E

WIPO
WORLD
INTELLECTUAL PROPERTY
ORGANIZATION

WIPO/INN/GE/19/INF/3
ORIGINAL: ENGLISH
DATE: MARCH 9, 2020

WIPO SYMPOSIUM ON TRADE SECRETS AND INNOVATION

organized by
the World Intellectual Property Organization (WIPO)

Geneva, November 25 to 26, 2019

SUMMARY OF DISCUSSION

prepared by the International Bureau of WIPO

Introduction

1. The present document, prepared by the International Bureau, contains a summary of discussions of the Symposium on Trade Secrets and Innovation, held at the WIPO headquarters on November 25 and 26, 2019. The meeting attracted participants from different backgrounds and from various countries. Judges, academics, IP professionals, economists, government and inter-governmental organization representatives, non-governmental organization representatives, and participants from the private sector shared their experiences and ideas on how best to protect trade secrets in an era of digital transformation, where keeping information secret is a growing challenge. Around 200 people participated in the Symposium.

2. The video of the Symposium can be found at webcasting and video-on-demand site of WIPO at: https://www.wipo.int/webcasting/en/. The program and presentations are available at: https://www.wipo.int/meetings/en/details.jsp?meeting_id=53212.

Keynote Speech by the Director General Francis Gurry

3. Trade secrets have been an increasingly important area of intellectual property, but have been somewhat neglected on the international scene. The Washington Act (1911) of the Paris Convention for the Protection of Industrial Property inserted certain provisions for protection against unfair competition in the Paris Convention, but they focused on marketing, branding and indications of source. The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) contains Article 39 regarding the protection of undisclosed information. Beyond those provisions, the issue of trade secret protection has been largely neglected in international discussions, explained the Director General.

4. The diversity of national legal approaches to the protection of trade secrets and confidential information might be at the source of the apparent neglect of the topic, the Director General said. Common law countries and civil law countries have adopted different legal approaches to protect trade secrets, with common law countries generally favoring a comprehensive approach, while civil law countries traditionally relied on specific provisions in the civil code and in the criminal code.

5. Recent years have seen change and some convergence of those two main approaches. For example, the Director General noted that enterprises and governments were giving more policy importance to trade secret protection, and in recent years, many countries, such as the European Union Member States, Japan, China, and the United States of America, had enacted new trade secret legislation, or amended their legislation, bringing more convergence in approaches.

6. The Director General listed four important reasons underlying the increased attention given to trade secrets. The first reason is the fact that digitization has transformed everything into data. Once that data is shared, or communicated, it becomes information, and trade secrets protect confidential information from misuse or misappropriation. The increasing value of data, which is a fundamental business and scientific asset, has witnessed a rise in demand for legal remedies when they are misused or misappropriated in the digital economy.

7. The second reason is that trade secret protection plays a fundamental role in all collaborative business relationships, whether it is in the context of employer/employee relationships, relationships with contractors or sub-contractors, or between university research and companies.

8. As a third reason, the Director General cited the increasing mobility of skilled personnel, as a direct consequence of globalization, and changing business models and global value chains. Enterprises are now more vigilant about the distinction between their proprietary information, on the one hand, and general information that might be shared without restriction among their employees, on the other hand.

9. The final reason is the increased vulnerability of information and data, which are now stored and used digitally through information and communication technologies. This vulnerability is underscored by various pernicious forms of commercial activities, such as cyber-intrusion, hacking or espionage.

10. A fundamental policy question is the apparent dichotomy between the policy of transparency of inventions protected by intellectual property rights, which eventually pass into the public domain, and the protection of trade secrets. Here, it may be noted that, paradoxically, the protection of limited forms of secrecy encourages sharing and disclosure in many types of commercial relationships, such as employment, contractors and R&D relationships.

11. The protection of trade secrets also provides an incentive to the generation of useful information, a lot of which cannot be protected by the patent system for various reasons: either because it deals with the types of information which are generally excluded from patentable subject matter in many countries, such as information relating to business or finance, or because it represents information generated after the patent application process that represents experience with the use of an invention. The heightened attention given to trade secrets has also a strong link to fair competition.

12. The time may now be ripe for the international community to pay more attention to the subject, the Director General indicated, adding that the Symposium had been set up as a conversation, but also an opportunity to explore the possibility for more discussions on the issue internationally, and the establishment of some principles on trade secret protection that might be shared.

13. Many or most trade secret disputes are more about facts than law, and very often, the law is not really in question, the Director General said, introducing a new WIPO digital time stamping service, expected to be operational at the end of March 2020. A digital time stamping service, he explained, is of particular value in having an evidentiary proof of the existence of data at a particular period of time, deposited by a particular person. He mentioned that intellectual property judges gathered in November at the 2019 Intellectual Property Judges Forum warmly welcomed this new WIPO service in the context of evidence that might be coming before them in the course of litigation.

Panel Discussions

14. The Symposium was organized around eight topics, each addressing one aspect of trade secret protection:

- Topic 1: Navigating Trade Secret Systems in the Changing Innovation Environment;
- Topic 2: Trade Secret Systems in innovation, IP Policies and Development;
- Topic 3: National and Regional Frameworks: Recent Developments;
- Topic 4: Economic Impact of Trade Secret Systems on Innovation;

- Topic 5: Integration of Trade Secrets in Business Strategies and Knowledge Management;

- Topic 6: Seeking Remedies for Misappropriation of Trade Secrets;

- Topic 7: Handling Trade Secrets Information during the Procedures before Judiciaries;

- Topic 8: Future of Trade Secret Systems: Addressing Innovation Gaps and Opportunities Derived from Emerging Technologies.

Topic 1 – Navigating Trade Secret Systems in the Changing Innovation Environment

15. The first panel gave an overview of current challenges in trade secrets protection, in particular in the digital age.

16. As the world moves into the fourth industrial revolution, and in the light of increasing interest for trade secret protection, the question is whether there is a need to revisit the approach which had generally been taken, said United Kingdom Ambassador Mr. Andrew Henry Staines, opening this first topic.

