TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Thuy Phuong Nguyen

TRADE SECRET PROTECTION OF SOFTWARE IN THREE COUNTRIES: FINLAND, THE U.S., AND CHINA

Master's thesis
Programme HAJM08, specialisation: law and technology

Supervisor: Agnes Kasper, PhD

Tallinn 2019

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 19890 words from the introduction to the end of conclusion.

Thuy Phuong Nguyen ……

(signature, date)

Student code: 174638HAJM

Student e-mail address: thuy.phg.nguyen@gmail.com

Supervisor: Agnes Kasper, Ph.D.

The paper conforms to requirements in force

……

(signature, date)

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT....5
INTRODUCTION....6
1. TRADE SECRETS AND SOFTWARE....8
1.1. Definition of trade secrets....8
1.2. Definition of software....9
1.3. Software-related contracts....9
1.4. Trade secret protection of software....10
2. CONTRACTUAL PROTECTION OF SOFTWARE-RELATED TRADE SECRETS IN THE TARGET COUNTRIES....12
2.1. Potential issues of trade secrets in software contracts....12
2.2. Country-specific approaches to trade secret protection in software contracts....12
2.2.1. Finland....12
2.2.1.1. EU law....13
2.2.1.2. Finnish law....14
2.2.1.3. Case law....16
2.2.2. United States....19
2.2.2.1. Legislation....20
2.2.2.2. Case law....23
2.2.3. China....26
2.2.3.1. Legislation....28
2.2.3.2. Case law....31
3. FINDINGS, RECOMMENDATIONS AND CONCLUSION....35
3.1. General findings and recommendations....35
3.1.1. IP audit....35
3.1.2. Security measures....35
3.1.3. Internal policies....36
3.1.4. Confidentiality and non-competition agreements....36
3.1.5. Alternative dispute resolution....37
3.1.6. Legal conflicts and harmonization....37
3.2. Finland and EU....38
3.2.1. Employee confidentiality agreements necessary....40
3.2.2. Confidentiality agreements in business useful but unnecessary....41
3.2.3. Detailed descriptions of protection measure obligations of licensees....41
3.2.4. Include copyright provisions together with trade secrets....42
3.2.5. Avoidance of cloud service....42
3.2.6. Avoidance of too wide rights granted to licensee....42

3.3. U.S. 43
3.3.1. Preemptive confidentiality agreement secrecy obligations 44
3.3.2. Auditing rights 44
3.3.3. Ruling out reverse engineering/decompilation 45
3.3.4. Dispute resolution 45
3.3.5. Confidentiality for visible parts 45
3.3.6. Concurrent use of trade secrets, patents, copyright 46
3.3.7. Associate confidentiality 46
3.3.8. Various contractual approaches 47
3.4. China 47
3.4.1. Protect IP immediately, avoid trade secret introduction to China 51
3.4.2. Preemptive bilingual confidentiality agreement 51
3.4.3. Chinese venue preferable 52
3.4.4. Liability should be wide for licensor 53
3.4.5. Check representative identity, signature, seal authenticity 53
3.4.6. Prohibition on damaging behavior 54
3.4.7. Broad definition of trade secrets 54
3.4.8. Employment confidentiality, non-competition, rights transfer 54
3.4.9. Diffuse production contracts 55
3.4.10. Contract language 55
3.4.11. Combine with other IP and have good policies in place 56
CONCLUSION 57
BIBLIOGRAPHY 60

ABSTRACT

Trade secrets can be extremely important for companies, especially for small businesses. Although software can be protected by copyrights and patents in most jurisdictions, trade secret protection can be vital for the success of many software producers. Also, software patents are usually difficult to obtain and they tend to be narrow while copyright in source code can be engineered around. Because of that, trade secrets can often be the preferred type of intellectual property protection for software companies. However, trade secret law can vary significantly between different countries. In this paper, three different countries, Finland, the US and China, are analyzed for their trade secret protection practice to determine each country's characteristic legal factors of trade secrets protection, which influence the enforceabilty of software-related contracts. The legislation, case law, and academic literature, as well as reports, are analyzed in this paper. Based on the analysis, both general and country-specific recommendations for drafting contracts with solid trade secret protection are given. These recommendations include internal policies and safety measures that any company with software trade secrets should adopt. The contractual recommendations attempt to address the common pitfalls experienced by local and foreign companies that own trade secrets who have been doing business in these countries, especially software companies. This paper desires to give businesses valuable insights for protecting their trade secrets in their various contracts related to software in the studied countries.

Keywords: trade secrets, software, contract, license, business

INTRODUCTION

The world of business property has dramatically shifted. Owning traditional properties such as pieces of land or large quantity of manufacturing equipment perhaps no longer significantly establish market position of a business. Owning intellectual property rights (IPRs), a term first used in 1769[1], has become the core asset of great numbers of businesses and would continue this way in future. The IPRs are nationally and internationally protected and classified under the names of patent, industrial design, trademark, copyright and trade secrets among others. Trade secrets, among all, however, are perhaps the least explored despite its history of appearance back to the year of 1817[2] in law case. The secrecy, the nature and lack of registration of trade secrets mean that this subject is rather hidden and can occasionally be difficult to empirically research, due to the relative lack of material, as majority of trade secrets are, as their name implies, secret. Nevertheless, trade secrets may have the greatest impact to business, out of all types of intellectual property. Most companies do own trade secrets and trade secrets are the main drivers of economic differentiation between businesses.[3] Trade secrets related to production costs, materials, client data, marketing approaches, among others, all help to differentiate different companies in the marketplace and contribute to healthy competition and diverse provision of services and goods offered to customers, among others. For this, trade secrets are crucial for the functioning of world economy and should be given the attention they deserve.

---

1 Griffiths, R., Griffiths, G. E., (1769), Conclusion of the Account of Dr. Smith's New and General System of Physic, from the last Review. *The Monthly Review, Or, Literary Journal*, Vol. 41, pp 278-292, p 290. Accessible : https://babel.hathitrust.org/cgi/pt?id=hvd.hxjfgw , 9 April 2019.

2 *Newbery v James and Others*, Court of Chancery, 27 March 1817, 35 E.R. 1011; (1817) 2 Mer. 446; [1817] 3 WLUK 29. Accessible: https://login.westlaw.co.uk/maf/wluk/app/document?&suppsrguid=i0ad69f8e0000016a01fb4236ca2d391b&docguid=I8977CFF20A2211DEB84D8BA069C5AE76&hitguid=I8977CFF00A2211DEB84D8BA069C5AE76&rank=1&spos=1&epos=1&td=1&crumb-action=append&context=3&resolvein=true , 9 April 2019.

3 (April 2013), Study on Trade Secrets and Confidential Business Information in the Internal Market. Final Study. Prepared for the European Commission. MARKT/2011/128/D, pp 103-105. Accessible: http://ec.europa.eu/DocsRoom/documents/14838/attachments/1/translations , 14 April 2019.; Anderson, R., Turner, S., (Hogan Lovells International LLP), (2011), Report on Trade Secrets for the European Commission: Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D, pp 5-6. Accessible: https://publications.europa.eu/en/publication-detail/-/publication/068c999d-06d2-4c8e-a681-a4ee2eb0e116 , 6 April 2019

However, the level of protection granted to trade secrets are different from country to country, and is, in general, considered weak, particularly in comparison with the protection granted by a patent. There are significant risks associated with reliance on trade secrets. These risks can be especially pronounced in the modern, software-reliant world. Particularly regarding software, it is crucial to discuss trade secret protection of computer programs and associated information, as the increasing impact of software on people's everyday lives, increasing revenues and the relative ease of reproduction can make this field vulnerable to trade secret theft and result in great cost to economy. Trade secret protection will be analyzed in three very different countries which are Finland, an advanced Nordic country with developed society and innovation-oriented approach, United States, one of the most innovative countries with high technological development, and China, an economically powerful countries known for IP infringement but becoming innovation exporter.

All this raises a question of what are the main characteristic legal factors of trade secrets protection in Finland, US, and China, in particular regarding the enforceability of software-related contracts.

To accomplish the aims of the thesis, qualitative methods, comparative method, report review and academic literature review, case-studies review, and interpretation of legislative instruments are used. It is important to put in place qualitative definitions related to software and trade secrets, followed by qualitative analysis on the differences of the trade secret systems, possible danger areas to businesses' trade secret protection arising from legislation and practice, to compare those results and to come up with contractual strategies for businesses with some general approaches coupled with country-specific recommendations designed to ensure enforceable protection of software-related trade secrets.

Chapter 1 of the thesis defines trade secrets and software explores possible types of contracts related to software and discusses the use of trade secrets among other software intellectual property rights. Chapter 2 focuses on each of the three countries, analysing their legislation and case law. Chapter 3 analyzes the approach taken in each country towards trade secret protection as a whole, discovering practical difficulties and recommended strategies arising from law and practice. The thesis concludes by summarizing the main findings and recommendations.

This thesis is dedicated to the author’s parents, siblings and beloved family members. Great thanks to dear friends, Sâm, Xue Mei, Carolina, and Marko for their encouragment and care. Special thanks to the supervisor, Dr. Agnes Kasper, for her guidance, advice, wisdom, and inspiration.

1. TRADE SECRETS AND SOFTWARE

Before diving into in-depth analysis on countries' approaches to trade secrets in software, understanding of the following definitions of trade secrets and software are needed.

1.1. Definition of trade secrets

Trade secrets is a form of intellectual property (IP) that is secret. Several definitions of trade secrets emphasize three main elements for granting the information the status of trade secret. First, the information involved must be secret, usually meaning that it should not be generally known,[4] not to the public, nor in the line of business related to the secret. The second criteria is the secret's economic benefit to its owner. This is usually considered as the negative effect that the company would suffer if they lost the secret to competitors. Mostly, this relates to losing market position, but could also mean the loss of considerable investment in innovation, potentially even driving companies out of business. The third criteria is the application of measures by the trade secret owner for maintaining the secrecy of the information. This is normally understood, although with some jurisdictional differences, as measures related to access and keeping of secrecy by those who are given access to secrets.[5] Those three criteria are normally used for determining whether a trade secret does exist and whether it can be protected. Effort put by the secret owner into development of trade secret is also taken into account in some jurisdictions.[6] Often, trade secrets and confidential information are used as synonyms, however, there can be differences, as confidential information is a wider concept, not requiring secrecy measures, for example.[7] Trade secrets are often shared in

---

4 Tay, L., Lin, J., (2015), Protecting Trade Secrets in Franchising. *Int'l J. Franchising L.*, Vol. 13, Iss. 5, pp 32-40, p 37. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/intjoflw13&collection=journals&id=191&startid=&endid=199 , 9 April 2019.

5 Quinto, D. W., Singer, S. H., (2009), *Trade Secrets : law and practice*. Oxford University Press, Inc., pp 15-23.

6 Carstens, D. W., (1994), Legal Protection of Computer Software: Patents, Copyrights, and Trade Secrets. *J. Contemp. L.*, Vol. 20, Iss. 1, pp 13-76, p 66. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/jcontemlaw20&collection=journals&id=17&startid=&endid=80 , 9 April 2019.

7 Stevens, L. K., (2001), Trade Secrets and Inevitable Disclosure. *Tort & Ins. L.J.*, Vol. 36, Iss. 4, pp 917-948, p 923. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/ttip36&collection=journals&id=931&startid=&endid=96

business dealings with franchisees,[8] during outsourcing manufacture, software development, also during joint ventures. An important feature of trade secrets is that they can be held indefinitely if secrecy is maintained, but they cease to exist if secrecy is lost.[9] The economic burden resulting from trade secret losses can be substantial. The main IP categories lost are R&D information, client lists, financial information, strategic documents.[10]

1.2. Definition of software

Software is another term for electronic programs. It is opposed to hardware, the mechanical component of the programmable device. Software can be understood as a complex of instructions to a machine, coupled with associated data and user interfaces.[11] In modern world, software can be found on any programmable device, mostly on computers, smartphones, and robots. Software can exist in two fundamental forms - source code and object code. Source code is an ordered collection of commands that are written in higher-level programming languages that together instruct the machine (computer or other device) to perform certain tasks.[12] They are designed to be human-readable. Source code must be turned into object code written in binary, the second mode of expression of software that is intelligible to the machine, by a compiler.[13] Other parts connected to software are its user interface, database interface, data formatting, among others.

1.3. Software-related contracts

Several types of contracts can be related to software. Software can be assigned through sale, inheritance, gift, compensation or other means, with the intellectual property rights trasferred through such agreements. Computer programs can be created through development contracts. Use of programs by both businesses and private users often occurs through licensing agreements that allow the use of software but do not transfer any ownership rights. These licenses can be included

---

2 , 9 April 2019.

8 Tay (2015), *supra nota* 4, p 32.

9 Carstens (1994), *supra nota* 6, p 67.

10 Newman, B. K., (2007), Protecting Trade Secrets. *Bus. L. Today*, Vol. 17, Iss. 2, pp 25-28, p 25. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/busiltom17&collection=journals&id=95&startid=&endid=100 , 9 April 2019.

11 Carstens (1994), *supra nota* 6, p 15.

12 Lipton, J. D., (2006), IP's Problem Child: Shifting the Paradigms for Software Protection. Hastings L.J., Vol. 58, Iss. 2, pp 205-250, pp 219-220. Accessible: https://heinonline.org/HOL/P?h=hein.journals/hastlj58&i=237 (5 May 2019)

13 *Ibid.*

in joint venture agreements between businesses. Employment contracts, public procurement contracts, service contracts, competition-related contracts can all be related to software.

1.4. Trade secret protection of software

Software can be protected through various means. In many jurisdictions, software is mainly protected through copyrights as literary works as defined by the Berne Convention.[14] Some jurisdictions allow computer programs to be patented or form a part of a patent application, although it is rare to allow purely computer program-based patents without involvement of other technologies. Mostly, computer programs are combined with other machinery or process in an innovative way to gain patent protection.[15] However, patent registration is significant investment to patentee, including registration fees and maintenance.

Besides the most common ways of protecting computer programs, copyright, and patent, trade secrets are increasingly used. This can have several reasons. Firstly, as mentioned, patenting computer programs is difficult. In addition, patent protection in most jurisdictions is rather limited, usually around 20 years. Copyrights enjoy much longer protection and both source code and object code are normally considered as literary works. However, the issue with copyrights is that they do not protect programming languages, functionality, data formats, and user interfaces – as part of a sofware program. Another problem is that software code can be written in multiple ways, varying commands and their sequences, meaning that it is fairly easy to reverse engineer known source code to achieve equivalent or even improved software with considerably less effort than the original developer.

Trade secrets can often be the most cost-efficient method for protecting the software. Trade secrets in software as well as in knowledge on how different, publicly available software interacts with

[14] Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979), Art. 2. Accessible: https://wipolex.wipo.int/en/text/283698 , 09 April 2019.; WIPO Copyright Treaty (WCT) (adopted in Geneva on December 20, 1996), Art. 4. Accessible: https://wipolex.wipo.int/en/text/295166 , 9 April 2019.

[15] Choudhary, V., (2011), The patentability of software under intellectual property rights: an analysis of US, European and Indian intellectual property rights. *E.I.P.R.*, Vol. 33, Iss. 7, pp 435-446, pp 441-443. Accessible: https://www.westlaw.com/Document/I4CF98F40881111E0B370896DBAF0B922/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 7 May 2019; Ho, K. L., (2015), American Invents - And So Can You: The Dichotomy of Subject-Matter Eligibility Challenges in Post-Grant Proceedings. *Colum. L. Rev.*, Vol. 115, Iss. 6, pp 1521-1562, pp 1527-1530. Accessible: https://heinonline.org/HOL/P?h=hein.journals/clr115&i=1593 7 May 2019.

each other are conceivable.[16] Software trade secrets are becoming increasingly important. Sometimes, software-related trade secrets can be of significant value for companies, such as the algorithm underlying Google's search engine.[17]

Next, ways of protecting software-related trade secrets in contracts will be analyzed.

[16] Quinto (2009), *supra nota* 5, pp 7-8.

[17] Gaido, C., (2017), The Trade Secrets Protection in U.S. and in Europe: A Comparative Study. *Rev. Prop. Inmaterial*, Vol. 24, pp 129-144, p 131. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/revpropin24&collection=journals&id=127&startid=&endid=142 , 9 April 2019.

2. CONTRACTUAL PROTECTION OF SOFTWARE-RELATED TRADE SECRETS IN THE TARGET COUNTRIES

2.1. Potential issues of trade secrets in software-related contracts

There are various contracts that can involve software such as joint venture agreements, consumer license agreements, corporate or volume license agreements, employment, and work-for-hire agreements, to name a few. Software-related contracts could pose several issues to trade secret owners. Some countries have strong labor laws that afford significant protection to workers, limiting the opportunities to put obligations on them. It can also be difficult to deal with subcontractors and ensure they follow proper procedure for handling secrets. Several countries restrict choice of law and choice of venue that parties can choose. There might also be issues with the recognition of foreign arbitral awards. All of those issues must be analyzed to come up with useful contractual approaches for businesses to develop their software-related business in the three countries.

Next, each of the three countries will be analyzed for their trade secret legislation and case law which can relate to software. The analysis starts from Finland, moving to United States, and finishing with China.

