised for (mis)use after termination cannot be lawfully used.

268. In England there is a distinction between general (low grade) confidential information that the employee is not entitled to disclose whilst employed but can use and disclose thereafter and "real trade secrets" which he cannot disclose or use without authority at any time. The distinction depends on a number of factors including whether the employer impressed the secrecy of the relevant information upon the employee; and whether the "secret" can be readily separated from other information which the employee has acquired during his previous employment. The policy in England is similar to that in Germany and many other States in that the employee should, in his new employment, be able to use the ordinary "skill and knowledge" that he has acquired. However, one can

³³ Statement by the Commission concerning Article 2 of Directive 2004/48/EC of the European Parliament and of the Council on the enforcement of intellectual property rights (2005/295/EC.)

see that the way in which this is achieved may produce very different results in some cases.

Remedies

269. Part III of the TRIPS Agreement sets out provisions on enforcement of intellectual property rights and under Article 1, paragraph 2 of TRIPS, "intellectual property" does include protection of undisclosed information. According to TRIPS, injunctions (Article 44), damages (Article 45) and other remedies such as destruction of infringing goods (Article 46) should be available as a minimum.
270. In practice, while injunctions and damages are available in most Member States, the remedies available do vary and appear to depend on the origin of the action. So, for example, in Belgium damages are available but not for claims brought under the Unfair Competition Act. The Belgian Courts have also refused to issue orders prohibiting the use of misappropriated trade secrets because trade secret protection can last forever and the courts are not willing to grant the holder of a trade secret a broader protection than most IP right holders. In Bulgaria it appears that final injunctions are not available with damages being the usual final remedy. In Latvia it is not clear which remedies are available as there is no case law as to whether the remedies provided in the civil procedure law apply to trade secrets.

Search orders

271. Because of the ease with which information can be copied using electronic means a general problem facing plaintiffs in trade secret actions is proving that their trade secrets have been misappropriated and identifying the nature and scale of misuse. If the victim cannot prove the "theft", he cannot institute legal proceedings.
272. One means of obtaining evidence of trade secret misappropriation is a search order. However, such orders are not generally available (see for example, Austria, Belgium, Denmark, the Netherlands, Poland and Romania). In other countries even where the right to apply for a search order exists, there is no case law on its use which suggests it is not seen to be a credible procedure in practice. (See, for example, the Czech Republic and Luxembourg.) In Cyprus, the courts are apparently reluctant to grant search orders.
273. The police or prosecutors have rights in some countries, for example, Denmark, Greece, Estonia, Hungary and Malta, to search premises in criminal proceedings and in many cases this evidence can then be used in civil proceedings.
274. Countries where search orders are available in civil proceedings include Greece, Italy, Finland, the UK and Ireland. However, outside the UK and Ireland the person executing the order is not the plaintiff or its representatives. This may make it difficult to identify the relevant evidential materials.

Customs procedures

275. Where the information is being used abroad it may not be possible to take effective action in the country of origin. Customs seizure³⁴ is possible in the case of trade marks and product patents. There is no reason why this system should not be extended to products manufactured abroad using "stolen" trade secrets. Of course gathering the necessary evidence may be difficult but there seems to be no reason why this procedure should not be available. Border control on the basis of trade secrets misuse is available in the US and appears to have been successfully invoked there.

³⁴ Under Regulation (EC) No 1383/2003.

NUMBERS OF TRADE SECRET ACTIONS

276. In our selected country analysis we considered the number of trade secret cases brought in each jurisdiction over the last five years. Data is not available for some countries, however, where it is, the numbers vary considerably – not only between Member States but from year to year within a particular jurisdiction.
277. Generally it seems that far fewer trade secret actions are heard by the courts than patent actions or other IP right cases. Statistics from the UK's Ministry of Justice indicate that the number of issued trade secret/confidential information claims³⁵ is growing (from three in 2006 to 95 in 2009) but is low compared to other IP cases (50 passing off and trade mark cases in 2006 to 146 in 2009; 57 patents and registered design cases in 2006 to 130 in 2009; and 120 copyright and design right cases in 2006 to 374 in 2009). Note that these statistics are for claims issued; only a handful of these cases will reach trial.
278. Where statistics are available we see relatively few trade secret cases reaching court. There are probably differing reasons for this. Many cases are settled (there are advantages to a plaintiff in avoiding a trial where there is always the danger of some further disclosure of information). In other cases the evidence may be so damning that the defendant has little to gain from a trial.