17. In the digital age, it is more challenging than ever to keep a secret, as employees could walk out of buildings with thousands of documents on a USB key, a business or research and development (R&D) partner can inadvertently share an entire dataset by clicking the mouse, he explained.

18. Mr. David Kappos, Partner, Cravath, Swaine & Moore LLP, New York, United States of America, said that many types of information can qualify as a trade secret, whether it is financial, business, or scientific information. For example, beyond the world famous Coca-Cola trade secret, supposedly locked in a vault for over a hundred years, how the New York Times decides what books get in its best sellers list is also a trade secret.

19. Globally, trade secret law is a patchwork of different legislations, panelists said, which accounts for the somewhat neglect of the subject internationally. Depending on the jurisdiction, trade secrets can be protected by statute or by common law, and could result in civil or criminal penalties. In the United States of America, the protection of trade secrets can fall under federal or state law and result in either civil or criminal sanctions depending on the circumstances, as illustrated by Mr. David Kappos.

20. However, trade secret has become big business, and with increased interest came increased sanctions, he said, citing Facebook's mishap during its acquisition of Oculus. Due to significant trade secret misappropriation issues with Oculus' files, Facebook was sued and was required to pay around US$250 million in damages.

Patents and Trade Secrets

21. Patents and trade secrets have very different legal frameworks, and have sometime been considered as opposite. Whether it is the kind of rights conferred by patent and trade secret protection, the time limitation of those rights, disclosure requirements, or the protectable subject matter under patents and trade secrets, for example, everything seems to set them apart. However, closer look to these legal mechanisms reveals that, when it comes to protecting innovation, their roles can be intertwined and complementary to each other.

22. According to Mr. José Manuel Otero Lastres, Professor of Commercial Law at the University of Alcalá de Henares, in Spain, trade secrets are not industrial property: it is protection against conduct, and not an exclusive right. While innovators seem to be presented with two choices, either seeking patent or trade secret protection is not the exhaustive choices available for innovators. There is a third way that is widely used, he said. In most cases, innovators decide to patent the core technical feature of their inventions, and keep the knowledge surrounding the patent, secret. Sometime the know-how will eventually lead to a new patent, adding to the previous one.

23. In 2017, the European Union issued Directive 2016/943 on the protection of undisclosed know-how and business information (hereafter referred to as the EU Directive) against their unlawful acquisition, use and disclosure. In 2019, the EU Directive was transcribed in Spanish law (Act N°1 of 2019), Mr. Otero Lastres said, adding that the Directive and the Spanish Act give a positive definition of what is considered secret (Article 2), and a list of limitations to the scope of protection (subject matter and scope).

24. While at present, trade secrets often receive indirect protection via unfair competition rules, countries can foster a dynamic innovation environment by protecting trade secrets under a *de jure* regime of its own, according to Mr. Kappos. He gave the example of China, which earlier this year enacted specific trade secret protection provisions in the Law against Unfair Competition.

Evolving Innovation Landscape

25. Ms. Elisabeth Kasznar Fekete, Senior Partner at Kasznar Leonardos, São Paulo, Brazil, discussed the issues from the conceptual, contractual and enforcement standpoint. She commented on the evolution of the innovation environment, citing several major changes, including: (i) the digital transformation and fast technological changes; (ii) the development of partnerships and joint research by teams of several countries at the same time; (iii) the cross-border transfer of knowledge; (iv) the growing importance of start-ups; (v) increasing incremental and less disruptive nature of innovation; (vi) the growth of services (not patentable) and rising customer demands; (vii) global supply chains; and (viii) high employee turnover. All of these featured in the context of constant threat of intrusion, she said.

26. Trade secret protection, she explained, is the only option for particular situations, such as the earliest stages of innovation, or if some innovations cannot get patents or other intellectual property protection, such as biological processes, abstract ideas, business or commercial procedures, methods and plans.

27. Ms. Kasznar Fekete highlighted that those challenges, as well as key harmonization issues of know-how licensing public policies, suggest that developing certain concepts under the TRIPS Agreement could have a positive effect, because trade secret infringement can jeopardize projects, impacting on the creation of jobs. Those concepts include, for example, “reasonable precautions” to protect a trade secret, adding criminal sanctions for trade secret misappropriators and taking border measures for trade secret infringement. She also called for specific trade secret legislation providing deterrent measures against trade secret theft. In her opinion, the trade secret protection regime is not in contradiction with public access to information: exceptions to trade secret protection being considered in cases of a transparency need of public interest.

Proof of Existence of a Trade Secret

28. Panelists commented on the importance and the challenge to prove the existence and the ownership of a trade secret.

29. Ms. Kasznar suggested that footnote 10 relating to Article 39.2 of the TRIPS Agreement be used more widely when applying that Article. In her view, imposing high standards of burden of proof on the person in control of a trade secret is not compatible with the nature and essence of that asset.

30. Registration of trade secrets with a trusted entity might address the challenges of proving the existence and ownership of a trade secret, but any registration requirements should not force disclosure of a trade secret as a price for demonstrating the existence and ownership of it, said Mr. Kappos. He suggested the use of blockchain-based solutions, which may provide a time-stamped, immutable and traceable record of the creation, continued existence and even the content of the trade secret, while simultaneously ensuring the trade secrets are not hackable or available to third parties. This verifiable record can be subsequently accessed to demonstrate ownership of a said trade secret by a particular party.

Employee Mobility

31. A balance needs to be achieved between the protection of trade secret and employees' mobility. People have their personal skills and experience that they should be able to use in the context of a new job, but workers must comply with rules of good faith and vigilance, said Mr. Otero Lastres.

32. Employee mobility is a tough issue, concurred Mr. Kappos, because it involves a balance between companies wanting legitimately to keep their secrets, and the need to permit employees to move around. The state of California, home of Silicon Valley, has virtually no restriction on employee mobility, which seems extreme, but correlates with an extremely innovative environment, he said.

Topic 2: Trade Secret Systems in Innovation, IP Policies and Development

33. In the second panel moderated by Mr. Kappos, panelists shared experiences from the European Union, Japan, India, and Israel, on how trade secrets are protected in different legislations and contexts.