2.2. Country-specific approaches to trade secret protection in software-related contracts

2.2.1. Finland

Throughout the last 60-70 years, the Nordic country of Finland has become a thriving welfare state that places emphasis on humanity, sustainability, and smart development. As a country with few profitable resources, Finland has put great emphasis on the development of climate that encourages business and innovation. Innovation has become a key part of Finnish society. For this reason, intellectual property has an important role for Finland.

A specific peculiarity that needs to be taken into account when discussing Finnish intellectual property law and practice is Finnish membership in the EU. This means that not only Finnish law and technology trends in Finland but also European Union law must be considered.

2.2.1.1. EU law

The Trade Secrets Directive provides definition to the term trade secret as valuable due to its secrecy and not widely accessible knowledge in the specific area of expertise belonging to an entity that has taken reasonable secrecy maintenance measures.[18] The Directive emphasizes the varying nature of secret information, from technical to commercial information.[19] The Directive does not apply to EU nor national regulations obliging trade secrets to be disclosed to authorities for public interest reasons, allowing authorities to reveal business information, also does not apply to parties to legal collective agreements.[20] Lawful secret aquisition is defined as through observation, testing, studying, independent creation, disassemblying, through labour union's representative's rights, through other honest business practices.[21] Unlawful use is use without secret owner's permission if access is through unauthorised way, using dishonest business practices, or if copying without approval takes place if revealed or used while breaching confidentiality or general contract terms.[22] These provisions also apply for entities that were or should have been aware of illegality of aquisition of trade secrets.[23] Also, knowingly transporting, storing, trading infringing goods is considered as misappropriation.[24] Art. 5 provides protection for whistleblowers, for public interest, for workers' union representatives and for freedom of speech reasons.[25] The Directive acknowledges the very varying nature of secret information and offers a rather common definition to trade secrets. It offers a flexible way of determining violations of trade secret law by first outlining several infringing actions and then widening the scope by adding dishonest business practices in general. Similar widening is added to allowable discovery, allowing methods for gaining information that is in line with good conduct but unforeseeable as of this point. The Directive also sets criteria for determining remedies for infringement to ensure proportionality.

---

18 Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful aquisition, use and disclosure. *The Official Journal of the European Union*, L 157/1, pp 1-18, Recit. 1, Art. 2. Accessible: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0943&from=EN , 9April 2019.

19 *Ibid.*, Recit. 2.

20 *Ibid.*, Art. 1(2).

21 *Ibid.*, Art. 3.

22 *Ibid.*, Art. 4(2), 4(3).

23 *Ibid.*, Art. 4(4).

24 *Ibid.*, Art. 4(5).

25 *Ibid.*, Art. 5.

Another directive that should be considered is the Computer Program Protection Directive, the main legislation for protecting computer programs in the EU. Computer programs are protected as literary works under this Directive.[26] Expressions of all forms are protected whereas ideas and algorithms are not, only criteria for affording protection is original contribution of the author.[27] If software is created as part of employee's duties, the econimic rights belong to employer, unless the parties have agreed otherwise.[28] Any unauthorized reproduction, distribution or alteration is prohibited, with distribution rights exhaustion towards a copy after copy's first sale.[29] Observation, studying, testing, backup copy making is allowable.[30] There is no violation if reverse engineering is necessary for interoperability reasons.[31] Art. 8 provides greater impact for trade secret protection law.[32] Although computer programs in the EU are mainly protected through copyright, trade secret protection is not ruled out and is sometimes beneficial, either as entire protection or in combination with copyright. The Directive gives good guidelines for software protection that are well adaptable to trade secret law too.

2.2.1.2. Finnish legislation

In 2018, Finland introduced the Trade Secrets Act that set the aim of applying EU Directive on trade secrets. The Act defines trade secrets according to relevant EU law as information which is not readily available or known, that has economic benefit to owner and that is reasonably safeguarded.[33] Sec. 3 identifies illegal aquisition of secret information as occurring through theft, reproduction or other means while also defining allowed mechanisms such as through independent creation, observing, testing of publicly available product or lawfully aquired product that is not accompanied by a prohibition of trade secret aquisition or through employee's tasks or through other means if corresponding to the principles of good conduct.[34] Section 4 forbids the use and disclosure of trade secrets by any person who has gained such secret information unlawfully.[35] Also, those who do have access to trade secrets, are not allowed to use or disclose trade secrets in

---

[26] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. The Official Journal of the European Union, L 111/16, pp 16-22, Art. 1(1). Accessible: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32009L0024&from=EN , 9 April 2019.
[27] *Ibid.*, Art. 1(2), 1(3).
[28] *Ibid.*, Art. 2(3).
[29] *Ibid.*, Art. 4.
[30] *Ibid.*, Art. 5.
[31] *Ibid.*, Art. 6.
[32] *Ibid.*, Art. 8.
[33] Liikesalaisuuslaki (Trade Secret Act) (595/2018), Sec. 2. Accessible: http://finlex.fi/fi/laki/alkup/2018/20180595 , 9 April 2019.
[34] *Ibid.*, Sec. 3.
[35] *Ibid.*, Sec. 4(1).

an unlawful manner, if they are bound by confidentiality agreement.[36] Section 5 of the Act is a whistleblower protection measure, allowing for use and disclosure of trade secrets to authorities for compelling reasons.[37] The disclosure and use of trade secrets is also allowed in the context of trade union activities and for carrying out commercial duties.[38] The Trade Secrets Act seems to incorporate the meaning of EU Directive on trade secrets well. It thoroughly but briefly defines trade secrets, infringement, allowed discovery and importance of good conduct and good faith. For a country such as Finland with long-standing labor union tradition, the provision protecting union representative is highly important.

The disclosure of trade secrets within employment relationship by either side without permission is also prohibited by Section 10 of the Act on the Right in Employee Inventions.[39] Also, Finnish Higher Education Institutions are obliged to confidentiality until the inventions they process have received sufficient IP protection.[40] Maintaining confidentiality of invention information is critical for its ability to get a registered patent. If the critical information related to the invention becomes available before submitting patent application, the patent could be invalidated due to information being publicly known. If this information is disclosed to a competitor, this could be used by the competitor to patent the invention for themselves.

Section 1 of the Finnish Unfair Business Practices Act (UBPA) forbids the use of unfair practices in business environment and derogations from good business practice.[41] Section 4 of the UBPA deals with trade secrets. The first paragraph forbids the attempts at uncovering a trade secret as well as revealing or using inappropriately aquired trade secrets.[42] Paragraph 2 sets rules for employees or service providers for the owner of trade secrets. It forbids them to use the business's trade secrets to benefit themselves or a third person or to harm any party, they are also not allowed to reveal those trade secrets.[43] This obligation lasts for as long as the service provider provides

[36] *Ibid.*, Sec. 4(2).
[37] *Ibid.*, Sec. 5.
[38] *Ibid.*, Sec. 6, 7.
[39] Laki oikeudesta työntekijän tekemiin keksintöihin (Act on the Right in Employee Inventions) (656/1967), Sec. 10, unofficial translation. Accessible: https://www.finlex.fi/fi/laki/ajantasa/1967/19670656 , 9 April 2019.
[40] Laki oikeudesta korkeakouluissa tehtäviin keksintöihin (Act on the Right in Inventions Made at Higher Education Institutions) (19.5.2006/369), Sec. 11. Accessible: http://finlex.fi/fi/laki/ajantasa/2006/20060369 , 9 April 2019.
[41] Laki sopimattomasta menettelystä elinkeinotoiminnassa (Unfair Business Practices Act) (1061/1978), Sec. 1, unofficial translation. Accessible: http://finlex.fi/fi/laki/ajantasa/1978/19781061 , 9 April 2019.
[42] *Ibid.*, Sec. 4, para 1.
[43] *Ibid.*, Sec. 4, para 2.

service for the entrepreneur.[44] Paragraph 3 introduces a more general rule, forbidding anyone from revealing or using trade secrets received from entrepreneur while performing some activity for that entrepreneur, that includes technical documents.[45] Paragraph 4 forbids to reveal or use trade secrets received from someone who has aquired them illegally or revealed them illegally.[46] It can be seen that UBPA protects trade secrets in principle. However, a gap in the law is that the service provider is only required to keep trade secrets for the duration of providing the services. This could potentially expose businesses to significant risks and be detrimental for outsourcing contracts. It must be borne in mind that the law also accentuates that the use or revelation of trade secrets must be unjustified to be forbidden. Therefore, with proper justification, revealing trade secrets could be legal.

Overall, Finnish law and EU law appear to have a proper trade secret scope and rather fair take on the balance of rights. Next, there is need to view the practical application of law in Finnish case law.

2.2.1.3. Case law

In Finland, IP cases are handled by the Market Court (Markkinaoikeus).[47] In the case of trade secrets, District Courts and Market Courts have double jurisdiction.[48] The majority of the decisions of the Market Court appears to handle public procurement, patent (including utility models) and copyright cases. However, there are occasional trade secret cases.

One such case is case nr MAO: 557/18 between Lynx Rifles Oy and Sako Oy.[49] In that case, Lynx developed rifles and its experience in rifle preparation allowed it to develop prototypes for new models of rifles.[50] Two prototypes were loaned to Sako in order to jointly develop new weaponry.[51] According to the applicant, the agreement for joint development never materialized and Sako

---

44 *Ibid.*, Sec. 4, para 2.
45 *Ibid.*, Sec. 4, para 3.
46 *Ibid.*, Sec. 4, para 4.
47 Laki oikeudenkäynnistä markkinaoikeudessa (Market Court Proceedings Act) (100/2013), Sec. 4, 5. Accessible: https://www.finlex.fi/fi/laki/ajantasa/2013/20130100 , 9 April 2019.
48 Finland Ministry of Economic Affairs and Employment, (2018), New Trade Secrets Act enters into force. Press release, 10.08.2018. Accessible: https://valtioneuvosto.fi/en/article/-/asset_publisher/1410877/uusi-liikesalaisuuslaki-voimaan , 9 April 2019.
49 *Lynx Rifles Oy v. Sako Oy*. MAO: 557/18. Issued: 06/11/2018. Accessed through FINLEX: https://www.finlex.fi/fi/oikeus/mao/2018/20180557?search%5Btype%5D=pika&search%5Bpika%5D=MAO%3A%20557%2F18 , 9 April 2019.
50 *Ibid.*
51 *Ibid.*

began to illegally copy and use Lynx's prototypes.[52] It considered that Sako's rifle was almost completely based on Lynx's rifle and Sako's reference to a patent proved irrelevant to the particular case.[53] The Court clarified the conditions for Sec. 4(3) UBPA infringement, noting that any drawings, writings or models, samples are considered as technical elements protected by the provision.[54] The Court also determined that even failed cooperation agreements oblige the receiver to secrecy until the trade secret has maintained economic significance to its holder.[55] The Court found that it is highly important to establish how much effort must the receiver endure to gain same amount of knowledge from different sources other than the trade secret.[56] In the case, the Court saw that due to several constraints caused by the specifics of the development process as well as due to the possibility of gaining knowledge of Lynx's innovative approach through disassembly of its commercial models, Lynx did not own any trade secrets in the rifles.[57] This is important conclusion due to the legality of gaining secret information through studying and disassembling of available product. This can also apply to software, if software architecture is completely or partially provided to licensees or if parts of the source code are provided or obvious.

In another case relating to copyright infringement, the Market Court granted the plaintiff's request to keep certain documents secret for extensive period of time.[58] These documents contained trade secrets relating to monitoring done by the plaintiffs, the methods used for monitoring operations.[59] This is important for software as many monitoring systems used by owners of intellectual property wish to ensure that their IP is not misused. However, the leakage of such methods could cause competitors to develop better methods or customers to develop methods for circumventing such methods.

The latest case in Market Court addressing software trade secrets was launched by MAK-System International Group against Finnish Red Cross Blood Service.[60] In the case, MAK-Systems alleged

---

52 *Ibid.*
53 *Ibid.*
54 *Ibid.*
55 *Ibid.*
56 *Ibid.*
57 *Ibid.*
58 *Crystalis Entertainment UG (haftungsbeschränkt), Scanbox Entertainment A/S ja Scanbox Entertainment Distribution Rights ApS v. A*. MAO: 383/18. Issued: 07/11/2018. Accessible: https://www.finlex.fi/fi/oikeus/mao/2018/20180383?search%5Btype%5D=pika&search%5Bpika%5D=MAO%3A%20383%2F18 , 9 April 2019.
59 *Ibid.*
60 *MAK-System International Group v. Suomen Punainen Risti Veripalvelu*. MAO: 320/18. Issued: 06/13/2018. Accessible: https://www.finlex.fi/fi/oikeus/mao/2018/20180320?search%5Btype%5D=pika&search%5Bpika%5D=MAO%3

that Blood Service had infringed MAK-System's copyright and trade secrets in their analysis software ePROGESA by gaining access to the source code of the software via translating backwards from the object code and then sharing this information with a third party CGI who allegedly used this information to develop competing software.[61] The Court first declared the license agreement between the parties confidential due to the presence of trade secrets within the license agreement.[62] However, the allegations were based on the fact that the competing software was developed rapidly, which was defended by claiming that another ready-made template software that can be easily adapted to their needs.[63] As the plaintiff did not claim that the source code of the software is technical information in the sense of UBPA, the Court could not analyze the issue.[64] The Court, however, agreed that data structure and also data model may be a trade secret.[65] As the License Agreement's Supplement gave Blood Service the right to use ePROGESA in an unlimited and irrevocable way, Blood Service was allowed to study the program.[66] This case is highly important as it makes very clear that confidential information must be clearly defined in contracts and software licensee should not be given unlimited use of software - certain conduct should be prohibited.

In the case of *Carement Oy v. Suomen Kuntotekniikka Oy*, the issue was the use of certain documents by a former employee of Carement.[67] This former employee had been working on a management position in Carement but had decided to quit and found their own company, Suomen Kuntotekniikka Oy.[68] It was found that this former manager had brought its former employee's documents which they had received by email attachments, to the new company.[69] These documents contained trade secrets of Carement Oy.[70] The Court fount that there was an infringment of Art. 4 of UBPA.[71] The case highlights the need to protect the information channels throughwhich secret information is sent. Networks should be monitored, sending confidential material to outside locations should be subject to authorization and information should become

A%20320%2F18 , 9 April 2019.

61 *Ibid.*
62 *Ibid.*
63 *Ibid.*
64 *Ibid.*
65 *Ibid.*
66 *Ibid.*
67 *Carement Oy v. Suomen Kuntotekniikka Oy*. MAO: 416/16. Issued: 07/01/2016. Accessible : https://www.finlex.fi/fi/oikeus/mao/2016/20160416?search%5Btype%5D=pika&search%5Bpika%5D=MAO%3A%20416%2F16 , 9 April 2019.
68 *Ibid.*
69 *Ibid.*
70 *Ibid.*
71 *Ibid.*

inaccessible from outside after a certain period of time.

Another case, this time a Supreme Court case, concerned a non-competition provision in employment contract.[72] In that case, the plaintiff, appealing lower-level case, had been employed in a robotics company where he was dealing with robot programming.[73] The employee was subject to a non-competition agreement lasting for a period of four months to protect the company's trade secrets.[74] The Court found that technical trade secrets were concerned during employment.[75] However, the Court found that such agreements cannot be concluded with mere workers, but with higher-level authorities within a company's hierarchy.[76] Although the employee had access to confidential information in company's information system, it was determined that there was also a valid confidentiality agreement in place, making non-competition agreement unnecessary and not justified.[77] This case illustrates the unnecessary nature of non-competition agreements. It also illustrates the worker protection status in Finland, giving less restrictions to workers and more on the higher management.

Finnish case law demonstrates in general that trade secrets appear rather well protected in Finland. In the case law, trade secret definition and requirements, employment-related issues and reverse engineering are touched upon. The *MAK-System* case demonstrated how important it is not to draft contracts in a way that give excessive rights to software licensees. Overall, Finnish law and case law appear well-adapted to trade secrets and protection levels seem high.

Next, it is time to move to the trade secret law and case law of the United States.

2.2.2. U.S.

Since the World Wars and the Cold War of the 20th century, United States has become the world's forefront technological innovator. However, this development can lead to other countries as well as foreign companies wishing to cash in on the new technology. This can result in unfair practices such as technological counterfeiting as well as theft of trade secrets.

---

72 *K Oy v. R.* KKO:2014:50. Issued: 04/07/2014. Ennakkopäätökset. Accessible: https://korkeinoikeus.fi/fi/index/ennakkopaatokset/precedent/1404377641859.html , 9 April 2019.
73 *Ibid.*
74 *Ibid.*
75 *Ibid.*, para 18.
76 *Ibid.*, para 19.
77 *Ibid.*, para 27-30.

As for software industry, in 1997 already, piracy practices cost the US economy 2.8 billion dollars, along with estimated 130,000 jobs and one billion dollars of tax money lost in the previous year.[78]

Trade secrets are well established in the US as part of intellectual property and something that the companies need to protect and that law needs to guard. One of the most prolific examples of trade secret protection in the US is the measures taken by the Coca-Cola Company to protect their secret recipe. It is only known to two employees who are barred from entering the same aircraft and who must use a variety of security measures to enter into the vault containing the recipe.[79] Legislation and case law of the US must be reviewed to gain an overview of trade secret protection there.