THE EFFECTIVENESS OF COURT PROCEDURES IN TRADE SECRETS ACTIONS

279. The effectiveness of protection depends not only on the law but also on court procedures. For example, the availability of interim relief, the speed of the proceedings, whether technical trade secrets cases will be heard by specialist judges and the risks the proceedings themselves can present to maintaining the secrecy of the information all have an effect.
280. It is pertinent to note that the TRIPS Agreement contains certain specific requirements in relation to the protection of "undisclosed information". First of all the signatory states are obliged to provide the "possibility" of preventing the disclosure, acquisition or use by others contrary to honest commercial practices. The only requirements in relation to the information is that it should be secret (in the sense of not being generally known), have been the subject of reasonable steps to keep it secret and that it has commercial value because it is secret. "In a manner contrary to honest business commercial practices" includes breach of contract and breach of confidence and inducement to breach; it also includes the acquisition of undisclosed information by third parties who knew, or who were grossly negligent in not knowing that such practices were involved in its acquisition.³⁶
281. TRIPS also requires that fair and equitable civil judicial procedures shall be made available to enforce these rights.³⁷ The remedies to be made available include injunctions and/or damages. There is no provision for the injunctions to be time limited. An important requirement is that, unless this would be contrary to an existing constitutional requirement, there have to be procedures in place to identify and protect confidential information in the course of proceedings. As is noted elsewhere the absence of protection from (further) disclosure of information as a consequence of court proceedings is a considerable deterrent from starting a legal action.³⁸

³⁵ Note these may include privacy cases too.

³⁶ Article 39 TRIPS

³⁷ Article 42 TRIPS

³⁸ As one commentator observes, "*Of course, both a trial and an entire legal proceeding may be conducted publicly and yet the confidentiality of some information may be preserved. It is just a matter of making that information available only to certain persons, like the judge him/herself and the attorneys of the parties (who are bound by the professional duty of confidentiality.) Maintaining confidentiality of information does not mean that all procedures must evolve in camera.*" The TRIPS Regime of Antitrust and Undisclosed Information, Nuno Pires de Carvalho at page 239.

282. As will be seen from commentaries on the laws of individual EU States there are questions as to whether these TRIPS requirements are currently met in every case.
283. In some countries, notably Belgium, there are no effective court procedures to prevent further disclosure of trade secrets in the course of proceedings. So, if a claim is brought, the information risks being disclosed in open court and thus becoming available to the public. Most countries have statutory provisions or procedures under which the public may be excluded from court proceedings if the publicity of the proceedings would endanger a trade secret. This would appear to be best practice.
284. In our selected country analysis we asked for information about the speed of proceedings and whether cases are heard by specialist judges.
285. Specialisations vary. In the UK, technical trade secret cases are heard in the Patents Courts by technically qualified judges. In Germany, while the judges are not technically trained, they are generally experts in unfair competition or IP law. The same is true in Italy where trade secret cases are heard by the specialist IP Courts. In Sweden, Belgium and Bulgaria cases are not heard by specialist judges.
286. Proceedings tend to be of similar length to (other) IP cases. Italy and Bulgaria appear to be the slowest, on average two to three years to obtain a first instance decision on the merits (although a preliminary injunction may be granted within two to three months). Sweden and Belgium tend to take 18 months to two years to reach a first instance decision - similar to the UK (although complex cases may take slightly longer).
287. Germany, usually renowned for its speed in patent cases, takes an average of one to two years from filing a claim to judgment at first instance.