European Union: Policies underpinning the EU Trade Secrets Directive[1]

34. A public consultation conducted before the adoption of the EU Directive revealed that large and small companies alike find that trade secrets have a positive impact on their competitiveness. SMEs tend to rely even more than larger companies on trade secrets, in particular but not only for cost-related reasons, according to Mr. Davide Follador, Legal and Policy Officer at the European Commission DG GROW.

35. In the context of the fast development of the service industry, globalization, longer supply chains, and an increasing reliance on IT, trade secrets misappropriation is on the rise in Europe. A recent study in the EU showed that theft of trade secrets through cyber means could represent some 60 billion euros/year of potential losses and could affect 1 million jobs.

36. In that new innovation environment, companies tend to use both patents and trade secrets. Studies show that cooperation with other firms on innovation significantly increases the propensity to use trade secrets, in particular when partners are geographically distant. Trade secrets often come as a complement to IP protection, with only a limited portion of critical

[1] Directive (EU) 2016/943 on the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

innovation being patented, the rest being protected by other means, most of the time as trade secrets, according to Mr. Follador.

37. The Directive, which provides for a common set of measures for civil law redress against misappropriation of trade secrets in the EU, nonetheless includes several safeguards, in particular regarding media freedom, the disclosure of trade secrets for the public interest, such as revealing illegal activities, misconduct or wrongdoing and disclosure by workers to their representatives. It provides a list of factors that courts should take into consideration when addressing the proportionality of measures for redress, in particular the public interest, he explained.

38. On employee mobility, the Directive clearly states that trade secret protection should not limit employees' use of information, knowledge and skills acquired in normal employment, striking a balance between the interests of businesses and employees.

39. The Directive does not create exclusive rights, and allows for independent discoveries, and reverse engineering of a lawfully acquired product is possible unless this activity is limited by legally valid duties. The Directive also provides measures so that trade secrets are not used to unduly restrict competition.

Israel: High-tech Hub

40. The Israeli National Technological Innovation Authority, a statutory corporation funded by the Israeli government, supports 1,500 projects and 670 companies. It is responsible for implementing the government policy in research and development (R&D) and innovation, and provides support to the high-tech sector, a leading sector for Israel, representing 12 percent of its gross domestic product, and 43 percent of the country's total export.

41. According to Mr. Zafrir Neuman, Chief Legal Counsel of the Israeli National Technological Innovation Authority, the short technological cycles which also changing social patterns give a growing role to some technologies, such as artificial intelligence, autonomous vehicles, bitcoins, and block chain. Technological change, however, goes faster than expected, and governments need to prepare for the next wave of technologies and create the appropriate infrastructure to facilitate support for those technologies, he said.

42. In the high tech sector, knowledge and IP are the main assets of a company, but changing jobs in Israel is very common and courts would be very reluctant to limit employee mobility on the grounds of trade secret protection. The burden of proof and evidence of trade secret theft is on the former employer.

Japan: Seeking to Raise Awareness

43. Japan considers trade secrets as important as other IP rights, and companies should pay as much attention to their protection, stated Ms. Kanako Watanabe, Director of the Japan IP Policy Office, Ministry of Economy, Trade and Industry. The Unfair Competition Prevention Act (UCPA) regulates protection of trade secrets in Japan. Its revision in 2015 addressed serious challenges of Japanese companies whose technical information was stolen and leaked to foreign entities. Under that revision, more effective civil remedies, such as adding distribution of infringing goods of trade secrets to unfair competition and including a presumption provision, were introduced. In addition, criminal punishments on infringement of trade secrets, such as fines, were increased, Ms. Watanabe explained.

44. Beyond the enforcement of the legislation against trade secret misappropriation, it is important that trade secret holders take measures to protect trade secrets from being stolen,

preventing leakage in daily operations, she said. Since the revision, the IP Policy Office has undertaken serious awareness raising efforts for the benefit of companies, including SMEs. The Office issued a trade secret management guideline, and a handbook for the protection of confidential information, Ms. Watanabe explained.

45. Companies need to delineate which information should be open, and which one should be closed, she added, further noting that it is sometimes difficult to protect data as trade secrets because some companies share data to create new value in their activities. She shared information on the new Japanese legislation regarding protection of shared data. She stressed the importance of ensuring the equivalent level of legal protection on trade secrets in every country in this digital/borderless era.

India: Basket of Rules to Protect Trade Secrets

46. At the time of India's independence, in 1947, the status of technology and industry was very poor in India. The country decided to build its science and technology infrastructure and launched into capacity building, according to Mr. Prabuddha Ganguli, CEO of Vision-IPR, and Visiting Professor at the Rajiv Gandhi School of IP rights, Indian Institute of Technology in Kharagpur. India then imported technology from different parts of the world, and the essential part of its innovation process was adaptation of that acquired technology.

47. To date, India does not have statutory protection of trade secrets, but relies on diverse provisions under which trade secrets are considered, including the Indian Contract Act of 1872, the Copyright Act of 1957, the Arbitration and Conciliation Act of 1996, and the Information Technology Act of 2000, which particularly protects confidential information when it is protected as a database in an electronic form.

48. Trade secrets should be given a distinct protection, and the Indian government, as it launched its 2016 national intellectual property rights policy, recognized for the first time the need to create a separate framework and codification for trade secrets.

49. Mr. Ganguli also highlighted the importance of data and the growing importance of trade secrets related to data, in particular in the context of artificial intelligence.

Topic 3: National and Regional Frameworks: Recent Developments

50. The panel introduced recent legal developments in the United States of America, the European Union and China in the protection of trade secrets. Mr. Mark Schultz, Professor of Law, Southern Illinois University School of Law moderated this panel. He noted that while increased convergence among national/regional legal frameworks on trade secrets was observed, there remain significant differences on core issues relating to protection of trade secrets. He considered that the recent developments in these countries and region are examples of approaches to tackle with modern challenges associated with the trade secret systems.