2.2.2.1. Legislation

In the United States, trade secrets had a slower start then other forms of intellectual property, entering into the category in 1939, being mentioned in the Restatement of Torts.[80] Section 757 subjects unauthorized use or disclosure of trade secrets to liability if it arises from knowing misbehaviour.[81] In addition to federal law, trade secrets are also protected by state laws, including District of Columbia.[82] Most states have enacted trade secrets-related provisions in statutes, although a few states mainly regulate the topic through common law.[83] In 1979, the Uniform Trade Secrets Act was adopted and has been adopted by the majority of states.[84] This Act, as amended in 1985, defines many trade secrets-related terms and principles. It defines improper means of aquiring trade secrets as arising from espionage, violation of confidentiality duties, bribery and theft.[85] Trade secret misappropriation is defined as aquiring trade secrets improperly, disclosing

---

78 Choe, A., (1999), Korea's Road toward Respecting Intellectual Property Rights. *Rutgers Computer & Tech. L.J.*, Vol. 25, Iss. 2, pp 341-374, p 343. Accessible: https://heinonline.org/HOL/Page?handle=hein.journals/rutcomt25&collection=journals&id=347&startid=&endid=380 , 9 April 2019.

79 Desai, S., (2018), Shhh! It's A Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive. *Ga. J. Int'l & Comp. L.*, Vol. 46, pp 481-513, p 482. Accessible: https://www.westlaw.com/Document/Iebb14e9464a411e89bf199c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 9 April 2019.

80 American Law Institute, (1939), Restatement (First) of Torts § 757 - Liability for Disclosure or Use of Another's Trade Secret - General Principle. Accessible: https://wipolex.wipo.int/en/text/130065 , 27 February 2019.

81 *Ibid.*; Goodhart, A. L., (1943), Restatement of the Law of Torts, Volume IV: A Comparison Between American and English Law. *U. Penn. L. Rev., American Law Register*, Vol. 91, Iss. 6, pp 487-516, p 488. Accessible: https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9307&context=penn_law_review , 27 February 2019.

82 *Supra nota* 80.

83 *Ibid*.

84 Desai (2018), *supra nota* 79, p 485.

85 National Conference of Commissioners on Uniform State Laws, (1985), Uniform Trade Secrets Act with 1985 Amendments, Model Law 1985 with Prefatory Notes and Comments, Sec. 1, p 5. Accessibe: https://www.wipo.int/edocs/lexdocs/laws/en/us/us034en.pdf , 28 February 2019.

improperly received secrets, violating confidentiality duties or being knowledgeable or presumed to be knowledgeable of improper aquisition or breach of duty.[86] Trade secrets are defined as economically beneficial information that is not generally known nor easily discoverable, while under reasonable efforts to maintain that secrecy.[87] In comments to UTSA, some proper methods for aquiring trade secrets were mentioned, such as reverse engineering, observing in public use as well as display, extracting the secret from publications, gaining access to secret through licensing, independently inventing.[88] Importantly, when in earlier legislation, trade secrets were required to be used, this requirement was deleted as even non-use can be economically useful or might have obstacles for use.[89] The statute of limitations is three years for trade secret misappropriation from learning of misappropriation or reasonable ability to learn.[90] This Act does not concern contractual remedies.[91] The UTSA provides for civilian damages for misappropriation and is applied in state courts (except in New York or Massachussets) and in federal courts in cases that concern multiple states.[92] The validity of trade secrets does not change if it is not used - this provision is of great relevance and rather different from some other jurisdictions where use is necessary to retain protection. This is important for businesses having ideas which technologies, processes, algorithms do not work. Those businesses can use that knowledge as an advantage in market. A disadvantage of US system is that every state can choose whether to adopt federal acts intra-state, however, for international companies, this issue is irrelevant as in interstate and international commerce area, federal acts apply.

However, in 1996, trade secret misappropriation was upgraded to a federal crime by Economic Espionage Act (EEA).[93] The EEA concerns actions that benefit a foreign (non-US) entity.[94] Stealing, gathering through fraud, copying in any way, knowingly buying misappropriated information, including attempts and conspiracies, receive criminal penalties including fines and improsonment terms.[95] The EEA also applies to actions taken in foreign territory if the committing person is citizen or entity or resident of the US or if the actions causing effects were acted within

[86] *Ibid.*, Sec. 1, p 5.
[87] *Ibid.*, Sec. 1, p 6.
[88] *Ibid.*, p 6.
[89] *Ibid.*, p 7.
[90] *Ibid.*, Sec. 6, p 14.
[91] *Ibid.*, Sec. 7, p 14.
[92] Desai (2018), *supra nota* 79, pp 485-486.
[93] *Ibid.*, p 486.
[94] United States Government Publishing Office, (1996), Economic Espionage Act of 1996. 18 U.S.C. 1, Ch. 90, Sec. 1831. Accessible: https://www.govinfo.gov/content/pkg/STATUTE-110/pdf/STATUTE-110-Pg3488.pdf , 28 February 2019.
[95] *Ibid.*, Sec. 1831-1832.

the US.[96] Trade secrets are defined slightly more widely in the EEA than in UTSA. Trade secrets are defined as comprising business, financial, technical, scientific information as well as economic data and engineering specifications in any form and of any type, which may or may not be tangible, which can be stored, as long as the owner of the information has taken steps that are reasonable to ensure the continuing of the secrecy and the secrecy affords the owner potential economic benefit.[97]

In 2016, the EEA was amended by the Public Law 114-153, the amendments became known as the Defend Trade Secrets Act.[98] The Act gives the owner of trade secrets opportunity to seek relief from misappropriation through civil action in court if the secret was connected to product or service in international or interstate setting.[99] This means that in interstate or international scope, the Act protects the owner of secret, but in the state, state's trade secret law is still applicable. The DTSA defines trade secret misappropriation as obtaining the secret by someone knowing that secret was gained dishonestly or should have known that.[100] Also, under the Act, revealing or using secrets without owner's consent that could be given directly by the owner or implied from conduct is illegal if it was gained by stealing, corruption, violation of confidentiality duty, espionage, if the revealer or user knew of such disallowed aquisition, if the revealer or user has confidentiality obligation.[101] Gaining trade secret is legal if discovered independently or reverse engineered, or gained through other allowed ways.[102] Section 7(a)(3) gives immunity to whistleblowers who disclose information to authorities, but only in confidential manner.[103] Defend Trade Secrets Act is the latest federal trade secret law in the US and as such, has relatively little attached case law. It will be seen in the future, how the application of the Act develops. However, trade secrets-related case law is available and will now be reviewed.

96 *Ibid.*, Sec. 1837.
97 *Ibid.*, Sec. 1839.
98 Desai (2018), *supra nota* 79, p 492.
99 US GPO, (2016), Defend Trade Secrets Act of 2016, Public Law 114-153, 114th Congress. Accessible: https://www.congress.gov/114/plaws/publ153/PLAW-114publ153.pdf, 28 February 2019; *Supra nota* 94, § 1831.
100 *Ibid.*, § 2(b)(5)(A).
101 *Ibid.*, § 2(b)(5)(B)-(6)(A).
102 *Ibid.*, § 2(b)(6)(B).
103 *Ibid.*, § 7(a)(3).

2.2.2.2 Case law

US case law is rich in trade secret-related cases. Currently, there are several software-related trade secret cases decided or being discussed in various levels of court proceedings. Here, only some of the decisions are outlined.

The first case to be discussed is *Broker Genius, Inc. v. Zalta*.[104] Broker Genius developed software for ticket brokers and licensed its use.[105] Broker Genius alleged that a set of licensees used their software to create a competing software TickPricer.[106] Broker Genius had contributed significant effort in time and finance to the developemnt of the program.[107] Broker Genius declared fourteen trade secrets in its software, including application architecture, its user interface, functioning rate, and scale enhancement measures, as categories.[108] As a whole, Broker Genius claimed secrecy on both backend solutions as well as for user-visible interface.[109] More specifically, it was alleged that the interface's graphic design, interaction process sequences and generated impressions in the user belong to the interface category.[110] Several of those function-based elements were common to both softwares.[111]

Broker Genius took action to defend their trade secrets through having employees sign up to Employee Handbook that incorporates confidentiality obligation.[112] The company also enters non-disclosure provisions into employment contracts while closing access to secret information right after end of employment relationship.[113] Special IP auditing was also conducted.[114] The company also tried to limit interface revelation to the public, limiting the amount of information disclosed.[115]

---

[104] *Broker Genius, Inc. v. Nathan Zalta et al.*, 280 F.Supp.3d 495, Signed 12/04/2017. Accessible: https://1.next.westlaw.com/Document/Ia968d950d98811e7b393b8b5a0417f3d/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0ad604ac0000016a024c984515f704b1%3FNav%3DCASE%26fragmentIdentifier%3DIa968d950d98811e7b393b8b5a0417f3d%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=c90c47cf1aef57c480d2347d622c3f67&list=CASE&rank=14&sessionScopeId=dd70ccef4a398b87ce360d2108e8be67e8d39baf3f8e9ad11c9bd7c7bfb16c47&originationContext=Search%20Result&transitionType=SearchItem&contextData=%28sc.Search%29, 9 April 2019.
[105] *Ibid.*
[106] *Ibid.*, p 498.
[107] *Ibid.*, p 499.
[108] *Ibid.*, p 500.
[109] *Ibid.*, pp 500-501.
[110] *Ibid.*, p 501.
[111] *Ibid.*, p 501.
[112] *Ibid.*, pp 501-502.
[113] *Ibid.*, p 502.
[114] *Ibid.*, p 502.
[115] *Ibid.*, p 502.

However, the company discloses several trade secrets, including interfaces and scaling solutions, to its clients who receive training too.[116] Through the obligatory acceptance of Terms of Use, the company attempts to rule out source code or algorithm discovery as well as reverse engineering and reproduction of the software in any way.[117] Long-term subscribers sign additional Service Agreement that contains slightly more extensive prohibitions and trade secret protection principles which also include maintaining some obligations after the end of contract.[118] It was determined that TickPricer was inspired greatly by Broker Genius's software.[119]

The Court determined that misappropriation claims could be successful as the information was used through breach of contract.[120] Importantly, the Court noted that for the establishment of copying, access to information and substantial similarity is enough.[121] Next, the Court established what kind of information needs to be established to determine if trade secrets are valid for the plaintiff. Knowledge of the secret outside company, knowledge inside the company, secrecy measures taken, secrecy value for competitors and company, development effort, ease of access are considered important factors.[122] According to earlier case law, the Court concludes that user interface can be a trade secret if its disclosure is accompanied by confidentiality provisions.[123] The Court maintained that even if each widget and its function is commonly known, their specific combination may be secret nevertheless.[124] It was seen that Broker Genius had made efforts to limit access to their interface by refraining from using it in advertisements, applying password-related access with password secrecy requirement for the clients, maintaining confidentiality clauses with employees.[125] However, in Court's view, Broker Genius gave all clients access to its trade secrets without telling them of its confidentiality nor requiring them to maintain secrecy.[126] Interestingly, the Court found that as Broker Genius had applied for a patent, it did not wish to use trade secrets as IPR protection mechanism, essentially the Court saw the two systems as mutually exclusive.[127] It was also established that sales representatives were not restricted in terms of

[116] *Ibid.*, p 502.
[117] *Ibid.*, p 503.
[118] *Ibid.*, p 503.
[119] *Ibid.*, p 504.
[120] *Ibid.*, p 511.
[121] *Ibid.*, p 512.
[122] *Ibid.*, p 513.
[123] *Ibid.*, p 515.
[124] *Ibid.*, p 516.
[125] *Ibid.*, p 517.
[126] *Ibid.*, pp 517-518.
[127] *Ibid.*, p 519.

features during demonstrations.[128] It was noted, however, that the scale of revelation of secret information to users through manuals, training, and helpdesk was so significant that it invalidated company's trade secrets.[129] The Court considered the Terms of Use as insufficient, proposing to use, for the very least, reference to those IP protection provisions in the Terms of Use during access procedure.[130] Moreover, as licenses were given to enterprises as opposed to individuals, each employee did not have access to Terms of Use.[131] The biggest failing by Broker Genius that was seen was the omission of confidentiality clauses from the Terms of Use.[132] The Court conceded the defendants' argument that the standard copyright protection clauses in the Terms of Use are unsuitable for protecting secrecy as such.[133] The Court pointed to similar cases that were solved differently as the license agreements there consisted of provisions banning demonstration, copying, disclosure of any information by any employees or client's agents.[134] Confidentiality part did exist in the Service Agreement but was limited to source code, program architecture, and algorithms.[135] Here, some considerations must be taken into account. If interface or other visible parts of software are accessible by licensees, they need to be accompanied by confidentiality agreements within license to maintain trade secrecy. The terms of service in licensing contracts must be tailored to trade secrets, not just mention copyright. Those aspects were crucial in development of the case and are important to be considered by parties wishing to protect their trade secrets.

Development of competing software resulting from misappropriation of secrets was also the main issue in an unpublished opinion in a 4th Circuit appeal. Decision Insights developed software that allows to develop negotiation strategies, assessing risk and analyzing comparative effects of various approaches.[136] The majority of another company's, Sentia's, founders were connected with

---

[128] *Ibid.*, p 520.
[129] *Ibid.*, p 520.
[130] *Ibid.*, p 521.
[131] *Ibid.*, p 521.
[132] *Ibid.*, p 522.
[133] *Ibid.*, p 522.
[134] *Ibid.*, p 523.
[135] *Ibid.*, p 523.
[136] *Decision Insights, Inc. v. Sentia Group, et al.,* 416 Fed.Appx. 324, Appeal No. 09-2300. U.S. Court of Appeals for the 4th Circuit. Decided Mar. 15, 2011, pp 1-19, pp 3-4. Accessible: https://1.next.westlaw.com/Document/I3500d8cc4f2f11e0b931b80af77abaf1/View/FullText.html?navigationPath=Search%2Fv1%2Fresults%2Fnavigation%2Fi0ad604ac0000016a024ea0a415f70669%3FNav%3DCASE%26fragmentIdentifier%3DI3500d8cc4f2f11e0b931b80af77abaf1%26startIndex%3D1%26contextData%3D%2528sc.Search%2529%26transitionType%3DSearchItem&listSource=Search&listPageSource=68c94d1641bc0b175b8e2837ba77856e&list=CASE&rank=10&sessionScopeId=dd70ccef4a398b87ce360d2108e8be67e8d39baf3f8e9ad11c9bd7c7bfb16c47&originationContext=Smart%20Answer&transitionType=SearchItem&contextData=%28sc.Search%29 , 9 April 2019.

Decision insights previously and two were bound by confidentiality obligations for the time of employment, one employee also had non-complete clause within their contract.[137] After failure of negotiations for licensing Decision Insights' software, Sentia hired another former employee to develop competing program.[138] Previously in case history, the Court of Appeal affirmed Decision Insights' trade secrets in the computer program as an aggregate of information.[139] The Court further reinforces that even public information can be regarded as a trade secret, as long as it is combined by secret methods, that Court views computer programs as compilations.[140] The Court also noted that in any case, contractual breach can be considered as a remedy to protect IPR, as a contract does not have the limitations of a statute.[141] This is an important decision. Firstly, even aggregates of publicly available information can be considered as trade secrets if the aggregate is useful and unknown to public. This is especially so in computer programs. Secondly, the Court agreed that agreements can provide even greater protection to IP than the law, being less limited.

From case law, it seems that trade secret law is very developed in the US, but some common sense considerations must be borne in mind such as defending the secrets with confidentiality obligations.

Next, Chinese law and case law for trade secrets must be explored in relation to software.

2.2.3. China

The People's Republic of China has become the world's second largest economy and a forefront technology innovator. Relatively low cost of production has moved a significant part of industrial production to China, creating the "Made in China" phenomenon.

However, investment and manufacture in China bears risks, especially in terms of IP. Along with Russia, China has been described as having greatest threat to companies due to their capabilities and motivation.[142] Although in principle, trade secrets are protected in Chinese law, China has a

[137] *Ibid.*, pp 4-5.
[138] *Ibid.*, p 5.
[139] *Ibid.*, p 7.
[140] *Ibid.*, p 12.
[141] *Ibid.*, p 18.
[142] Reid, M., (2016), A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat? *U. Miami L. Rev.*, Vol. 70, pp 757-829, pp 783-784. Accessible: https://www.westlaw.com/Document/I2532287f385811e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 13 January 2019; Dreyfuss, R. C., Lobel, O., (2016), Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security. *Lewis &*

tendency of protecting its own enterprises against foreign actors and aquiring foreign trade secrets.[143] This has been a concern for many enterprises and can be seen from major IP infringement proceedings involving foreign large technology companies, where small Chinese companies claim infringement of their IP rights by popular and financially successful products in the West.[144] In order to do business in China, companies often have to give up their IP rights, especially trade secrets.[145] In particular, information technology, high-tech engineering, biotechnology, semiconductors, military technology, and energy solutions appear to be in Chinese focused interests.[146] It has been pointed out that the three main ways how Chinese agents aquire foreign trade secrets are through exploiting cyber weaknesses, recruiting insiders and stealing them from companies acting in the Chinese territory.[147] Cyberespionage, in particular, has been claimed to have direct links to Chinese military.[148] The main issues relating to joint ventures with Chinese companies is policy of China in favoring IP theft and protecting Chinese companies.[149] Chinese companies normally tend to demand some IP sharing for the business deals to be completed.[150] Major Chinese companies are effectively state-owned and the trade secret stealing policies originate from government.[151] A survey done amongst IT experts that aimed to identify IP vulnerabilities showed that China was seen as the biggest threat to IP and several questioneers avoid processing any of their data within PRC.[152] Considering the long-lasting history of Chinese

Clark L. Rev., Vol. 20, pp 419-475, pp 438-441. Accessible: https://www.westlaw.com/Document/I440d85fe54a611e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 22 January 2019; Cunningham Jr, K. E. T., (2017), Fine China? A Look Into Chinese Intellectual Property Infringement, Treaty Obligations, and International Responses. *J. Pat. & Trademark Off. Soc'y*, Vol. 99, pp 279-304, p 281. Accessible: https://www.westlaw.com/Document/I1a72992856eb11e79bef99c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 21 April 2019.