GENERAL OBSERVATIONS AND CONCLUSIONS

288. Trade secrets are important to industry and provide protection for the results of investment of time and money and research and development that are difficult to protect by other means. Their importance in industry seems to be growing.
289. The need for adequate protection has probably become even more important because technology today allows the simple and quick reproduction of documents and their transmission.
290. The law in relation to trade secrets in the EU is a patchwork. In some countries the protection is effective; in others – sometimes because of the difficulty in enforcement - the law provides inadequate protection.³⁹ The law is also fragmented in some States in that different courts are competent to hear different aspects of a trade secrets case.
291. It would be advantageous if there were consistency as to the types of information that can be protected. However, attempting to produce a both detailed and comprehensive definition of "trade secret" is probably unnecessary. TRIPS simply uses the expression "*undisclosed information*" and specifies criteria which must be met for such information to be protectable. Practitioners in most Member States seem to agree that this neutral expression and criteria are a good basis to describe confidential information that deserves protection.
292. The enforcement action should not depend upon there being an existing contractual relationship with the defendant. Many cases of serious industrial espionage involve individuals or companies with whom no such relationship exists.
293. Although generally restrictions imposed by the law during employment are similar from State to State, the position varies to some extent post-employment. This is important because a large proportion of cases involve ex-employees.⁴⁰ This issue is entangled with employment law and public policy and some differences are, perhaps, unsurprising. Member States attempt to reach a balance between the interests of the employer and employee. The balance varies from State to State. In some countries there is no protection post-employment or only in extreme circumstances. This limited, or lack of, protection can cause problems.
294. There are differences in approach to remedies available against "innocent" recipients of trade secrets. In some countries it is possible to prevent third parties making use of the information however innocent they are. In other cases it is necessary to show bad faith on behalf of that party otherwise nothing can be done. Where no injunction is available to prevent further use of the trade secret this may cause considerable damage to the owner.
295. There can be considerable difficulties in obtaining evidence of misuse and damage. If the necessary evidence cannot be obtained the action may never get off the ground. Some courts will not (or cannot) compel defendants to provide the relevant documents or information. To be effective there is a need for:
- (a) procedures to be available to compel defendants to provide information and/or documents; and/or
 - (b) effective search orders to be granted on an ex parte application where there are serious grounds to suspect the defendant is dishonest.

³⁹ There is no clear correlation between the existence of statutory protection and the effectiveness of protection. Common law countries which do not have statutory provisions have good and effective protection in the main, as does Germany which does have specific legislation.

⁴⁰ See *A Statistical Analysis of Trade Secret Litigation in the Federal Court*, Aimeling, D.S., March 2010.

296. Any procedures for search/seizure especially involving complex technical subject matter should be conducted by or with the assistance of representatives of the plaintiff with the relevant technical knowledge and skills.
297. Complex technical trade secret cases may require specialist judges.
298. Including trade secret violations within the scope of the existing Enforcement Directive would assist in improving procedures. At least the same remedies should be available for trade secret infringement as for IP infringement. However, as it stands, Article 7 of the Enforcement Directive does not require States to provide effective search and seizure procedures. This provision might be reviewed.
299. The availability of preliminary and effective final injunctions might be considered.
300. The methods used to calculate damages might also be reviewed to ensure plaintiffs are properly compensated.
301. The courts need to have means to protect secret information during proceedings. This can be achieved with confidential schedules to pleadings and restricting the disclosure of information during trial and in the judgment itself. At the moment there is inconsistency between Member States on the use of "in camera" hearings (hearings excluding the public) and the protection of information contained in court documents.
302. Amending the Customs Regulation to include trade secrets may be of some assistance in controlling the flow of unlawfully manufactured goods, although, in practice, this may not be effective in complex cases.
303. Many countries have criminal remedies. However, although criminal proceedings may be appropriate these are probably not a substitute for effective civil actions.
304. Overall there are disparities across the EU in what can be protected, in what circumstances and what the courts can or will do.

Hogan Lovells International LLP
Atlantic House
50 Holborn Viaduct
London EC1A 2FG

23 September 2011

For any enquiries or further information about this report, please contact the authors:

Robert Anderson
robert.anderson@hoganlovells.com
Tel: + 44 207 296 2511

Sarah Turner
sarah.turner@hoganlovells.com
Tel: +44 207 296 5525

The authors would like to thank those who generously contributed their time and expertise to complete this Study, in particular, the Contributing Legal Practitioners, who are listed in Appendix 1. We also gratefully acknowledge the valuable assistance of the following individuals:

Emma Fulton, Hogan Lovells
Rachael Perkin, Hogan Lovells
Sahira Khwaja, Hogan Lovells
David Latham, Hogan Lovells
Vera McManus, Hogan Lovells
Ian Moss, Hogan Lovells
Chris Heron, Hogan Lovells
Julie Griffin, Hogan Lovells
Hector MacQueen, University of Edinburgh
Katarzyna Czapracka, TSIC.