Legislative Developments in the United States of America

51. The USA Uniform Trade Secrets Act (UTSA), enacted around 30 years ago, was adopted by 49 States, with varying levels of modification, according to Ms. Jennifer Blank, Attorney-Advisor, Office of Policy and International Affairs, United States Patent and Trademark Office (USPTO). The UTSA, she said, harmonizes a number of important issues in State law on trade secrets, such as definition and injunctive relief. According to the UTSA, a trade secret should have an economic value by being a secret and reasonable efforts have to be deployed to protect it. Its misappropriation includes unauthorized disclosure, acquisition or

use, by improper means. "Improper means" includes theft, bribery and misrepresentation. "Improper means" does not include methods such as independent discovery or reverse engineering. The UTSA held a promise of uniformity but the way it was implemented and interpreted in the 49 states could not hold that promise, Ms. Blank noted.

52. In 2016, the Defend Trade Secrets Act (DTSA) was enacted, establishing a federal civil cause of action for the misappropriation of a trade secret for the first time, she said. It intended to provide businesses with a uniform, reliable, and predictable way to protect trade secrets nationwide. The DTSA, does not however pre-empt existing State laws, so businesses can still approach the State courts.

53. One of the new provisions of the DTSA is a seizure order, which can be issued under "extraordinary circumstances". A court may enter an *ex parte* seizure order to "prevent the propagation or dissemination" of the trade secret which is the object of the action. Extraordinary circumstances may include a perpetrator about to flee the country, or an imminent risk that the trade secret will be disclosed to a third party.

54. The provisions of the DTSA seek to provide a framework which would address a variety of situations, and balance the rights of various parties. Particular conditions are attached to a seizure order, including requiring that the application must describe with reasonable particularity what is to be seized, and circumstances identifying the location where the item can be found. Also required is proof that if the person subject to the order had advance notice, he/she would not comply with the Court's order to preserve the evidence and might destroy the evidence.

The EU Directive sets Minimum Standards

55. Each EU Member has to transpose the EU Directive into their own legislation. The Directive sets minimum standards, leaving Member States free to introduce more far-reaching protection measures against misappropriation of trade secrets, if they ensure the safeguards enshrined in the Directive, according to Mr. Follador.

56. The Directive, which sought to harmonize the protection of trade secrets in the European Union, covers a number of aspects, such as the definition of trade secrets, lawful and unlawful acquisition, exceptions and measures against abusive litigations, damages and preservation of confidentiality during legal proceedings. The Directive, however, does not provide harmonized rules (for example, in terms of preservation of/access to evidence), leaving its Member States to regulate that as well as other enforcement-related issues not covered by the scope of the Directive, he said. In this case, Member States' legislations provide for the applicable rules.[2]

57. EU Member States were required to transpose the EU Directive into national legislation by June 9, 2018. An initial report on the implementation of the Directive will be prepared by the EU Observatory to the European Commission in 2021. The Commission will prepare an initial report to the European Parliament and Council in 2022, which will be followed by an impact evaluation report in 2026, he said.

China: Growing attention to Trade Secrets

58. China has been paying steady attention to the protection of trade secrets. It has been part of the 1993 Chinese Law against Unfair Competition (Article 10), which was subsequently

[2] Some national legislators in Europe decided to apply the provisions of the IPR Enforcement Directive to trade secrets (Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights - IPRED).

revised in 2017 and in 2019, as explained by Mr. Huang Wushuang, Professor of Law, Director of the Institute for Intellectual Property at East China University of Political Science and Law.

59. The 2019 revision introduced new elements, for example illicit use and electronic intrusion of trade secret information. The revision also involves confidentiality between employer and employees, between licensor and licensees, and implicates people aiding a person to steal a trade secret. Previous versions or the Law against Unfair Competition only considered businesses and consumers in its scope. A punitive damage provision is also introduced by the revision.

60. Another new element is the updated definition of trade secrets, which now includes technical, operational or other commercial information unknown to the public. In the preceding version, trade secrets were strictly limited to technical information and business information, and did not include other information such as employees' salaries. A major change in the new revised article is the shifting of the burden of evidence to the defendant, Mr. Wushuang said.

Confidentiality of Information during Court Proceedings

61. Confidentiality of information during legal proceedings is often a dilemma, with the need for the Court and lawyers to access confidential information, and the need for the trade secret owner to keep the information secret. The EU Directive seeks to balance the right to a fair trial and the protection of confidentiality, and much leeway is left to the countries and the judges, according to Mr. Follador.

62. In the United States of America, both parties can ask many pieces of information prior to the trial, but in trade secret cases, the courts came up with diverse mechanisms for controlling the discovery process, and meet both the needs of the trade secret holder and those of the defendant. One option is to only permit the lawyers of the parties to see critical evidence, or the judge may be the only one to review evidence in his/her chambers. Courts can be closed for some part of the proceedings while evidence is displayed, explained Ms. Blank.

63. In China, the shifting of the burden of evidence has been discussed for the last 10 years. Under the current Law, where a trade secret holder provides preliminary evidence to prove that it has taken measures to keep the information secret and reasonably demonstrate that the secret information has been misappropriated, the alleged infringer shall prove that there is no such misappropriation, explained Mr. Wushuang.

<u>Topic 4: Economic Impact of Trade Secret Systems on Innovation</u>

64. With little empirical evidence on use and misappropriation of trade secrets, economists are now trying to fill the gaps. Panelists discussed why trade secret theft is generally underreported, and reasons to choose trade secrets over patents.

65. According to Mr. Carsten Fink, WIPO Chief Economist, it is quite difficult to put numbers on trade secrets use, but it is reasonable to assume that they are extremely widely used, in one form or another, by most companies. Economists should worry about trade secret protection, he said, for two main reasons, the first of which are the policy questions around the issue. For example, what constitutes lawful disclosure, in particular in the context of employee mobility? Trade secrets also have a close relationship to patent policies, which rely on disclosure as a means to sustain innovation systems, while trade secrets are based on keeping the invention secret. It is interesting to know about possible long-term effects on what kind of technology gets disclosed or not to the public.