143 Reid (2016), *Supra nota* 142, p 785.

144 Love, B. J., Helmers, C., Eberhardt, M., (2016), Patent Litigation in China: Protecting Rights or the Local Economy? *Vand. J. Ent. & Tech. L.*, Vol. 18, pp 713-741, p 717. Accessible: https://www.westlaw.com/Document/Icd7134c54a7b11e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 25 January 2019.

145 Kahn, R. A., (2017), Economic Espionage in 2017 and Beyond: 10 Shocking Ways They are Stealing Your Intellectual Property and Corporate Mojo. *Bus. L. Today*, Vol. 2017-MAY, pp 1-5, p 4. Accessible: https://www.westlaw.com/Document/I9e3934ff4da911e798dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 22 January 2019.

146 Reid (2016), *supra nota* 142, p 785.

147 *Ibid.*, pp 785-786.

148 Engelman, E. D., (2015), Burdensome Secrets: A Comparative Approach to Improving China's Trade Secrets Protections. *Fordham Intell. Prop. Media & Ent. L.J.*, Vol. 25, pp 589-638, p 593. Accessible: https://www.westlaw.com/Document/I4e9ea0eacd3011e498db8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 15 January 2019.

149 Reid (2016), *supra nota* 142, p 790.

150 Liu, X., (2016), A Long-Overdue Reform: China's Grant-Back Regime in Technology Transfer. *Fordham Intell. Prop. Media & Ent. L.J.*, Vol. 26, pp 741-768, p 749-750. Accessible: https://www.westlaw.com/Document/If4aee5b7174a11e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 15 January 2019.

151 Reid (2016), *supra nota* 142, p 791.

152 *Ibid.*, p 597.

IP violation and its growing impact in the world economy, its rising innovation output and influence around the world, it is beneficial to look at how the law of the People's Republic has evolved and if there are trends in the application of IP law.

2.2.3.1. Legislation

There are two types of most commonly used dealings between foreign and Chinese companies in PRC. Contract manufacturing involves foreign businesses outsourcing their production wholly to China, in this case, they need to share their IP, including trade secrets, with their Chinese business partners.[153] In the case of foreign direct investment model, foreign companies create a joint venture with other Chinese businesses or their own subsidiaries[154] , In that case, the IP rights stay with the foreign company, but they need to be transferred to their local business entity.[155] The People's Republic of China Regulations on Administration of Technology Import and Export stipulates that the licensees own any potential improvements to the licensed technology that they have made.[156] This is an important distinction in comparison with several other states where ownership of improvements made either belong to the licensor by default or is shared between the parties equally or is regulated by licensing contract.

It is stated in the Article 329 of PRC's Uniform Contract Law that technology-related contracts are not valid if they infringe on others' technologies, cause an illegal monopoly to arise or if they obstruct technological development in general.[157] Parties jointly developing trade secret-protected technologies must divide their rights, if no contract exist, parties have equivalent rights, except that the commissioned party must give technology to commissioner first.[158] Scope of use of trade secret may be agreed upon but it cannot damage competition nor technological development.[159] Trade secret transferor must provide transferee with all necessary information, warrant its usability and keep secrecy, while transferee must use secret technology, pay royalties and fees, keep

[153] Liu, (2016), *supra nota* 150, p 743.
[154] *Ibid.*, p 743.
[155] *Ibid.*, p 743.
[156] Regulations on Administration of Import and Export of Technologies (promulgated by the St. Council, Dec. 10, 2001, effective Jan. 1, 2002), art. 27. Accessible: https://www.wipo.int/edocs/lexdocs/laws/en/cn/cn125en.pdf , 15 January 2019
[157] Contract Law of the People's Republic of China (adopted by the National People's Congress on March 15, 1999, and promulgated by the Presidential Order No. 15)(中华人民共和国合同法（于1999年3月15日由全国人民代表大会通过，并以中华人民共和国主席令第15号公布)), Art. 329. Accessible: https://wipolex.wipo.int/en/legislation/details/6597 , 9 April 2019.
[158] *Ibid.*, Art. 341.
[159] *Ibid.*, Art. 343.

secrecy.[160] Transferor must warrant its ownership, usability, and effectiveness, that technology is error-free.[161] Unless parties have excluded this, transferee's use of secret technology based on transfer contract that results in damage to third party, transferor is responsible.[162] An important thing to be remembered here is that the transferor of the technical trade secret must ensure its quality, that the technology actually works and does not have any faults. This means that companies wishing to protect their secrets must make sure that their technology is really effective.

Parties to IP transfer and licensing agreements are free as for the choice of law, otherwise, contract law applies.[163] This can be used to circumvent the effectiveness requirement for the secrecy transfer contracts. For example, CISG could be applied if software is considered as 'goods'. However, one obstacle in applying CISG to software-related contracts could become the reservation of Article 95 of CISG by PRC.[164] The consequence of which is that CISG cannot be applicable in China if one of the contracting parties is based in a country that is not a party to CISG.[165] This can become problematic in terms of some countries such as United Kingdom.[166] Nevertheless, Chinese arbitral decisions have, on several occasions, successfully applied CISG in quality decisions.[167] However, it must be said that CISG has been used significantly in drafting of Chinese Contract Law.[168] The courts have given effect and respected the CISG as the choice of law by the parties.[169] The choice of law appears to apply even if it has no real connection to the contract, as long as both parties expressly agree.[170]

---

160 *Ibid.*, Art. 347-348, 350.
161 *Ibid.*, Art. 349.
162 *Ibid.*, Art. 353.
163 Law of the People's Republic of China on the Laws Applicable to Foreign-Related Civil Relations (中华人民共和国涉外民事关系法律适用法), Art. 49. Accessible: https://wipolex.wipo.int/en/legislation/details/8423 , 09 April 2019.
164 Zhen, P., (2016), China's Withdrawal of Article 96 of the CISG: A Roadmap for the United States and China to Reconsider Withdrawing the Article 95 Reservation. *U. Miami Bus. L. Rev.*, Vol. 25, pp 141-167, p 143. Accessible: https://www.westlaw.com/Document/I42744549bbfb11e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 15 January 2019.
165 *Ibid.*
166 CISG Status as of early 2019. Accessible: http://www.uncitral.org/uncitral/en/uncitral_texts/sale_goods/1980CISG_status_map.html , 9 April 2019.
167 Jingen W., DiMatteo, L. A., (2016), Chinese Reception and Transplantation of Western Contract Law. *Berkeley J. Int'l L.*, Vol. 34, pp 44-99, p 47. Accessible: https://www.westlaw.com/Document/Ic79cb5f59c8811e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 17 January 2019.
168 Liu, Q., Ren, X., (2017), CISG in Chinese Courts: The Issue of Applicability. *Am. J. Comp. L.*, Vol. 65, pp 873-918, p 877. Accessible: https://www.westlaw.com/Document/Ia07f51d3281611e89bf099c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 19 January 2019.
169 *Ibid.*, pp 903-904.
170 *Ibid.*, p 904.

Chinese Copyright Law protects both the software itself and also the documents related to the software as literary work.[171] In the past, the regulatory checks and amendments to technology transfer agreements were used to favor Chinese partners, including, by limiting confidentiality requirements only to the period of validity of the contract.[172] The 2001 Regulations on the Administration of Import and Export of Technologies addressed this issue, amongst others, attempting to get IP policies in line with international agreements.[173] New rules allow the trade secret assignment or licensing to have a perpetual validity period.[174] Also, the confidentiality provisions can continue indefinitely, regardless of the expiration of the term for the main technology transfer contract.[175]

The Foreign Trade Law aims to protect both the intellectual property of foreign traders as well as licensees of this IP through its Chapter V where it mandates that the authorities must enforce IP laws but are unlimited in taking measures against mandatory package licensing, exclusive grant-backs and exclusion of challenge provisions in licensing agreements.[176] Technology import and export agreements, including technical secret access provisions, must be registered.[177]

When trade secrets are misappropriated, it has been noted that there are few remedies against such conduct.[178] For example, the Anti-Unfair Competition Law provides only order to cease illegal conduct and a small fine for trade secret infringement.[179]

---

[171] Miao, F., (2007), Protection of Intellectual Property Rights in Software Products and How to Accomplish a Technology Transfer Transaction in China. *Fordham Intell. Prop. & Media L.J.*, Vol. 18, pp 61-115, p 70. Accessible: https://www.westlaw.com/Document/Ife73ce14a74011dc80f68c7818c06073/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 28 January 2019

[172] *Ibid.*, p 80.

[173] *Ibid.*, pp 81-82.

[174] *Ibid.*, pp 82-83.

[175] *Ibid.*, p 83.

[176] The Foreign Trade Law of the People's Republic of China (中华人民共和国对外贸易法), Art. 29-31. Full text. Accessible: https://wipolex.wipo.int/en/legislation/details/6584 , 9 April 2019.

[177] Decree No. 3 [2009] of the Ministry of Commerce of the People's Republic of China Concerning the Measures of the Administration of Technology Import and Export Contracts Registration (中华人民共和国技术进出口合同登记管理办法), Art. 2. Feb. 1, 2009. Accessible: https://wipolex.wipo.int/en/legislation/details/6588 , 9 April 2019.

[178] Froman, M. B. G., (2014), USTR 2014 Special 301 Report to Congress FINAL, pp 1-63, pp 30-31. Accessible: https://ustr.gov/sites/default/files/USTR%202014%20Special%20301%20Report%20to%20Congress%20FINAL.pdf , 9 April 2019.

[179] Law of the People's Republic of China Against Unfair Competition (as revised at the 30th Meeting of the Standing Committee of the 12th National People's Congress on November 4, 2017)(中华人民共和国反不正当竞争法（2017年11月4日第十二届全国人民代表大会常务委员会第三十次会议修订)), Art. 25. Full text.

The Law for Countering Unfair Competition also aims to protect trade secrets in PRC.[180] The definition of trade secrets appears to be in line with the general international approach.[181] The potential plaintiff must show that trade secret exists and that it was infringed upon.[182] Also, theft, intimidation, bribery, inticement to such acts and violation of confidentiality obligations, also knowing use of infringing information by third party is considered as infringement.[183] The burden of proof is on the plaintiff and the lack of discovery provisions and admissibility concerns of evidence can cause great disturbances.[184] Despite the concerns regarding Chinese IP enforcement policies, it is the country with many IP-related cases.[185] The plaintiff can provide administrative, civil or criminal action against infringer.[186] It appears that the law is increasingly corresponding international understanding of IP. What is difficult in China is the plaintiff's ability to prove infringement as China does not have discovery provisions, leaving evidence collection almost entirely in the shoulders of the secrets owner. However, the increasing experience of authorities with IP can potentially improve the situation.

Followingly, Chinese case law must be studied to reveal the practice of protecting trade secrets in software.

2.2.3.2. Case law

Chinese case law regarding trade secrets is rather rich. However, there are less cases regarding software trade secrets. This paper will take a look at a few software-related cases from the PRC as well as a few non-software-related cases to get a good view of trade secret situation in general.

The first case studied here concerns a retrial application launched by Wu Yinjie and Guo Zhiming and decided in the Supreme People's Court.[187] The plaintiffs were required to develop a new energy

Accessible: https://wipolex.wipo.int/en/legislation/details/18705 , 9 April 2019.

[180] Cheng, Y., (1996), Legal Protection of Trade Secrets in the People's Republic of China. *Pac. Rim L. & Pol'y J.*, Vol. 5, Iss. 2, pp 261-298, p 262. Accessible: https://heinonline.org/HOL/P?h=hein.journals/pacrimlp5&i=269 , 9 April 2019.

[181] *Supra nota* 179, Art. 10.

[182] Bai, J. B., Da, G., (2011), Strategies for Trade Secrets Protection in China. *Nw. J. Tech. & Intell. Prop.*, Vol. 9, Iss. 7, pp 351-376, p 356. Accessible: https://heinonline.org/HOL/P?h=hein.journals/nwteintp9&i=363 , 9 April 2019.

[183] *Supra nota* 179, Art. 10.

[184] Engelman (2015), *supra nota* 148, p 613.

[185] *Ibid.*, pp 605-611.

[186] *Ibid.*, pp 599-605.

[187] *Wu Yunjie, Guo Zhiming v. Chongqing Paiwei Energy Management Co., Ltd.*, (2012), Min Shen Zi No. 855. Civil judgment.(伍韵洁、郭志明与重庆派威能源管理有限责任公司计算机软件开发合同纠纷再审审查民事裁定书，（2012）民申字第855号). Accessible: http://wenshu.court.gov.cn/content/content?DocID=eff454b0-b647-11e3-84e9-

management software, both the B/S and C/S architecture variants, of which the B/S was commissioned and C/S was made for another company by developers previously; the agreement between the developers and Chongqing Paiwei Energy Management Co., Ltd. (Paiwei) obliges the developers to provide complete source codes for any energy management software, adjust the software for databases, convert the architecture of the program from C/S to B/S and upgrade interfaces for database information exchange.[188] The issue in the case was that the C/S version was determined to belong to a third party, Jialida, as a trade secret and the plaintiffs, who were found to be at fault in previous proceedings, argued that Paiwei knew about the ownership and still decided to seek copyright protection to it.[189] The Court determined that the plaintiffs themselves provided the software to Paiwei and there was no proof that Paiwei knew of the infringement, the application for retrial was rejected and the developers bore complete responsibility.[190] In this case, infringement by a company using another's trade secrets was not proven. The case appears rather comprehensive and fair.

Another retrial application submitted to the Supreme People's Court concerned software packets RestAPI and Client SDK that plaintiff Lanling (Beijing) Technology Co., Ltd. (Lanling Company) provided for Beijing Hiujinbao Technology Co., Ltd. (Huijinbao).[191] According to the contract between the parties, Lanling Company was to provide source code of the two software packets to Huijinbao, with IP rights to the software remaining to Lanling Company until full reimbursement has been paid and after payment, those rights would be transferred to Huijinbao.[192] However, Huijinbao was not able to obtain copyright for the source code as it turned out that the software belonged to third party, prompting the Court to determine that the Lanling Company conducted a fundamental breach between the two companies and must bear the responsibility, rejecting the retrial application.[193] Even though in the case, Lanling did not violate trade secrets of the source code's owner as the software was freely accessible, Huijinbao was not able to gain ownership to protect software as its trade secret or copyright, bringing the software partly into trade secret area.

5cf3fc0c2c18&KeyWord=%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86 , 7 April 2019.

188 *Ibid.*

189 *Ibid.*

190 *Ibid.*

191 *Lanling (Beijing) Technology Co., Ltd. v. Beijing Huijinbao Technology Co., Ltd.*, (2017), Supreme People's Court No. 5042. Civil judgment.(蓝凌（北京）科技有限公司、北京汇金宝科技有限公司计算机软件开发合同纠纷再审审查与审判监督民事裁定书，（2017）最高法民申5042号). Accessible: http://wenshu.court.gov.cn/content/content?DocID=6104ee35-3f8a-4c64-8cd6-a8a500bef985&KeyWord=%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%7C%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86 , 7 April 2019.

192 *Ibid.*

193 *Ibid.*

In an appeal case, a former software developer in Tianjin Qisi Technology Co., Ltd. (Qisi) had signed a non-compete agreement with Qisi, obliging not to work for the company's competitors (Baidu specifically mentioned) or their subsidies in any form for a full year since the termination of the work contract, receiving compensation of 50% of former pay.[194] Nevertheless, the developer began working for Baidu's subsidiary during non-competition period and was obliged to pay the reasonable damages as a compensation to Qisi for potential harm to the company's trade secrets.[195] This case is important in terms of employee's liability as it affirms that such liability is valid, that the owner of trade secrets must be compensated even for potential harm and even large compensations are justifiable if not excessive.