Trade Secret Theft Underreported

66. There is currently very limited empirical evidence on trade secrets. Ms. Nicola Searle of the Institute for Creative and Cultural Entrepreneurship at Goldsmiths University of London, collected all court cases from online records from 1996 to 2018, some 200, in which the defendant was accused of trade secret theft.

67. Her preliminary analysis finds that in 70 of the cases brought under the US Economic Espionage Act, victims were listed companies, i.e., large enough to be on the stock market. Some 60 percent were manufacturing companies, including pharmaceutical companies and defense, 18 percent were service companies and 13 percent were small businesses.

68. Defendants were mostly insiders, someone who could access to the information, like employees or contractors. There was, however, a “surprisingly” low level of computer skills among the defendants, she said, adding that the classic vision of the employee walking out the door with a USB key seems to be holding true. Perpetrators usually target a specific trade secret, she said, adding that a few trade secrets are worth a lot, but most trade secrets are not.

69. In general, very little is known about both trade secrets and trade secrets theft, since they are largely underreported. That trend led to firms not being really aware of what they should do to protect their trade secrets adequately, and left policy makers with a lack of data to respond appropriately. According to a model presented by Ms. Searle, underreporting of cybercrime, which are linked to trade secrets, leads to more cybercrime. She explained that firms generally underreport cybercrime because they are wary of their reputational damage. Consequently, governments are not aware of the extent of the cybercrime, lowering their guard, and issuing less effective policies resulting in more cybercrime incidences. Theoretical modeling suggests that a firm is more likely to invest in high security if breaches can remain private.

70. Ms. Searle further listed some potential solutions proposed for problem of underreporting of trade secrets thefts, such as mandatory theft reporting requirements, financial reporting requirements, data breach reporting requirements, and noted some policy implications relating to those solutions.

Protecting Trade Secret is a Challenge

71. The major economic justification for IP protection is to provide a framework under which innovations can be rewarded, according to Ms. Pallavi Seth, Principal of USA-based The Brattle Group. Trade secrets are used to protect intangible, informational goods. Beyond ingredients, recipes and software algorithms, trade secrets could also include cost structure, pricing strategy, business strategy, specific customer requirements, business plans, product development and timelines, and customer lists.

72. However, their protection is a challenge. Trade secrets are shared with employees and commercial partners, they can be reverse engineered and discovered independently. The cost to maintain their protection is high, and trade secrets could hinder labor mobility.

73. Companies should consider the pros and cons of trade secrets against patents, she said, considering for example, the stage of innovation, the cost of enforcing a trade secret, ability to reverse engineer, and level of competition for related product. She suggested, for example, that manufacturing processes and a unique formula might be best protected through trade secrets. The level of competition can also influence a company choice. If there are multiple competitors on the market, and one of them has the lead, then this company might prefer opting for a trade secret, however if all competitors are fighting for the lead, then patenting might be a better option, according to Ms. Seth.

74. She presented a case based on an investigation at the United States International Trade Commission (USITC), featuring two companies manufacturing activity tracking devices: Jawbone v. Fitbit. Jawbone was an early entrant in wearable technology. Fitbit was the market leader in fitness wearables. At the time of the investigation, they both made watch-sized devices keeping track of steps taken by the holder, and his/her related activity. Jawbone alleged patent infringement and trade secret misappropriation through six former employees, with the theft of some 300,000 confidential files, including product line-ups, supply chain, financial data, designs and consumer surveys.

75. Introduction of new models in that emerging market could lead to “extraordinary” returns, which can accrue to the first supplier to identify and serve a large portion of the market with unmet needs, she explained. Moreover, if products are difficult to copy, premium prices and returns may persist for a significant period, she said. Accessing a competitor’s technological and manufacturing information can signal what technology is ripe for development, and might signal to the misappropriator that he/she should accelerate the development of comparable capabilities for his/her own products, and provide potential shortcuts. The two companies settled the dispute, according to Ms. Seth, who added that the people responsible for the trade secret theft had been indicted at the time of the Symposium.

Topic 5: Integration of Trade Secrets in Business Strategies and Knowledge Management

76. Mr. Héctor E. Chagoya, Senior Partner, Patents & Technology Director, BC&B., Mexico City, moderated this panel, which gathered panelists from various industries and from different sizes of enterprises. They discussed the role and importance of trade secrets in the intellectual property strategy of their companies and how they manage trade secrets and confidentiality within the company as well as vis-à-vis external business partners.

77. Although trade secrets are central to all companies, in the experience of Ms. Sophie Blum, Founding Partner of Ycor Corp, in Geneva, they are less straightforward than patents, and have proved challenging to manage.

78. In the context of a start-ups open ecosystem she set up 10 years ago for Procter & Gamble, which put together big corporations and small start-ups, the issue was to find a way to protect both sides, and take particular care of the small companies. She underlined the importance of the terms of agreements, which, if made public, are damageable to both parties. Another challenge of trade secrets is identification of a trade secrets and the time it takes to properly manage them in the company: describing, updating, and maintaining them to keep the trade secret assets alive. The digital transformation has brought a complete new paradigm on the way to protect trade secrets, and the infinite possibilities of exploitation and exploration of trade secrets, she said.

Complex Products and Products under Legal Obligations

79. Some businesses make a choice not to seek patents. Ms. Nicole Weiland said that her company, Xenometrix, manufactures toxicology test systems, which are complex products and not easily reproducible. She explained that it had had the opportunity to patent their innovation 20 years ago, but had decided not to do it and favored trade secrets. Patenting innovation is a huge investment for a small company like hers, not only in terms of costs but also with respect to human resources commitment. The company would also have struggled to enforce its patents against infringement by large companies, she observed.

80. Some particular legal obligations can also determine choices a company makes. For example, Ms. Rachel S. Lovejoy, Senior Counsel of the US-based company SpaceX, said that

her company specializes in space exploration technology, and designs, manufactures and operates advanced rockets and space crafts. The company launches business and commercial satellites, and manufacture their own satellites. She explained that in the USA, launch technologies are subject to export control obligations, meaning that the disclosure of the technology is not allowed. Thus, keeping the technology as trade secrets fell in line with those obligations. SpaceX has relied on trade secrets, specifically, in relation to launch technologies. She listed several aspects which they would look at in deciding whether to opt for trade secrets or patent protection: rate of innovation in the field, whether the technology requires wide distribution, cost of patenting, competitors interest in the technology, and whether the technology would be mainly domestic or marketed outside.

81. The lack of harmonization on trade secret regulation, scope and standards on the global market is creating increasing problems, said Mr. Zhu Xianmin, Director of Legal Affairs Department for Zhejiang Weixing New Building Materials in China. Noting that trade secrets increases the enterprise value and inspires companies for continuous innovation, he called for the need to improve cross-border protection of trade secrets.

Internal Strategies to Protect Trade Secrets

82. Protecting trade secrets needs a solid internal strategy and best practices. At SpaceX, Ms. Lovejoy thinks first and foremost about who the gate keepers of the trade secret are within the company and makes sure that those people are properly engaged in maintaining that secret. Non-disclosure agreements between employees and third parties with which they interact is important but not fail-safe.

83. As a general principle, she said, third parties should only be shared what they need to know for the service or goods they provide to the company. The IT team also has to understand where the data is held and that it is properly encrypted. Employees, in particular younger ones, have to be reminded that they cannot share pictures of their work to put it online.

84. It is also however important to train staff to protect the trade secrets of others as well, she said, so that SpaceX employees do not purposefully or inadvertently incorporate a trade secret technology of their business partners into SpaceX production.

85. As a small company, Xenometrix does not have a specific strategy but relies on the fact that the staff is a small team and everything that is published crosses Ms. Weiland's desk. The company also takes security steps, sometimes coding a few important chemicals, and concluding non-disclosure agreements.

86. Ycor Corp.'s strategy for protecting trade secrets is based on the concept of "need to know" basis. Ycor Corp. also has a formal process of non-disclosure agreements, and systematic awareness raising, Ms. Blum said.

87. At Zheijiang Weixing New Building Materials, the legal department is in charge of the IP management and has developed internal guidelines to identify and classify trade secrets, Mr. Xianmin said. In relation to licensing of trade secrets, the company chooses its Original Design Manufacturing (ODM) partners with care, based on several criteria, such as credit, infringement history, reputation on the market, and the quality of production people. Regular training is also provided to the partners to protect the company's trade secret assets.

88. Answering to a question about the need for start-ups to provide IP protection of their invention to attract investors, Ms. Blum said some investors would certainly request patent protection for the invention, although if investors understand the potential impact and profit of

the invention, protecting it with a trade secret would be accepted. Ms. Lovejoy added that investors are also interested in protection efforts made by start-ups.

Topic 6: Seeking Remedies for Misappropriation of Trade Secrets

89. Several challenges are in the way of legal remedies for trade secrets thefts. The moderator of this panel, Ms. Nari Lee, Professor, Hanken School of Economics, Helsinki, highlighted some issues relating to misappropriation of trade secrets and available remedies, including causes of actions, forum, civil and/or criminal liability and third party liability as well as practical measures relating to preservation of evidence and cross-border enforcement.

Seeking Remedies in Europe

90. The question as to whether trade secrets are an IP right or not is not clear-cut. In the EU Directive, trade secrets are not considered as an IP rights, which has consequences when seeking remedies, according to Mr. Stefan Dittmer, Partner at Dentons, Berlin.

91. Access to evidence is problematic particularly in trade secret cases, and some facts need to be checked, such as whether the company actually have a trade secret, and whether the trade secret holder has legitimate ownership of the information, he said. This can be challenging, since unlike patent holders who can show registration of his/her patent, there is no trade secret register and no presumption of ownership. Companies have to make sure that when an information that could qualify as a trade secret is created, it would be recorded.

92. According to Mr. Dittmer, although the EU Directive provides some relief concerning the preservation of confidentiality during court proceedings, it has not dispelled the issue, and this lack of trust has led to a shortage of trade secret cases in front of German courts.

93. The list of exceptions contained in the Directive can lead to problematic interpretations, he said. Exceptions include, among others, acquisition, use or disclosure of trade secrets for revealing misconduct, wrongdoing “or” illegal activity (emphasis added). The word “or” could result in including certain legal activities in the list of exceptions. The Directive exonerates such whistle-blowers who acted for the purpose of protecting the general public interest. The general public interest is not defined by the Directive, and such a broad exception makes it difficult for the companies and the whistle blower to apply the provision, he asserted.

94. When assessing the proportionality of remedy, the court has to take into consideration the measures the trade secret holder has applied for preserving the confidentiality of the trade secret. This is open to questions, for instance, should the strength of the measures play a role in remedies, he asked.

USA: Recent Trade Secret Act Does not Stop at Borders

95. As the digital age prompted high interest in trade secret protection, the 2016 Defend Trade Secrets Act (DTSA), passed with overwhelming majority, is a watershed event for IP law, according to Mark Halligan, Partner at Fisher Broyles in the United States of America.

96. One of the major clause of the DTSA is inclusion of Sections 1831 and 1832 of the Economic Espionage Act (EEA) to Section 1961 of the Racketeer Influenced and Corrupt Organizations Act (RICO) as RICO predicate acts. Due to this addition, companies and other victims of trade secret theft can file RICO civil actions based on Section 1831 and 1832 predicate offenses, and obtain treble damages, attorney’s fees and cost for RICO violation, he explained.

97. Sections 1831 and 1832 include a long list of offences relating to the theft of trade secrets, and economic espionage. Section 1837 of the EEA, also included in the DTSA, extends to extraterritorial jurisdictions to conducts occurring outside of the United States under two conditions: "(1) the offender is a natural person who is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof"; or "(2) an act in furtherance of the offense was committed in the United States." Therefore, RICO applies to extraterritorial conducts and US companies now have the tools to protect their trade secret assets not only in the United States but worldwide, Mr. Halligan stressed.

Cooperation between States Needed for Enforcement

98. This point was shared by Mr. Chagoya who underlined the importance of the DTSA's provision on extra territorial issues. This is particularly interesting, he said, as data is everywhere and with cloud computing, servers can be anywhere in the world.