Another case concerns non-disclosure agreement between Di Sijie (Beijing) Digital Technology Co., Ltd. (Di Sijie) and its employee.[196] During the employment, employee sold the company's database disaster recovery software via another firm and also provided this software to Beijing Jiuqiao Software Co., Ltd. (Jiuqiao) which applied for copyright protection.[197] The non-disclosure agreement forbode the employee from disclosing Di Sijie's trade secrets and stipulated that all employment-related IP rights belong to the company unless employee declares and it is proven that the IP is not connected to work.[198] Confidentiality obligation was set to last for 5 years after end of employment and con-competition obligation was set to last for 2 years.[199] The case was a continuation for an earlier District-level criminal trade secret infringement case on the same matter, where it was determined that the source code was not known in general, was economically beneficial, properly protected, therefore trade secret, and that the source codes of original program and infringing product were substantially similar.[200] The Court determined that as the IP was

---

194 *Yan Jiping v. Tianjin Qisi Technology Co., Ltd.*, (2016), Beijing Third Intermediate People's Court, No. 934. Civil judgment.(闫继平与天津奇思科技有限公司劳动争议二审民事判决书，（2016）京03民终934号) Accessible: http://wenshu.court.gov.cn/content/content?DocID=63174e86-d852-4cb2-a1b4-1123970ba214&KeyWord=%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%7C%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%7C%E4%BF%9D%E5%AF%86%E4%B9%89%E5%8A%A1 , 7 April 2019.

195 *Ibid.*

196 *Di Sijie (Beijing) Digital Technology Co., Ltd. v. Beijing Jiuqiao Software Co., Ltd. and Chuang Chuhua*, (2012), Beijing Haidian District People's Court, No. 20314. Civil judgment.(迪思杰（北京）数码技术有限公司与成楚华等著作权权属、侵权纠纷一审民事判决书，（2012）海民初字第20314号). Accessible: http://wenshu.court.gov.cn/content/content?DocID=5d457563-0888-4d19-85c9-22b02a84a3c8&KeyWord=%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%7C%E5%95%86%E4%B8%9A%E7%A7%98%E5%AF%86%7C%E4%BE%B5%E6%9D%83%E8%A1%8C%E4%B8%BA , 7 April 2019.

197 *Ibid.*

198 *Ibid.*

199 *Ibid.*

200 *Ibid.*

created as a result of work assignments and defendant employee did not declare otherwise to plaintiff, the IP belongs to Di Sijie.[201] Jiuqiao was determined to having been participant in the trade secret infringement scheme.[202] It was also important to consider that database disaster management as a highly specialized field needs a great deal of investments to achieve competitive breakthrough and Jiuqiao achieved large sales and software product rapidly after its establishment, suggesting movement of research personnel.[203] Here, the infringement verification procedure is important. Similarity of the infringing software source code, dealings between the parties, the specificity of the field were all important aspects. This can give foreign companies significant clarity in measures that can be taken to defend secrets.

Chinese legal IP landscape is changing. The laws and regulations increasingly resemble international approach towards IP. Nevertheless, there are a few peculiar provisions, such as registration of foreign-related trade secret contracts, obligation to ensure effectiveness of secret technology, licensee's right to all improvements and relatively low remedies. Available court cases seem to indicate a rather developed approach towards trade secret litigation, although it must be remembered that the selected case law concerns Chinese parties. Overall, it appears that the legal landscape in China is transitioning.

In next Part, each country's practice regarding trade secrets, contracts and software will be studied and contract-related recommendations will be given.

[201] *Ibid.*
[202] *Ibid.*
[203] *Ibid.*

3. FINDINGS, RECOMMENDATIONS, AND CONCLUSION

3.1. General findings and recommendations

Expanding to another country is a major decision especially for companies dealing with software, and can cause uncertainty and risks. Therefore, in order to mitigate danger to companies' trade secrets, some key issues will be pointed out for consideration for the benefit of companies wishing to protect trade secrets even before entering new markets.

3.1.1. IP audit

Before entry into new markets, establishment of joint ventures or other kinds of cooperation, it is necessary to know if the company has any intellectual property and how protected it is. To do this, IP audit of company's assets should be conducted. Documents possessed by the company should be analyzed with the help of IP counsel to identify potential inventions, copyrightable items and trade secrets, among other IPRs. Licensing agreements should be reviewed for their validity and fairness of their terms, whether company complies with licensors' terms and whether company's licensees appear to comply with their terms. Employment contracts should be reviewed for confidentiality and non-competition clauses.

3.1.2. Security measures

Once IP audit has been conducted and trade secrets are determined to exist for the company, security measures in place that aim to protect those trade secrets must be reviewed. These include the security of physical premises where physical trade secrets or access to trade secrets is located (locking of rooms, video surveillance, login, security services)[204]. These measures also include the use of encryption of documents and communications, protection of computers and internal network access by passwords and accounts, separation of internal and public networks.

[204] Quinto (2009), *supra nota* 5, p 206.

3.1.3. Internal policies

To effectively protect trade secrets, internal policies of company must be well throught through. First and foremost, staff needs to be educated about the nature of trade secrets and measures they need to take to protect them. Employment contracts of people who have access to trade secrets should contain confidentiality provisions and sometimes, non-competition provisions. In some areas, a separate confidentiality agreement should be signed by employee. Confidentiality agreements should be signed preventively by anyone who will gain access to trade secrets such as business partners, licensees, licensors, among others.

Access to confidential information should be limited on a need-to-know basis, all access should be recorded and based on identification and existence of permit. Any outsider needing access should be subject to previous scrutiny and permit from the management. Cybersecurity measures such as firewalls and antivirus and anti-spyware should be kept up to date. Network policies should aim to limit downloads from third party websites and recording of any activities related to confidential files. With strong internal policies, it is much easier to protect trade secrets than with weak policies.

3.1.4. Confidentiality and non-competition agreements

All persons and companies having access to secret information must previously sign confidentiality agreements. Access to information must be subject to such agreement, even in the negotiation stage. In confidentiality agreements, it is advisable to construct the kinds of confidential information as widely as possible, to avoid giving away confidential information through the specific description of this information, while excluding certain kinds of data such as previously known, public, legally disclosed, among others.[205]

Non-competition agreements with employees with access to trade secrets should also be considered. They must normally be limited in time. In general, these agreements need remuneration.

[205] Kelly, E. A., (1999), Effective Contracting in Software Licensing. *U.N.B.L.J.*, Vol. 48, pp 275-282, pp 280-281. Accessible: https://heinonline.org/HOL/P?h=hein.journals/unblj48&i=279 , 9 April 2019.

3.1.5. Alternative dispute resolution

Alternative dispute resolution (ADR) is increasingly accepted throughout the world. Especially in business, ADR is preferable to litigation, especially when trade secrets are involved. Some countries, especially those in Asia, favor negotiations and conciliation to litigation, having mistrust towards judicature. However, some larger and more powerful states such as the US and China have occasionally been reluctant to recognize the choice of different law and venue than their own.

3.1.6. Legal conflicts and harmonization

Legal regimes studied in this paper have their similarities and differences. All three have similar definition of trade secrets. However, there can be considerable differences in treatment of trade secrets and related contracts. For example, work-related regulations have significant differences across jurisdictions, with some providing temporary, statutory obligation of secrecy upon workers (Finland) while others require confidentiality agreements for the legal obligation of secrecy to arise. In the United States, non-competition provisions can be easily enforced against workers (except in California[206]) but it is more difficult in China and in EU. In Finland, businesses are obliged to secrecy by law whereas, in China, such agreements are strictly necessary to establish misappropriation.

Further, there is considerable difference in ways of protecting trade secrets in these different countries, arising from the characteristics of their legal systems. In the United States, most limitations of legislation can be contracted around, partially owing to the economic freedom embedded in the legal culture. In China, however, transactions tend to be tightly controlled, despite privatization, to ensure state's objectives are fulfilled. In Finland, market is free but kept in check by different regulations directed at consumers, environment, and workers, all of which can have an impact on IPRs.

Despite international agreements regarding IPRs, there are significant differences between those three jurisdictions regarding the protection of trade secrets. In that regard, one might wonder if those systems need to be harmonized.

[206] Quinto (2009), *supra nota* 5, pp 205, 243-244.

In order to harmonize regulations in a certain field, certain conditions have to be met. First, there needs to be certain unsurmountable difficulty in the field, bringing motivation for change. Arguably in IPRs, China's record of infringement[207] would prove such a need. However, it must be kept in mind that China has adopted Western notion of IPRs to a great extent into its legislation and the issues seem to be rather related to enforcement, lack of discovery procedures, administrative difficulties and legal standards related to contract, technology, representation, business, investment.

In that regard, as the difficulties in Chinese law do not arise significantly from IPRs legislation itself, harmonization would become difficult. Not to mention that the legal culture in China is rather different from the West. Moreover, although certain risks do exist and it is rather difficult to adequately protect trade secrets in China, it is nevertheless possible to obtain adequate protection there through wise implementation of internal policies and through contractual means. As it is possible to protect trade secrets through contractual means, legal harmonization proves unnecessary.

Likewise, the minor differences between trade secret protection between EU (Finland) and US do not warrant harmonization. Most difficulties can be overcome in both regimes through contracts.

Overall, contracts appear to be a better method of protecting trade secrets in each of the discussed regimes. Although laws can vary considerably, there are usually applicable non-IPR provisions that can be used for protection. These provisions can work on their own, without their inclusion into contracts, or they can arise from allowable limitations that contracts can pose. As a result, there is no significant need to harmonize the legal systems of Finland, US, and China.

Next, specific country-based approaches will be offered.

3.2. Finland and EU

Finland can be regarded as a country with rather strong protection of IP, including trade secrets. However, EU member states (MSs) had no common definition of trade secrets, nor was there any

[207] Reid (2016), *supra nota* 142, pp 783-793.

EU-level standardization[208] before 2016. Trade secrets in earlier times were considered less deserving of protection than other IPs.[209] Litigation of trade secrets appears to be outnumbered by patent and trademark cases, whereas in the UK, for example, the difference was not great.[210] It has also been noted that European Commission had put emphasis on competition as opposed to trade secret guardship.[211] It has been noted that the different terms used in some MSs can become confusing and that some EU states do not protect trade secrets at all.[212] Some common features among trade secret protecting MSs are the requirement of reasonable secrecy efforts and economic benefit of the fact of secrecy.[213] Many countries do provide criminal and contractual remedies for misappropriation.[214] The study by Commission found that companies see trade secrets as vital for innovation and furthering competition, but that messy legal system discouraged companies from sharing trade secrets and from litigating.[215] This inactivity occurred despite one fifth of companies having suffered from at least attempted trade secret misappropriation.[216] In order to harmonize the field, EU adopted the Trade Secrets Directive in 2016.[217]

The Directive has been criticized, however, based on difficulties encountered in the US with its own trade secret law, about lack of discussion of employee-created trade secrets and different agreements covering trade secret protection (non-competition, non-disclosure, assignment).[218] Some used definitions, possibility or lack thereof of criminal sanctions, unclarity about employee movement and scope of application of trade secrets.[219] An especially distinctive concern has been differentiating a highly experienced worker's knowledge from trade secrets of a company.[220] Some issues raised concern the generality of the Directive.[221] Another raised concern is if agreements

---

[208] Czapracka, K. A., (2008), Antitrust and Trade Secrets: The U.S. and the EU Approach. *Santa Clara Computer & High Tech. L.J.*, Vol. 24, pp 207-272, p 230. Accessible: https://www.westlaw.com/Document/I6992fe18d0d311dc817c8c7818c06073/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 09 April 2019.
[209] *Ibid.*, p 209.
[210] Anderson (2011), *supra nota* 3.
[211] Czapracka (2008), *supra nota* 208, p 209.
[212] Desai (2018), *supra nota* 79, p 487.
[213] *Ibid.*, p 488.
[214] *Ibid.*, p 489.
[215] *Supra nota* 3, p 135.
[216] *Ibid.*, p 142.
[217] Trade Secrets Directive, *supra nota* 18, Recit. 10.
[218] Sandeen, S. K., (2017), Implementing the EU Trade Secret Directive: a view from the United States. *E.I.P.R.*, Vol. 39, Iss. 1, pp 4-11, p 5. Accessible: https://www.westlaw.com/Document/I4A84AF30B58B11E6B256F4FE4F80B413/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 10 April 2019.
[219] *Ibid*.
[220] *Ibid*.
[221] *Ibid*.

can prevent independent discovery.[222] It can be especially relevant in the case of software as in the EU, reverse engineering is allowed for some purposes. Considering the EU and Finnish law and their general principles together, however, it appears that contractual limitations to discovery-directed activities could be feasible. An important problem is seen in regards producing and marketing goods that result from misappropriation, with concerns related to collateral third party liability.[223]

In terms of applicable law to trade secret misappropriation in the EU in non-contractual obligations, it has been found that Art. 4(1) of Rome II Regulation applies, making law of country of damage occurrence predominant.[224] This occurs unless both the one at fault and sufferor reside in same state or the case is closely connected to one specific state.[225] Fortunately, the selection of forum and applicable law in tort cases is fairly well regulated in the EU.

Overall, Finland appears to be enjoying a quite strong protection of trade secrets, although increasing use of cloud technology can put some secrets in risk. The adoption and implementation of Trade Secrets Directive in EU level is an encouraging sign towards harmonization and clarity of trade secret status in the rest of the Union. Finland has made a strong progress and lies at the forefront of European trade secret protection.

As Finland is a Member State of the European Union, one needs to take into account both Finnish and EU law when making contracts for protecting software trade secrets in Finland. Next, recommendations for protecting trade secrets in Finland are given.

3.2.1. Employee confidentiality agreements necessary

Trade secrets are rather well protected in Finnish and European law. Normally, gaining access to trade secrets unlawfully is considered misappropriation. However, care must be taken when giving lawful access to trade secrets to anyone. This is because the confidentiality obligations to those who possess knowledge of the secret only apply if there is a confidentiality agreement between the secret's owner and the accessor. Although Finnish law does contain provision prohibiting

[222] *Ibid.*, p 6.
[223] *Ibid.*, p 6.
[224] Wadlow, C., (2008), Trade secrets and the Rome II Regulation on the law applicable to non-contractual obligations. *E.I.P.R.*, Vol. 30, Iss. 8, pp 309-319, p 312. Accessible: https://www.westlaw.com/Document/I2764D490468F11DDA218AF32497F9DAB/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 10 April 2019.
[225] *Ibid.*, pp 312-313.

disclosure of trade secrets after employment termination, it only lasts for two years and information needing protection as secret for longer needs to be covered for an extended period of time, which the Finnish law does not enable.[226] For this reason, confidentiality agreements should be concluded with anyone who needs access to the company's trade secrets. This is especially important because the EU Directive gives more manouvering space for the employees in order not to prevent them from moving between MSs and finding work. Therefore, confidentiality provisions should be included in the employment contracts. It has also been suggested that sanctions for breaching the contract should be included as well.[227] It is suggested that it is not too wise to add competition clauses into the contract if confidentiality clauses are already there as the non-competition provisions could turn out excessive for both sides and are unnecessary.[228]

3.2.2. Confidentiality agreements in business useful but unnecessary

Despite limited durability of trade secrets after end of employment, the situation can be different in dealings between businesses. As evidenced by the *Lynx Rifles* case, a company receiving other company's trade secrets for cooperation projects must keep secrecy even after the cooperation ceases to exist, it must be kept for the entire period when the secret has economic use for its owner. From here, we get an intriguing conclusion that the contractual approach towards trade secrets in employment and business-to-business dealings must be different. In employment cases, non-competition provisions should not be applied and confidentiality agreements should cover the period from two years after the end of employment onwards. In joint venture deals, confidentiality is written in law but confidentiality agreement is still useful, outlying the types of information to be regarded as a secret, to ensure maximum probability of success in court, should a dispute arise.

3.2.3. Detailed descriptions on protection measure obligations of licensees

Measures that the licensee of trade secrets or employee having access should take, should be described with reasonable accuracy but they cannot go into exceptional lengths if fulfilling them would become excessively hard for the other party. An example of reasonable efforts would be the maintenance of trade secret-related information in servers that utilize log-in to limit access.[229]

---

[226] Rikoslaki(The Criminal Code of Finland) (39/1889, amendments up to 766/2015), Ch. 30, Sec. 5(2). Unofficial translation. Accessible: https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001 , 9 April 2019.

[227] Njord Law Firm , (2018), It just became a little easier to protect trade secrets in Sweden and Finland. 07.11.2018. Accessible: https://www.njordlaw.com/it-just-became-a-little-easier-to-protect-trade-secrets-in-sweden-and-finland/ , 9 April 2019.

[228] *Ibid.*

[229] *Ibid.*

3.2.4. Include copyright provisions together with trade secrets

It has also been suggested that companies could rely on copyright provisions to protect their trade secrets and that such reliance could ensure better quality of protection than trade secrets alone.[230] This can make good sense especially for software and its associated trade secrets. Moreover, copyright can also protect parts of the software accessible to end users. It would be useful to include provisions explaining that materials related to software are protected by copyrights in addition to trade secrecy. This is because even though copyrights can be enforced well in courts, the value of trade secrets is their secrecy. Including copyright provisions can prevent infringement through dissuading from copyright infringement. The two IP regimes do not rule each other out and can work together.

3.2.5. Avoidance of cloud service

As cloud technology has emerged and businesses increasingly store their information in the cloud, the technology's effect to trade secrets may arise. It has been seen that storing secrets in cloud basically means outsourcing secret information keeping and this would not be seen as disclosure from this perspective.[231] However, liability restrictions in cloud service providers' terms could negate the confidentiality obligation and amount to disclosure.[232] On that basis, it has been found that the information in cloud loses its secrecy protection.[233] This is an important consideration as Finland is one of the most advanced information-technology-savvy nations in the world, where cloud use is spread.