99. He regretted the lack of global harmonization in the protection of trade secrets, and the conflicting rules between jurisdictions in cases of trade secret misappropriation outside of the owner's country. In that case, some cooperation between countries is needed for successful enforcement of judicial decisions. Trade secret protection also falls under different rules, in different countries, such as labor law, commercial law, and cybercrime. This fragmentation affects liability and enforcement against trade secret theft, he said.

100. Measures to keep a trade secret have to do with contracts and confidentiality agreements, but since different laws might be applicable according to jurisdictions, the result is a number of different agreements related to the same trade secret, Mr. Chagoya observed.

101. He underlined the difficulties linked to a necessary harmonization, because trade secrets are based on possession, and rules on possession are not generally harmonized in the world. It would be like trying to harmonize contract law or criminal law, he said.

Identifying Trade Secrets Key

102. Trade secrets are at the core of the competitiveness of a company and linked to its survival, according to Mr. Tong Wu, Vice President and Co-founder of Iptalent Consulting in China. He advised that the most important action a company can take in case of trade secret infringement is to stop the leak in an efficient manner. He called for companies to identify their trade secrets according to the applicable legal regulations. Many companies have a misunderstanding of trade secrets and consider all personal information as trade secrets, making it impossible to recourse to judicial assistance. The cash value of the trade secret must also be assessed, he said.

103. In China, companies can chose remedial measures according to specific situations. For example, if a secret is divulged but has not yet been disclosed publicly or put into practical use, the best approach would be to resort to negotiation with the infringer, which require careful pre-negotiation preparation, including a letter of commitment and a statement of confession.

104. If the secret is publicly disclosed or used illegally, the best option is to seek remedial measures through judicial means, including criminal litigation, civil litigation and administrative penalty, he said.

105. Mr. Chagoya and Mr. Halligan also stated that a trade secret has to be identifiable. Mr. Halligan highlighted the fact that the first step in trade secret protection is to identify and

describe what is to be protected. Only then, the trade secret can be classified, protected and valuated. He referred to a trade secret management software tool, the Trade Secret Examiner®.

Topic 7: Handling Trade Secret Information during the Procedures before Judiciaries

106. This panel discussed measures taken by courts during court proceedings to maintain trade secrets of parties confidential. Ms. Eun Joo Min, Director, WIPO Judicial Institute moderated this panel.

107. According to Judge Jörn Feddersen, Federal Court of Justice, Karlsruhe, Germany, parties in a trial should be ensured of the right to be heard, and the right to a fair trial. The right to be heard includes parties' access to all information provided to and by the court. Should the court limit parties' access to information, it would touch upon their right to be heard. The principle of fair trial is based on the public nature of court hearings and is the centerpiece of the rule of law, which can only be suspended for important reasons: trade secrets being one of them.

108. In Germany, following the direct implementation of the EU Directive, the court can now issue a confidentiality order relating to certain information that is by *prima facie* evidence deemed a trade secret. As a consequence of the confidentiality order, parties, their lawyers, witnesses, experts and any other party participating in legal proceedings are not permitted to use or disclose any trade secret or alleged trade secret, he explained.

109. Wide discretion is given to the court as to which measures should be taken to protect some information. It can be restriction of access to any document containing the trade secret, or alleged trade secret, submitted by the parties, or access to some information could be restricted to a limited number of trustworthy persons. The confidentiality obligation continues to exist after the trial ends, according to Judge Feddersen.

110. Companies had been wary to take their case to court for fear of losing their trade secret, but the new law protecting trade secrets under the German judicial system is expected to confront this hesitation, and lead to an increase in trade secret litigation in Germany.

111. In South Africa, a common law country in this area of law, the protection of trade secrets and confidential information in the course of court proceedings is based on three main principles: fairness; the protection of confidential information; and the right of litigants to give informed instructions to their legal representatives. As transactions are so often well documented, and the disclosure process by way of discovery can be substantial, the risk of disclosure of confidential information is high in certain types of litigation. Therefore, trade secrets are in need of protection, explained Judge David Unterhalter, Justice of the High Court Johannesburg, South Africa.

112. It is for the court to weigh the need for disclosure and risks of disclosure. Usually, the court permits disclosure of relevant confidential information under restrictions of varying degrees of rigor, seeking to retain the essential features of confidentiality, while allowing access to a few persons who are placed under use-restraints, he said.

113. Restraining access can create problems, in particular, for attorneys and counsel who are required to provide advice to their clients on the basis of full information. Some courts are concerned that clients could be deprived of their fundamental right to fairness if their advisors have access to information that they do not, according to Judge Unterhalter. The same question of access arises in the context of regulatory decision-making. How can a regulator decide a contested merger proceeding when it has access to confidential information that is not shared with the parties, he asked.

114. Under Brazilian statutory law, the judge must take measures to protect judicial secrecy in the case of trade secrets, said Ms. Kasznar Fekete. Only the parties' attorneys then have access to the records. She mentioned confidentiality precautions in administrative procedures dealing with IP rights still need improvements: in some cases, rules are inexistent.

115. A variety of non-statutory measures can be requested by the parties and taken by the court to mitigate risks, and can include restriction of access to defendants, a prohibition of copies or photos of confidential documents, in-camera hearing, and closed-door testimony. At issue, however, is the infrastructure of courts, which may not have high security system, and may leave the trade secret at a risk of theft or accidental leak, Ms. Kasznar Fekete said. Another challenging issue is to what extent the judge should require the details of the confidential technology to be disclosed in the judicial dockets by the concerned party and/or by the technical expert appointed by court.

116. With regard to handling trade secret during the court proceeding, Mr. Richard L. Thurston, Of Counsel, Duane Morris LLP, United States of America, stressed the importance of taking reasonable measures to preserve secrecy. In particular, he noted the need to stay vigilant, monitor people in attendance to restrict attendance, and raise appropriate objections to certain exhibits.

Topic 8: Future of Trade Secret Systems: Addressing Innovation Gaps and Opportunities Derived from Emerging Technologies

117. Mr. Yoshiyuki Takagi, Assistant Director General of WIPO moderated this panel. Trying to look into the future of trade secret systems seems like peering through a crystal ball, according to panelists. They provided some insights on what could be expected in the coming years.

118. Entering the digital age meant entering a completely new paradigm, with new possibilities for communication, reproduction, preservation, and utilization of information and knowledge. For some technologies, legitimate reverse engineering becomes easier by the hour, said Mr. Ganguli. He painted a world where new emerging technologies allow what was only science fiction a few years ago becomes a reality, with the development of non-intrusive techniques for mind-reading and mind-recording. Predicting that in 15 years, those techniques will be a commodity, he asked: what would happen to a trade secret if minds can be read? What would be "secret" information?

119. The same question arises in the context of artificial intelligence and self-learning autonomous systems, he noted. Should they be considered as legal entities or employees, trade secrets are going to take a totally different dimension, he said, urging policy makers to consider those questions. There is an imperative need to understand technologies and their potential impact to have a firmer idea of the new paradigm, he explained.

Worldwide Technical Standard a Must

120. Mr. Richard L. Thurston, concurred, saying that technology is evolving so fast that most people cannot keep up with it. Rapidly advancing technological developments in the post computer age, such as borderless shared pools of information in the cloud, are increasing risks for trade secrets, he said. As a potential solution, he mentioned an international knowledge registry, which establishes a different kind of proof of existence of an electronic document. It is a neutral third party system, and has already been deployed for the last three years within several companies, academic institutions, public and private institutes and government entities, he said, adding that it could quickly become a global standard.

121. A formal worldwide standard is a must in an era where trade secrets are more digitally inter-connected, said Mr. Thurston, indicating that WIPO could actually provide such a standard using one or more technology.

WIPO Digital Stamp Service

122. In relation to proof of existence of a trade secret, Mr. Takagi referred to “WIPO Proof”, a new digital timestamping service that WIPO will start next spring. It will allow uses of the service to prove the existence of the digital content. Although it will not automatically prove the ownership of that digital file, it will establish that this file was created at a certain point in time. Nobody can change and modify that file, Mr. Takagi detailed.

Digital Technology, Major Disruptor and Ally

123. Considering the future of trade secret systems, Mr. Jacques de Werra, Professor from the University of Geneva, focused on data and four main challenges related to them: data accessibility, data vulnerability, data mobility/portability and data transparency.

124. With respect to data accessibility, the power of new technologies to collect a massive amount of data raises a fundamental question about the existence of secrecy, and the concept of secrecy. In a 2010 US case, the court found that the information was in fact not secret because it was accessible on-line. Most rules on trade secret protection request reasonable steps to protect the secret, but in an age where digital threats are everywhere, what should be expected as reasonable steps, he asked about the issue of data vulnerability. The issue gets even more complicated in the context of multiple standards and regulations in various jurisdictions.

125. However, technology might also prove an ally in trade secret protection, he said. It might help to identify and protect trade secrets, for example, by recording them on block chain-like systems with a time stamp and use of smart contracts.

126. The mobility/portability of data making it possible to move data from one provider to the other, is a major topic, Mr. de Werra said. The last issue of data transparency and the resulting tension with trade secret protection is also debated, for example, in the context of transparency of algorithms and of clinical data submitted for market authorization applications. Since privately owned data might be part of trade secrets of a company, it is important to find a way to balance competing rights, Mr. de Werra said.

127. Looking ahead, Mr. de Werra raised the issue of the need to adapt the legal standards for trade secret protection, as applied in the context of the new digital technology, and find a way to make the system of trade secret protection enforceable through creative dispute settlement mechanisms (ADR).

Artificial Intelligence and Data Sharing

128. Following up the discussion on the importance of data, Mr. Takagi noted that national policies concerning data ownership or data localization might affect the protection of trade secret and data policy in general. Our economies, he said, are increasingly being driven by data, and due consideration has to be given to data policy in order to establish a level playing field for businesses across borders. This is particularly important in the context of artificial intelligence, as data is used to train algorithms. It seems that nobody has enough data, and already certain partnerships are being formed to share data, he said.

129. Mr. de Werra said that a data sharing agreement needs to specify the conditions under which data can be used. Since data providers might not have any interest in controlling data but might rather be seeking economic remuneration for their use, it might be appropriate to conceive new approaches in order to foster the sharing of data.

130. Mr. Ganguli shared information on the National Digital Library of India. He said it is a digital platform, which integrates various information centers across India, and linking all the libraries in the country, including museums and archives. Metadata are shared by each source, being curated, certified and time-stamped. The sharing of metadata is conditioned by an agreement, i.e., the National Digital Library of India does not own the data. This could serve as a model for other digital data, he said.

131. In concluding, Mr. Takagi noted that the ideas put forward by the panelists on the future of trade secrets seem to gather around the areas of: (i) a hybrid legal framework to cope with emerging needs; (ii) feasible measures to establish evidence; (iii) creative development of dispute settlement procedures, both in court proceedings and alternative dispute resolution systems; and (iv) policy coordination in relation to data sharing or data pooling.

Closing Remarks

132. Mr. John Sandage, Deputy Director General, delivered closing remarks on behalf of the Director General. He thanked all speakers and participants who came to discuss and share their knowledge and experiences on the topic of trade secrets. He said that the Symposium was timely and addressed a wide range of issues relating to the interface between trade secrets and innovation, covering policy, law, economics and business. It also explored new challenges and opportunities for trade secret protection, for large and small companies alike, in particular the potential impact of emerging technologies on the integration of trade secrets in the modern innovation ecosystem.

133. He noted that the Symposium allowed the sharing of information on trade secret protection. Insights from practitioners, academics, policy makers and other stakeholders gleaned during the Symposium have been very useful, he observed. Mr. Sandage expressed his hope that the participants will have found those insights enriching as they consider their own approaches to trade secrets and their protection.

134. He concluded that this first discussion on the topic of trade secrets at WIPO would not be the last, and that the Symposium would open the door to deeper reflections on this subject.

[End of document]