3.2.6. Avoidance of too wide rights granted to licensee

Owners of software trade secrets may wish to include provisions banning reverse engineering of software products, however, it is not certain they will be accepted under the EU law. The key here is to include such a ban for software that is not made available for the general public but only to the other business or employee. This was important in *MAK-System* case where the defendant was allowed unlimited use of plaintiff's software, causing court to reject infringement claims arising

---

[230] Hynönen, K., (2015), The Copyright Act as a tool for efficient trade secret protection. Newsletters, 11.08.2015. Asianajotoimisto Krogerus Oy. Accessible: https://www.krogerus.com/news_events/newsletters/the-copyright-act-as-a-tool-for-efficient-trade-secret-protection , 9 April 2019.

[231] Psaroudakis, G., (2016), Trade secrets in the cloud. *E.I.P.R.*, Vol. 38, Iss. 6, pp 344-350, p 346. Accessible: https://www.westlaw.com/Document/IE9E6F5501D5211E696F984AF31868E18/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 10 April 2019.

[232] *Ibid.*, p 347.

[233] *Ibid.*, p 348.

from reverse engineering. Therefore, the ban of reverse engineering should apply for the software or its parts if they are not widely distributed.

Altogether, these measures help to protect software companies' trade secrets in Finland.

Next, measures to be taken when entering US market will be given.

3.3. U.S.

The good protection of trade secrets in the US arises from the many economic espionage cases that US businesses have been victim to over the years. Cases involving large corporations like Intel and Microsoft illustrate the danger.[234] It has been viewed that occasions, where secrets are stolen, can pose enforcement hurdles through different attitude in US courts regarding choice of law and extraterritorial application of decisions.[235] In the US, reasonable secrecy protection includes confidentiality, access limitation and information to employees about trade secrets.[236] Employment has been seen as the key danger for trade secrets.[237] Importantly, in the United States, the economic value of the secrets must exist also for competitors, not just owner business.[238] Apparently, the US courts have considered software trade secrets to be exhausted if the product containing it is widely distributed and its architecture has been publicized.[239] The protection of trade secrets in the US is very strong. Software has been considered as a trade secret.[240] The history of the US as a common law country with a great deal of judicial lawmaking has developed this area significantly through case law. In recent decades, Congress has recognized the importance of trade secters and has adopted several federal measures to codify trade secret law.

---

[234] Van Arnam, R. C., (2001), Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection. *N.C.J. Int'l L. & Com. Reg.*, Vol. 27, pp 95-140, pp 95-96. Accessible: https://heinonline.org/HOL/P?h=hein.journals/ncjint27&i=103 9 April 2019.

[235] Rowe, E. A., Mahfood, D. M., (2014), Trade Secrets, Trade, and Extraterritoriality. *Ala. L. Rev.*, Vol. 66, pp 63-104, p 73. Accessible: https://heinonline.org/HOL/P?h=hein.journals/bamalr66&i=73 , 9 April 2019.

[236] Van Arnam (2001), *supra nota* 234, p 103.

[237] Newman (2007), *supra nota* 10, p 25.

[238] Van Arnam (2001), *supra nota* 234, p 104.

[239] Vinje, T. C., (1994), Threat to reverse engineering practices overstated. *E.I.P.R.*, Vol. 16, Iss. 8, pp 364-366, p 364. Accessible: https://www.westlaw.com/Document/IB91E5201E72111DA9D198AF4F85CA028/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 10 April 2019.

[240] Dial, A. A., (2016-2017), Modern Protection of Business Interests through Trade Secret Enforcement. *J. Marshall L.J.*, Vol. 10, pp 19-44, p 26. Accessible: https://heinonline.org/HOL/P?h=hein.journals/jmlwj10&i=25 , 9 April 2019.

Overall, United States uses standard definitions of trade secrets. Source code and object code of computer programs seems to be well established as information that can be covered by trade secrecy. Reverse engineering is usually considered permissible, though, if its sole purpose is to ensure the interoperability between different programs. As a country founded on freedom of individuals in their conduct, contractual terms are given a rather large degree of freedom, allowing for the owners of software to draft agreements offering sufficient protection to their programs. Through contractual protection, even trade secrets that could potentially fail their qualification analysis, could perhaps still be protected through other contractual obligations and infringer tried not for trade secret misappropriation but for contract breach.

From here, it is possible to develop main recommendations for contractual protection of trade secrets in the US.

3.3.1. Preemptive confidentiality agreement secrecy obligations

Any information desired to be protected as trade secrets should be accompanied by a confidentiality agreement and the agreement's acceptance should be the precondition for the access to software by licensee. In addition, the licensor should enter secrecy maintenance procedures and measures into the contract to ensure that licensee is well-equipped for defending the secrecy of information. However, for the sake of practicality, such measures hould not be overly complicated or confusing.[241] Non-compete agreements should be signed with those workers located outside of Californian state.[242]

3.3.2. Auditing rights

Auditing rights should be included to verify compliance. These auditing rights can be wide, in temporal, scope-wise way.[243] Auditing rights should include unannounced (or with short announcement time) visits to licensee’s business premises, access to log data regarding the identities of people gaining access to secret information, time, duration, authorization of access. All operations done such as alterations, copying, downloading should be made available for the licensor. Auditing rights should also include an up-to-date overview of protective measures by licensee, including procedure for obtaining authorization for accessing confidential data.

---

[241] Quinto (2009), *supra nota* 5, p 203.
[242] *Ibid.*, p 205.
[243] Machal-Fulks, J., Barnett, C., (2012), Enterprise Software Licensing - New Options, New Obligations. *Tex. Wesleyan L. Rev.*, Vol. 18, pp 753-766, p 764. Accessible: https://heinonline.org/HOL/P?h=hein.journals/twlr18&i=765 , 9 April 2019.

3.3.3. Ruling out reverse engineering/decompilation

Reverse engineering is usually permitted in the US but can be outruled through contractual measures, although it may come under judicial scrutinity. However, it has been suggested that if the contracts are truly negotiated between parties that are likely to know the area of business, decompilation and other reverse engineering prohibitions could be valid and enforceable.[244] Prohibition of decompilation is actually rather common in software license agreements.[245]

3.3.4. Dispute resolution

United States as a common law country is very pro-judicature, unlike Asian countries, and arbitration could potentially sometimes be met with judicial skepticism. In the last hundred years, however, arbitration has become more accepted and several arbitration panels exist in the US. Parties can choose the applicable law and venue, although it cannot be ruled out that some courts may potentially see US law as applicable. As a result, the first line of dispute resolution should be negotiations, followed by arbitration or courts, according to parties' choice.

3.3.5. Confidentiality for visible parts

Unlike in many other jurisdictions, publicly known data can also become a trade secret in the US. For this, the compilation of publicly known information is what can be a trade secret. Therefore, such compilations should be protected with confidentiality provisions. They should be specifically mentioned to give the other party clear information on which data and in which form is restricted. Confidential information should be clearly marked, without unduly complex categorization.[246] If a company also wishes to protect visible parts of the software, these can be protected as trade secrets, but to do this, they must be mentioned in the confidentiality provisions. Also, the software cannot be so widely distributed so that the user interface becomes publicly known. If confidentiality is not included, as happened in *Broker Genius* case, then visible parts of software lose their secret status.

---

[244] O'Rourke, M. A., (1995), Drawing the Boundary between Copyright and Contract: Copyright Preemption of Software License Terms. *Duke L.J.*, Vol. 45, Iss. 3, pp 479-558, p 535. Accessible: https://heinonline.org/HOL/P?h=hein.journals/duklr45&i=505 , 9 April 2019

[245] Azar, D., (2008), A Method to Protect Computer Programs: The Integration of Copyright, Trade Secrets, and Anticircumvention Measures. *Utah L. Rev.*, Vol. 2008, Iss. 4, pp 1395-1432, p 1423. Accessible: https://heinonline.org/HOL/P?h=hein.journals/utahlr2008&i=1401 , 9 April 2019.

[246] Quinto (2009), *supra nota* 5, p 203.

3.3.6. Concurrent use of trade secrets, patents, copyright

In the US, software is patentable under certain conditions. However, in *Broker Genius*, the Court invalidated trade secret claims by plaintiff because the plaintiff had applied for a patent. This is an important consideration. Patenting software means that software and most of its parts are made public. However, the accompanying information not directly necessary for executing the program (such as user interface architecture, design features, and accessory algorithms, among others) can remain secret under proper management. However, the Court's judgment in *Broker Genius* casts this in doubt. A solution for software producers would be to limit the information disclosed in patent application to bare minimum while specifically outlining trade secrets in the confidentiality agreement. This can help to reap benefits from both IP areas.

Copyright protection can provide additional protection to software. Trade secrets do not invalidate the copyright in software code. It has been noted that contractual licensing does not affect validity of copyright protection.[247] However, it is possible to limit distribution of copyrighted software through contractual means,[248] potentially aiding to keep trade secrets limited in spread. However, as in *Broker Genius*, mere copyright protection provisions are unsuitable for trade secret protection, meaning that to keep trade secrets protected, confidentiality provisions addressing trade secrets specifically should be included. Therefore, the most beneficial strategy would be to include both copyright and confidentiality provisions into contracts. Nevertheless, distribution of software can be limited contractually by specific conditions or through banning it outright. It has been noted that as neither patents of software nor copyright in the US require source code to be revealed, they can be used at the same time with trade secrets.[249]

3.3.7. Associate confidentiality

The confidentiality provisions in contracts directed to business partners should also expand the obligations of confidentiality to partner's agents, subsidiaries, employees and such, obliging the partnering company to give guidance to them. It has been emphasized that confidentiality contracts should be separate agreements to avoid disputes relating to validity after expiry of original

[247] Rowland, D., Campbell, A., (2002), Supply of Software: Copyright and Contract Issues. *Int'l J.L. & Info. Tech.*, Vol. 23-40, p 27. Accessible: https://heinonline.org/HOL/P?h=hein.journals/ijlit10&i=29 , 9 April 2019

[248] Nadan, C. H., (2004), Software Licensing in the 21st Century: Are Software "Licenses" Really Sales, and How Will the Software Industry Respond? *AIPLA Q. J.*, Vol. 32, Iss. 4, pp 555-656, p 586. Accessible: https://heinonline.org/HOL/P?h=hein.journals/aiplaqj32&i=563 , 9 April 2019.

[249] Azar (2008), *supra nota* 245, p 1422.

software contract[250] in addition to being included in original agreement.

3.3.8. Various contractual approaches

Case law in the US has also recognized that in any case, contracts can patch up gaps left by law. Contracts could be drafted to protect new technology, including software. Such measures could include limiting software use to licensee's internal functions, certain locations of licensee's business[251] or forbidding the use of software for commercial purposes[252] outside the scope of the agreement. It has been suggested that when licensing out source code without derivative work ban, a reciprocal license to improvements without fees should be included.[253] For custom-developed programs, the licensor could consider retaining ownership while paying fees to licensee for relicensing.[254] In such cases, even if trade secrets should prove invalid in court or arbitral proceedings, the owner of trade secrets can still obtain relief through asserting claims of breach of contract.

In conclusion, there are many ways of protecting trade secrets through contractual means in the United States.

Next, recommendations are provided for China.

3.4. China

In terms of recognition of foreign judgments, China has two regimes written in the Chinese Civil Procedure Code.[255] This occurs either through a bilateral judgment enforcement treaties or through a principle of reciprocity if it does not contradict main principles of Chinese law, PRC's sovereignty, public interest or public security.[256] Judgment regime of China has not been viewed

---

[250] Classen, H. W., (1996), Fundamentals of Software Licensing. *IDEA*, Vol. 37, pp 1-86, pp 33-34. Accessible: https://heinonline.org/HOL/P?h=hein.journals/idea37&i=11 , 9 April 2019.

[251] *Ibid.*, pp 8-9.

[252] Marotta-Wurgler, F., (2007), What's in a Standard Form Contract - An Empirical Analysis of Software License Agreements. *J. Empirical Legal Stud.*, Vol. 4, pp 677-714, p 695. Accessible: https://heinonline.org/HOL/P?h=hein.journals/emplest4&i=687 9 April 2019.

[253] Classen (1996), *supra nota* 250, p 11.

[254] *Ibid.*, p 29.

[255] Tsang, K. F., (2017), Chinese Bilateral Judgment Enforcement Treaties. *Loy. L.A. Int'l & Comp. L. Rev.*, Vol. 40, pp 1-49, p 3. Accessible: https://www.westlaw.com/Document/I14bea741768b11e79bef99c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 17 January 2019.

[256] *Ibid.*, pp 3-4.

with confidence due to its unpredictability, causing arbitration to rise as a recommended dispute resolution regime for businesses operating in China.[257] The enforcement of IP rights in some areas of China is lacking potentially due to the view of the local authorities in protecting the local industry.[258] It has been suggested that the two enforcement options possible within China should be chosen according to the purpose - administrative route for a fast result with a higher chance of encountering a more technologically knowledgeable personnel while judicial route can provide a more lasting solution, especially in higher courts with specialized panels.[259] Arbitration decisions originating in a foreign entity have seldom been rejected in China.[260] Instead, it appears that in the case where lower courts reject foreign arbitration awards, they need to send those rejections for approval to the higher level, culminating in the highest level.[261] However, there have been opinions that in reality, the recognition of foreign arbitration awards might be more infrequent than some studies show.[262] In the 1990s, the enforcement of arbitral awards originating in foreign countries were considered by some as unenforceable in practice.[263] While in recent years, several practicioners have taken on a more positive view on Chinese enforcement situation, others continue to be sceptical.[264] The grounds for refusal of enforcement written in the New York Convention have been used on several occasions by Chinese courts to refuse recognition of awards.[265] In some cases, the Chinese courts have concluded that although parties had chosen English law to govern the arbitration, that law only applied to substantive portions of the dispute, while law of venue (Hong Kong) governed the procedural part.[266] Although those entities who

[257] *Ibid.*, pp 4-5.
[258] Cunningham Jr (2017), *supra nota* 142, p 297.
[259] Chien-Hale, E., (2008), Intellectual Property Aspects of Doing Business in China. The realities of the Chinese intellectual property protection system make it essential to apply for protection as early as possible. *Prac. Law.*, Vol. 54, Iss. 4, pp 23-28, p 26. Accessible: https://www.westlaw.com/Document/I0aa3a06c626411dd935de7477da167c1/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 22 January 2019.
[260] Zhang, T., (2017), Judicial Sovereignty and Public Policy Under Chinese Arbitration Law. *Am. Rev. Int'l Arb.*, Vol. 28, pp 369-403. Accessible: https://www.westlaw.com/Document/I3c732daf660911e89bf199c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 22 January 2019.
[261] *Ibid.*, pp 383-384.; Alford, R. P., Ku, J. G., Xiao, B., (2016), Perceptions and Reality: The Enforcement of Foreign Arbitral Awards in China. *UCLA Pac. Basin L.J.*, Vol. 33, pp 1-26, p 10. Accessible: https://www.westlaw.com/Document/I379e39b2a7ee11e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 27 January 2019; Gu, W., (2017), Piercing the Veil of Arbitration Reform in China: Promises, Pitfalls, Patterns, Prognoses, and Prospects. *Am. J. Comp. L.*, Vol. 65, pp 799-840. Accessible: https://www.westlaw.com/Document/Ia07f51cf281611e89bf099c0ee06c731/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 27 January 2019.
[262] Alford (2016), *supra nota* 261, p 3.
[263] *Ibid.*, pp 5-6.
[264] *Ibid.*, p 6.
[265] *Ibid.*, pp 1-26.
[266] *Ibid.*, p 17.

have recently tried to enforce awards have reported greater success rates, it should be noted that almost half of survey respondents had chosen settlement rather than enforcement.[267] Lack of measures to implement independence provisions of the Arbitration Law, the administrativeness and financial independence concerns cast doubt on the Chinese arbitration system.[268] It seems that there are significant issues in China related to acceptance of foreign arbitral awards. Also, the choice of law recognition seems to favor the law close to Chinese culture and legal system. However, some see that improvements have been made over past decades.

As for the arbitration itself, the business culture in China appears to favor arbitration over litigation.[269] The Arbitration Law of China seems to have been modeled after international instruments, but there are some modifications such as subjecting jurisdictional issues of arbitration under judicial control.[270] Although there are competing arbitration entities in China nowadays, CIETAC remains the primary arbitration organization dealing with foreign-related disputes.[271] CIETAC has received criticism of its strict rules and heavy involvement of arbitrators in the cases as well as for having authority to point arbitrators, most of whom turn out to be of Chinese descent.[272] Because of this, it is often believed in practice that it is more beneficial for foreign businesses to arbitrate by CIETAC rules in Hong Kong, rather than in mainland.[273] However, of all the arbitration centers in mainland, CIETAC is recommended to businesses in practice.[274] The arbitration rules of CIETAC appear to be more favorable to foreign-related disputants than domestic ones in several matters, including composition of arbitral commissions, interim measures, among others.[275] Chinese culture is mistrustful of judicature. Therefore, direct negotiation is preferred method for resolving disputes, followed by arbitration. Despite its problems, CIETAC is recommended venue for mainland disputes.

In litigation, especially in patent litigation, it appears that the subject matter of the cases are geographically rather concentrated by industry type, with pharmaceuticals-based cases litigated in

---

[267] *Ibid.*, p 24.
[268] Gu (2017), *supra nota* 261.
[269] Huang, J., (2017), One Country, Two Systems: Hong Kong's Unique Status and the Development and Growth of Arbitration in China. *Cardozo J. Conflict Resol.*, Vol. 18, pp 423-455, p 423. Accessible: https://www.westlaw.com/Document/Id46abecbd9e211e698dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 23 January2019.
[270] *Ibid.*, p 435.
[271] *Ibid.*, pp 435-436.
[272] *Ibid.*, p 440.
[273] *Ibid.*, p 441.
[274] *Ibid.*, p 443.
[275] Gu, (2017), *supra nota* 253, pp 805-806.

Beijing, as well as ICT-related cases, while automotive case law is mostly discussed in Shanghai.[276] It has been claimed that litigation success rate for plaintiffs tended to very between 40 and 70 %.[277]

Of all forms of intellectual property, trade secrets are the most difficult type to protect adequately in China.[278] Firstly, there are differences in Chinese business culture regarding confidentiality, with secrets often shared with family members or friends who can then take advantage of them.[279] It has been observed that often, foreign companies wishing to enforce their intellectual property rights make payments to authorities which can lead to increased demands for payment and multiplication of demanders.[280] This presents problem for foreign companies, especially for those from the US because not only are these payments illegal by Chinese law but they are also forbidden by Foreign Corrupt Practices Act in the US.[281] Enforcement of the Unfair Competition Law has been considered ineffective due to protectionism.[282]

Trade secret protection in China appears to have variable results. The situation appears to improve, with greater recognition of freedom of contract and greater acceptance of foreign judgments. Arbitration appears to develop. However, enforcement issues remain and the superiority of PRC law and courts may pose problems.

Next, the focus shifts to giving SMEs contractual tools to use on the basis of previous analyses in order to ensure that their trade secrets are well protected.

---

[276] Love (2016), *supra nota* 141, p 727.
[277] *Ibid.*, p 728.
[278] Stiebel, T., (2013), Protecting Trade Secrets in China: A Roadmap. *Aspatore*, Vol. 2013 WL 4192390, pp 1-12, p 1. Accessible: https://www.westlaw.com/Document/I45761eb2064711e38578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 28 January 2019.
[279] *Ibid.*, p 1.
[280] Chow, D. C. K., (2016), Why Multinational Companies Doing Business in China Fall Into the Trap of Making Payments to China's Police. *Rich. J. Global L. & Bus.*, Vol. 16, pp 1-19, p 2. Accessible: https://www.westlaw.com/Document/I6797a21a1a9c11e798dc8b09b4f043e0/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 9 April 2019.
[281] *Ibid.*, p 3.
[282] Mei, L., (2012), *Conducting Business in China: An Intellectual Property Perspective*. (United States of America: Oxford University Press), p 26.

3.4.1. Protect IP immediately, avoid trade secret introduction to China

In terms of practically protecting trade secrets, it has been advised that companies file the applications for the protection of their intellectual property right after entering China.[283] On that note, it must be remembered that China does not willingly grant software patents.[284] For trademarks, it is advisable to take care and file the English, Traditional Chinese, Simplified Chinese and Pinyin forms of the trademark, along with translations.[285] To aid in the enforcement of intellectual property rights, Service Centers have been set up in China that help the aggrieved party put together necessary paperwork.[286] It has been suggested that after evaluation of trade secret importance for the enterprise has been analysed and determined to be crucial, trade secrets should be kept away from China.[287] This advice should be adhered to. It is always best policy to avoid risk altogether. However, often it is not possible to exclude trade secrets from partners. In such cases, all available IP protection measures should be used, including patent and copyright protection, without revealing trade secrets. Trade secrets protection measures in China should work in cooperation with other IP rights to ensure best protection.[288] Trade secrets protection should start with intra-company confidentiality policy. This policy should clarify which information is confidential, how it should be handled, what are the consequences for violations.[289] Confidentiality agreements should be applied. Computers containing trade secrets should not be connected to networks and downloading and installing non-work-related programs should be restricted.[290]

3.4.2. Preemptive bilingual confidentiality agreement

The main instrument for protection of trade secrets for whichever the form of foreign-related business entity is confidentiality agreements.[291] A foreign party operating in China should definitely sign confidentiality agreements with any entity that wishes to have or may have access to confidential information, and if such entity refuses to sign such an agreement, a foreign company

---

283 Chien-Hale (2008), *supra nota* 259, p 23.
284 *Ibid.*, p 25.
285 *Ibid.*, p 26.
286 *Ibid.*, p 27.
287 Bai (2011), *supra nota* 182, p 370.
288 Bach, J., (2009), Strategies for IP Protection in China. *Aspatore*, Vol. 2009 WL 533083, pp 1-9, p 8. Accessible: https://www.westlaw.com/Document/Ide6168b112cb11deb055de4196f001f3/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 30 January 2019.
289 Bai (2011), *supra nota* 182, p 365.
290 *Ibid.*, p 366.
291 Stiebel (2013), *supra nota* 278, p 3.

must be careful in any further dealings with this entity.[292] Refusal to sign such an agreement should raise concern regarding the purpose of such refusal. In such situations, it is better to be wary.

It is important aspect to note that the confidentiality/non-disclosure agreements that are used in China must be adapted to Chinese legal environment to assure that they remain enforceable.[293] It is important to draft the confidentiality agreement in both English and Chinese as it makes it faster to be understood by the court and can speed up the application of protective measures, which in turn can significantly reduce or even prevent damage.[294]

It is advised that non-disclosure clauses should be drafted so that they will be applied to subsidies, partners or other entities that the contractor deals with to ensure that information is shared on a need-to-know basis only and that those who receive confidential information have identical non-disclosure agreements in place with the main contractor.[295]

It must also be understood that even if the business partner is honest and respects the foreign businesses's trade secrets, this does not mean that trade secrets cannot leak through them. This means that companies doing business in China need to have good trade secret protection policies and they need to include provisions into the non-disclosure agreements that put the obligation on other party to follow these procedures as well.

3.4.3. Chinese venue preferable

It has been suggested that contrary to popular opinion, it may not be best to select a foreign jurisdiction but rather a Chinese court or arbitration organization.[296] It is also important to remember that when asserting a claim, the legal council must be a local, advisably proficient in English.[297] For this reason, it is good to choose a major city as a venue, as it is more likely to find a good English-speaking counsel there. In remote areas, there can be a risk of local protectionism and lack of suitable legal counsel.

[292] *Ibid*.
[293] *Ibid.*
[294] *Ibid.*
[295] *Ibid.*, p 4.
[296] *Ibid.*, p 3.
[297] *Ibid.*, p 3.

A highly recommendable provision in contracts involving Chinese partners is the provision for arbitration. Such a provision should be in Chinese, the clause itself must have specific language, examples can be found in CIETAC's website.[298] It is also worth noting that using this arbitration body and having one foreign member in arbitration panel is rarely opposed by Chinese parties.[299] This makes it a highly recommendable provision. In Chinese business culture, conflict is not focused on, rather, negotiations are seen as the main tool for addressing differences and negotiations are seen as beginning with an agreement.[300] Therefore, it is recommendable to begin dispute resolution chapter of the contract with negotiations and failing to reach agreement, arbitration should be provided for, applying most suitable law, possibly CISG, Hong Kong or Singaporean law and having venue in CIETAC offices. If a foreign company absolutely does not wish to have a Chinese venue, Singapore has been established as an acceptable venue for Chinese courts. Singapore is also a common law country and may be preferable for companies originating from a common law country. Singapore is also generally regarded as a country with strong rule of law, making it an attractive venue together with its experience in technology.

3.4.4. Liability should be wide for licensor

Limitation of liability clauses are not looked well upon in China and if the damages are limited, such provisions might not be enforced.[301] Therefore, a good strategy would be to provide a reasonable amount of damages while limiting excessive claims. Damages could be limited to direct damages with a few easily provable indirect damages to achieve necessary balance.

3.4.5. Check representative identity, signature, seal authenticity

It is also important to pay attention to the signature on the document and make sure that the person signing is the actual representative of the company (names can be received from the local Administration for Industry and Commerce Offices) and that the actual seal or chop of the company accompany the signature.[302] If this is not done, it may happen that the employee signing the contract does not have a representation function within the company. This can later cause problems as the foreign company may wish to enforce contract or seek relief from court, only to discover that the contract is unenforceable. Companies in China can use such a method for gaining access to trade secrets, escaping responsibility. Forgery of documents can also take place.

---

[298] *Ibid.*, p 5.
[299] *Ibid.*, p 5.
[300] Bach (2009), *supra nota* 288, p 3.
[301] Miao (2007), *supra nota* 171, p 104.
[302] Stiebel (2013), *supra nota* 278, p 3.

3.4.6. Prohibition on damaging behavior

Doing business in China runs the risk that after secrets have been disclosed to the partner and the partner has become proficient in their application, they might try to compete with the foreign business directly.[303] To avoid this, there needs to be a Chinese-tailored provision in the confidentiality agreement barring either party from directly or indirectly circumventing or otherwise damaging the other party's interests or the business relationship.[304] A provision also needs to be in place in Chinese-related contracts that prevents parties from using confidential information in a way that can damage the owner of the information, barring any use that was not agreed upon, preventing reverse engineering.[305] This is important to circumvent the Contract Law's assignment of ownership of improvements to licensee. Otherwise, licensee could improve upon trade secrets and gain advantage that it then uses against the foreign company. Reverse engineering, behavior that can damage business partner, using information in ways not previously agreed upon should all be specifically banned by a separate provision.

3.4.7. Broad definition of trade secrets

What constitutes trade secrets or confidential information should be broadly defined in the beginning of contract and should include any communication or data in any form.[306] Although, it may happen that some information is exempted in proceedings, such a provision allows to protect the greatest possible amount of secrets. In addition to standard confidentiality agreement, a receipt should be put in place that the entity or person that gets access to trade secrets should sign.[307]

3.4.8. Employment confidentiality, non-competition, rights transfer

For employment contracts, it is important to include confidentiality provisions and specify the company's ownership to any secrets created by the employee during employment,[308] this is especially important for software adaptation done in China.[309] Applying non-compete provisions

---

303 *Ibid.*, p 4.
304 *Ibid.*, p 4.
305 *Ibid.*, pp 4-5.
306 Kantner, R., (2013), Protecting Trade Secrets Internationally Through a Comprehensive Trade Secret Policy. *Prac. Law.*, Vol. 59, Iss. 1, pp 17-27, p 25. Accessible: https://www.westlaw.com/Document/I15dbc1036f6c11e28578f7ccc38dcbee/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 28 January 2019.
307 Bai (2011), *supra nota* 182, p 363.
308 Stiebel (2013), *supra nota* 278, p 6.
309 Miao (2007), *supra nota* 171, p 72.

to employees must take less than two years unless exceptional conditions exist.[310] Art. 92 of Chinese Contract Law maintains confidentiality obligations and good faith principle for the period of time after the contract is terminated.[311] The confidentiality obligation is also set out in Art. 26 of the Regulation on Technology Import and Export.[312] For up to two years after end of employment, non-compete agreement may be entered into for compensation to the employee.[313] Any damages subjected to employee must be efficient but reasonable to ensure their enforcement. Confidentiality provisions are well established in employment contracts but employers should beware that non-compete obligations can only last for two years after end of the person's employment. Remuneration must be sufficient and that requirement can be interpreted strictly by the court. Assignment of IP rights created by employee should be provided.

3.4.9. Diffuse production contracts

In general measures, it is advised to diffuse production or operation by producing different components or parts in different companies and locations to prevent all useful information from coming into partners' view.[314] Another strategy is to produce the most advanced or latest products or components in IP-secure jurisdictions such as US or Europe while producing older models or less relevant components in China.[315] In China, there is no discovery possibility, requiring the owner of trade secrets to prove misappropriation with original documents.[316] As can be seen, software trade secrets can be protected through licensing the use of different components or modules to different companies in different regions. In that case, the modules should be assembled into a functional software either outside China or if not possible, in licensor-controlled premises in China to avoid any contractor from knowing substantial portions of trade secrets of the software.

3.4.10. Contract language

Another important consideration is keeping the contract language understandable, reducing legal terms.[317] this is important and can affect both signing of the contract as well as possible enforcement. Contract language should be understandable and jargon-free to remain enforceable.

---

[310] Stiebel (2013), *supra nota* 278, p 6.
[311] Bai (2011), *supra nota* 182, p 368.
[312] *Ibid.*, p 368.
[313] *Ibid.*, p 369.
[314] Stiebel (2013), *supra nota* 278, p 8.
[315] *Ibid.*, p 8.
[316] Stiebel (2013), *supra nota* 278, p 8.
[317] Miao (2007), *supra nota* 171, p 98.

3.4.11. Other considerations

It could be useful for Western companies to bear the principle of *guanxi* in mind while doing business in China. It has been suggested on the examples of GM and Google that aggressive action against infringer can be more harmful, with direct contact and striving for a win-win solution being more effective.[318] In the future, trade secret law is likely to be refined in all countries viewed but especially so in China. This is the inevitable result of technological development. In the Asia-Pacific region, Regional Comprehensive Economic Partnership is being negotiated, with substantial emphasis on intellectual property in its draft version.[319] It will be seen how this agreement will affect the intellectual property rights for foreign enterprises doing business in the region. However, it has been suggested that the draft version could benefit European and American firms.[320] As Asia is developing rapidly and innovation is rising as the key economic driver in the region, it can be predicted that at least some point in the future, enforcement in the region will be improved.

[318] Mei (2012), *supra nota* 282, pp 35-38.

[319] Chander, A., Sunder, M., (2018), The Battle to Define Asia's Intellectual Property Law: From TPP to RCEP. *UC Irvine L. Rev.*, Vol. 8, pp 331-361. Accessible: https://www.westlaw.com/Document/I6c7a7b55bc9711e8a5b3e3d9e23d7429/View/FullText.html?transitionType=Default&contextData=(sc.Default)&VR=3.0&RS=cblt1.0 , 3 February 2019.

[320] *Ibid.*, pp 351-352.

CONCLUSION

All three countries have similarities and differences. There are different, characteristic attributes that give each country a distinctive character in trade secret area.

On the basis of recently adopted EU Directive, Finland has adopted a new Act that consolidates regulations on trade secrets, information that was previously scattered between different legal acts. Finnish trade secret protection has been regarded as strong. Finnish case law emphasizes employee protection, limiting the scope of non-competion agreements, also scrutinizing the secrecy of information. Case law also reveals contractual dangers and opportunities.

United States has had several trade secret laws throughout the years, latest of which is the Defend Trade Secrets Act. US is a strong advocate of IP protection. Case law has determined that the scope of trade secrets can be very wide, even consisting of visible and easily ascertainable information (differently from Finnish approach), but such information must be accompanied by confidentiality agreements. Importantly, the courts sometimes view different IP types as mutually exclusive, making it more complex to use multiple systems at the same time.

China has been seen as one of the main intellectual property infringers in the world. However, in recent years, changes have been noticed. Legislation of China has been updated according to international standards. However, enforcement problems exist, due to corruption, protectionism, lack of acceptance of foreign decisions. IP theft and lack of remedies remains a siginificant obstacle for foreign companies. The danger to trade secrets is accentuated by some requirements in Chinese contract law.

Before any company wishes to enter into business in a foreign country, they need to take preventive measures. These preventive measures should include a properly conducted and through IP audit to identify trade secrets and possible gaps in their security. Every business should take precautionary measures for protecting trade secrets, having proper security systems in place. Internal policies directed at trade secret protection must be strong. Those measures help to ensure that trade secrets

are well defended in the studied countries.

For companies wishing to do business in Finland, it is necessary to sign confidentiality agreements with employees, but they should begin from two years after the end of their employment. They can be formed with businesses for extra protection too. It is also advisable to not sign non-competition agreements with employees. Additionally, in license contracts, the measures of trade secret protection that licensees must take have to be detailed but not excessive. On the other hand, licensees should not be given too wide rights, reverse engineering can be prohibited for limited-distribution software. Cloud services should not be used for trade secret-containing information management. These measures can best ensure proper trade secret protection in Finland.

For companies wishing to do business in US, the advice is following. In license agreements, licensee's obligations must be made clear and the agreement should include auditing rights of the licensor and can include ADR measures with free choice of law and venue. In case the agreement is not a standard form contract, reverse engineering can be banned. The agreement should widen the obligation to sign confidentiality agreements to licensee's associates who have access to trade secrets. Contracts can limit the use of software. In case a company produces custom-made software, it should maintain its ownership regarding the customized parts while paying fees to licensee when licensing the custom part to another client. Further, it is possible to protect even visible parts of the software if it is accompanied by confidentiality agreement. It is also advisable to protect trade secrets, copyrights and patents at the same time, but it is important to draft patent claims carefully to avoid disclosing excessive information and thereby invalidating trade secrets. Several details must be kept in mind for good protection of trade secrets in the US.

For companies wishing to do business in China, the following suggestions should be considered. It is best to avoid bringing trade secrets to China and sharing them with Chinese partners. However, if it must be done, it is advisable to protect all IP through copyright and patent (without disclosing too much information). When disclosing trade secrets to business partners and making contracts regarding trade secrets, confidentiality agreements should be signed before any information exchange and confidentiality should extend to associates of the business partner. In China, limitation of liability clauses are unwelcome and there should be reasonably wide liability ò the licensor included. ADR is favored over litigation, with free choice of law (although Chinese law recommended) and venue (best to choose China, then Singapore). In contracts, trade secrets should be defined broadly, including every and all information exchange between the parties. Contracts

can include provisions banning non-agreed-upon use, reverse engineering and damaging behavio towards licensor's business. Contract language should be kept simple and understandable, should not contain excessive jargon. In employment contracts, two-year non-competition provision and confidentiality provisions mút be included as well as provisions about transfer of IP ownership created by employee. It is strongly advisable to check the identity of the representative of partner company and authenticity of signatures and stamps. In case of litigation, local, English-speaking counsel should be used and litigation should take place in major cities. In addition to previous, operations of the company should be divided into parts and separate tasks into separate contracts with separate partners to difuse risks. All companies doing business in China must maintain solid IP policies.

Discussed countries have similarities and differences in their approach towards trade secret protection. Before embarking on business ventures in any of them, recommendable measures including IP audits, internal information policies, and security measures should be taken. In Finland, it is essential to keep contracts simple and to avoid cloud use. In US, almost all matters can be contractually regulated, even protection of visible trade secrets. In China, it is vital to follow legal procedures precisely while keeping contracts simple and to check validity of partner's credentials. On the whole, each viewed country has their particularities regarding trade secret protection, but with careful, culturally sound drafting, it is possible to keep software-related trade secrets safe in all three nations.

BIBLIOGRAPHY

Academic Books:

1. Mei, L., (2012), *Conducting Business in China: An Intellectual Property Perspective*. (United States of America: Oxford University Press), p 26.

2. Quinto, D. W., Singer, S. H., (2009), *Trade Secrets: law and practice*. United States: Oxford University Press, Inc.

Academic Articles:

3. Alford, R. P., Ku, J. G., Xiao, B., (2016), Perceptions and Reality: The Enforcement of Foreign Arbitral Awards in China. *UCLA Pac. Basin L.J.*, Vol. 33, pp 1-26.

4. Azar, D., (2008), A Method to Protect Computer Programs: The Integration of Copyright, Trade Secrets, and Anticircumvention Measures. *Utah L. Rev.*, Vol. 2008, Iss. 4, pp 1395-1432.

5. Bach, J., (2009), Strategies for IP Protection in China. *Aspatore*, Vol. 2009 WL 533083, pp 1-9.

6. Bai, J. B., Da, G., (2011), Strategies for Trade Secrets Protection in China. *Nw. J. Tech. & Intell. Prop.*, Vol. 9, Iss. 7, pp 351-376.

7. Carstens, D. W., (1994), Legal Protection of Computer Software: Patents, Copyrights, and Trade Secrets. *J. Contemp. L.*, Vol. 20, Iss. 1, pp 13-76.

8. Chander, A., Sunder, M., (2018), The Battle to Define Asia's Intellectual Property Law: From TPP to RCEP. *UC Irvine L. Rev.*, Vol. 8, pp 331-361.

9. Cheng, Y., (1996), Legal Protection of Trade Secrets in the People's Republic of China. *Pac. Rim L. & Pol'y J.*, Vol. 5, Iss. 2, pp 261-298.

10. Chien-Hale, E., (2008), Intellectual Property Aspects of Doing Business in China. The realities of the Chinese intellectual property protection system make it essential to apply for protection as early as possible. *Prac. Law.*, Vol. 54, Iss. 4, pp 23-28.

11. Choe, A., (1999), Korea's Road toward Respecting Intellectual Property Rights. *Rutgers Computer & Tech. L.J.*, Vol. 25, Is. 2, pp 341-374.

12. Choudhary, V., (2011), The patentability of software under intellectual property rights: an analysis of US, European and Indian intellectual property rights. *E.I.P.R.*, Vol. 33, Iss. 7, pp 435-446.

13. Chow, D. C. K., (2016), Why Multinational Companies Doing Business in China Fall Into the Trap of Making Payments to China's Police. *Rich. J. Global L. & Bus.*, Vol. 16, pp 1-19.

14. Classen, H. W., (1996), Fundamentals of Software Licensing. *IDEA*, Vol. 37, pp 1-86.

15. Cunningham Jr, K. E. T., (2017), Fine China? A Look Into Chinese Intellectual Property Infringement, Treaty Obligations, and International Responses. *J. Pat. & Trademark Off. Soc'y*, Vol. 99, pp 279-304.

16. Czapracka, K. A., (2008), Antitrust and Trade Secrets: The U.S. and the EU Approach. *Santa Clara Computer & High Tech. L.J.*, Vol. 24, pp 207-272.

17. Desai, S., (2018), Shhh! It's A Secret: A Comparison of the United States Defend Trade Secrets Act and European Union Trade Secrets Directive. *Ga. J. Int'l & Comp. L.*, Vol. 46, pp 481-513.

18. Dial, A. A., (2016-2017), Modern Protection of Business Interests through Trade Secret Enforcement. *J. Marshall L.J.*, Vol. 10, pp 19-44.

19. Dreyfuss, R. C., Lobel, O., (2016), Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security. *Lewis & Clark L. Rev.*, Vol. 20, pp 419-475.

20. Engelman, E. D., (2015), Burdensome Secrets: A Comparative Approach to Improving China's Trade Secrets Protections. *Fordham Intell. Prop. Media & Ent. L.J.*, Vol. 25, pp 589-638.

21. Gaido, C., (2017), The Trade Secrets Protection in U.S. and in Europe: A Comparative Study. *Rev. Prop. Inmaterial*, Vol. 24, pp 129-144.

22. Goodhart, A. L., (1943), Restatement of the Law of Torts, Volume IV: A Comparison Between American and English Law. *U. Penn. L. Rev., American Law Register*, Vol. 91, Iss. 6, pp 487-516.

23. Gu, W., (2017), Piercing the Veil of Arbitration Reform in China: Promises, Pitfalls, Patterns, Prognoses, and Prospects. *Am. J. Comp. L.*, Vol. 65, pp 799-840.

24. Ho, K. L., (2015), American Invents - And So Can You: The Dichotomy of Subject-Matter Eligibility Challenges in Post-Grant Proceedings. *Colum. L. Rev.*, Vol. 115, Iss. 6, pp 1521-1562.

25. Huang, J., (2017), One Country, Two Systems: Hong Kong's Unique Status and the Development and Growth of Arbitration in China. *Cardozo J. Conflict Resol.*, Vol. 18, pp 423-455.

26. Jingen W., DiMatteo, L. A., (2016), Chinese Reception and Transplantation of Western Contract Law. *Berkeley J. Int'l L.*, Vol. 34, pp 44-99.

27. Kahn, R. A., (2017), Economic Espionage in 2017 and Beyond: 10 Shocking Ways They are Stealing Your Intellectual Property and Corporate Mojo. *Bus. L. Today*, Vol. 2017-MAY, pp 1-5.

28. Kantner, R., (2013), Protecting Trade Secrets Internationally Through a Comprehensive Trade Secret Policy. *Prac. Law.*, Vol. 59, Iss. 1, pp 17-27.

29. Kelly, E. A., (1999), Effective Contracting in Software Licensing. *U.N.B.L.J.*, Vol. 48, pp 275-282.

30. Liu, Q., Ren, X., (2017), CISG in Chinese Courts: The Issue of Applicability. *Am. J. Comp. L.*, Vol. 65, pp 873-918.

31. Liu, X., (2016), A Long-Overdue Reform: China's Grant-Back Regime in Technology Transfer. *Fordham Intell. Prop. Media & Ent. L.J.*, Vol. 26, pp 741-768.

32. Love, B. J., Helmers, C., Eberhardt, M., (2016), Patent Litigation in China: Protecting Rights or the Local Economy? *Vand. J. Ent. & Tech. L.*, Vol. 18, pp 713-741.

33. Machal-Fulks, J., Barnett, C., (2012), Enterprise Software Licensing - New Options, New Obligations. *Tex. Wesleyan L. Rev.*, Vol. 18, pp 753-766.

34. Marotta-Wurgler, F., (2007), What's in a Standard Form Contract - An Empirical Analysis of Software License Agreements. *J. Empirical Legal Stud.*, Vol. 4, pp 677-714.

35. Miao, F., (2007), Protection of Intellectual Property Rights in Software Products and How to Accomplish a Technology Transfer Transaction in China. *Fordham Intell. Prop. & Media L.J.*, Vol. 18, pp 61-115.

36. Nadan, C. H., (2004), Software Licensing in the 21st Century: Are Software "Licenses" Really Sales, and How Will the Software Industry Respond? *AIPLA Q. J.*, Vol. 32, Iss. 4, pp 555-656.

37. Newman, B. K., (2007), Protecting Trade Secrets. *Bus. L. Today*, Vol. 17, pp 25-28.

38. O'Rourke, M. A., (1995), Drawing the Boundary between Copyright and Contract: Copyright Preemption of Software License Terms. *Duke L.J.*, Vol. 45, Iss. 3, pp 479-558.

39. Psaroudakis, G., (2016), Trade secrets in the cloud. *E.I.P.R.*, Vol. 38, Iss. 6, pp 344-350.

40. Reid, M., (2016), A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat? *U. Miami L. Rev.*, Vol. 70, pp 757-829.

41. Rowe, E. A., Mahfood, D. M., (2014), Trade Secrets, Trade, and Extraterritoriality. *Ala. L. Rev.*, Vol. 66, pp 63-104.

42. Rowland, D., Campbell, A., (2002), Supply of Software: Copyright and Contract Issues. *Int'l J.L. & Info. Tech.*, Vol. 23-40.

43. Sandeen, S. K., (2017), Implementing the EU Trade Secret Directive: a view from the United States. *E.I.P.R.*, Vol. 39, Iss. 1, pp 4-11.

44. Stevens, L. K., (2001), Trade Secrets and Inevitable Disclosure. *Tort & Ins. L.J.*, Vol. 36, pp 917-948.

45. Stiebel, T., (2013), Protecting Trade Secrets in China: A Roadmap. *Aspatore*, Vol. 2013 WL 4192390, pp 1-12.

46. Tay, L., Lin, J., (2015), Protecting Trade Secrets in Franchising. *Int'l J. Franchising L.*, Vol. 13, Iss. 5, pp 32-40.

47. Tsang, K. F., (2017), Chinese Bilateral Judgment Enforcement Treaties. *Loy. L.A. Int'l & Comp. L. Rev.*, Vol. 40, pp 1-49.

48. Van Arnam, R. C., (2001), Business War: Economic Espionage in the United States and the European Union and the Need for Greater Trade Secret Protection. *N.C.J. Int'l L. & Com. Reg.*, Vol. 27, pp 95-140.

49. Vinje, T. C., (1994), Threat to reverse engineering practices overstated. *E.I.P.R.*, Vol. 16, Iss. 8, pp 364-366.

50. Wadlow, C., (2008), Trade secrets and the Rome II Regulation on the law applicable to non-contractual obligations. *E.I.P.R.*, Vol. 30, Iss. 8, pp 309-319.

51. Zhang, T., (2017), Judicial Sovereignty and Public Policy Under Chinese Arbitration Law. *Am. Rev. Int'l Arb.*, Vol. 28, pp 369-403.

Legislation:

EU:

52. Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful aquisition, use, and disclosure. *The Official Journal of the European Union*, L 157/1, pp 1-18.

53. Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. The Official Journal of the European Union, L 111/16, pp 16-22.

International:

54. Berne Convention for the Protection of Literary and Artistic Works (as amended on September 28, 1979).

55. WIPO Copyright Treaty (WCT) (adopted in Geneva on December 20, 1996).

Finland:

56. Trade Secret Act (Liikesalaisuuslaki) (595/2018), Sec. 2-7.

57. Laki oikeudesta työntekijän tekemiin keksintöihin. Act on the Right in Employee Inventions (21.12.1967/656), Sec. 10, unofficial translation.

58. Laki oikeudesta korkeakouluissa tehtäviin keksintöihin. Act on the Right in Inventions Made at Higher Education Institutions (19.5.2006/369), Sec. 11, unofficial translation.

59. Ministry of Trade and Industry, Finland, Laki sopimattomasta menettelystä elinkeinotoiminnassa. Unfair Business Practices Act (1061/78, amendments up to 461/2002 included), Sec. 1, 4, unofficial translation.

60. Ministry of Justice, Finland, Market Court Proceedings Act (100/2013), Sec. 4, 5, unofficial translation.

61. The Criminal Code of Finland (39/1889, amendments up to 766/2015), Ch. 30, Sec. 5(2). Unofficial translation.

U.S.:

62. American Law Institute, (1939), Restatement (First) of Torts § 757 - Liability for Disclosure or Use of Another's Trade Secret - General Principle.

63. National Conference of Commissioners on Uniform State Laws, (1985), Uniform Trade Secrets Act with 1985 Amendments, Model Law 1985 with Prefatory Notes and Comments.

64. United States Government Publishing Office, (1996), Economic Espionage Act of 1996. 18 U.S.C. 1, Ch. 90, Sec. 1831, 1832, 1837, 1839.

65. US GPO, (2016), Defend Trade Secrets Act of 2016, Public Law 114-153, 114th Congress.

China:

66. Contract Law of the People's Republic of China.

67. Law of the People's Republic of China on the Laws Applicable to Foreign-Related Civil Relations.

68. The Foreign Trade Law of the People's Republic of China. Full text.

69. Law of the People's Republic of China Against Unfair Competition. Full text.

Case law:
Finland:

70. Korkein oikeus, *K Oy v. R*. KKO:2014:50. Issued: 04/07/2014.

71. Markkinaoikeus, *Carement Oy v. Suomen Kuntotekniikka Oy*. MAO: 416/16. Issued: 07/01/2016.

72. Markkinaoikeus, *Lynx Rifles Oy v. Sako Oy*. MAO: 557/18. Issued: 06/11/2018.

73. Markkinaoikeus, *MAK-System International Group v. Finnish Red Cross, Blood Service*. MAO: 320/18. Issued: 06/13/2018.

74. Markkinaoikeus, *Crystalis Entertainment UG, Scanbox Entertainment A/S and Scanbox Entertainment Distribution Rights ApS v. A*. MAO: 383/18. Issued: 07/11/2018.

U.S.:

75. *Decision Insights, Inc. v. Sentia Group, et al.*, Appeal No. 09-2300. U.S. Court of Appeals for the 4th Circuit. Decided Mar. 15, 2011, pp 1-19.

76. *Broker Genius, Inc. v. Nathan Zalta et al.*, 280 F.Supp.3d 495, Signed 12/04/2017.

China:

77. *Di Sijie (Beijing) Digital Technology Co., Ltd. v. Beijing Jiuqiao Software Co., Ltd., and Chuang Chuhua*, (2012), Beijing Haidian District People's Court, No. 20314. Civil judgment.

78. *Wu Yunjie, Guo Zhiming v. Chongqing Paiwei Energy Management Co., Ltd.*, (2012), Min Shen Zi No. 855. Civil judgment.

79. *Yan Jiping v. Tianjin Qisi Technology Co., Ltd.*, (2016), Beijing Third Intermediate People's Court, No. 934. Civil judgment.

80. *Lanling (Beijing) Technology Co., Ltd. v. Beijing Huijinbao Technology Co., Ltd.*, (2017), Supreme People's Court No. 5042. Civil judgment.

UK:

81. *Newbery v James and Others*, Court of Chancery, 27 March 1817, 35 E.R. 1011; (1817) 2 Mer. 446; [1817] 3 WLUK 29.

Regulations:

China:

82. Decree No. 3 [2009] of the Ministry of Commerce of the People's Republic of China Concerning the Measures of the Administration of Technology Import and Export Contracts Registration. Feb. 1, 2009.

83. Regulations on Administration of Import and Export of Technologies (promulgated by the St. Council, Dec. 10, 2001, effective Jan. 1, 2002).

Press releases:

84. Finland Ministry of Economic Affairs and Employment, (2018), New Trade Secrets Act enters into force. Press release, 10.08.2018.

Official Reports:

85. Anderson, R., Turner, S., (Hogan Lovells International LLP), (2011), Report on Trade Secrets for the European Commission: Study on Trade Secrets and Parasitic Copying (Look-alikes) MARKT/2010/20/D.

86. Froman, M. B. G., (2014), USTR 2014 Special 301 Report to Congress FINAL, pp 1-63.

87. (April 2013), Study on Trade Secrets and Confidential Business Information in the Internal Market. Final Study. Prepared for the European Commission. MARKT/2011/128/D, p 135.

Other sources:

88. CISG Status as of early 2019.

89. Griffiths, R., Griffiths, G. E., (1769), Conclusion of the Account of Dr. Smith's New and General System of Physic, from the last Review. *The Monthly Review, Or, Literary Journal*, Vol. 41, pp 278-292.

90. Hynönen, K., (2015), The Copyright Act as a tool for efficient trade secret protection. Newsletters, 11.08.2015. Asianajotoimisto Krogerus Oy.

91. Njord Law Firm, (2018), It just became a little easier to protect trade secrets in Sweden and Finland. 07.11.2018.

92. Schröder, V., (2018), A New Trade Secrets Act Now in Force in Finland. *Roschier*. 23. August 2018.