The Case for Enhanced Protection of Trade Secrets in the Trans-Pacific Partnership Agreement

U.S. CHAMBER OF COMMERCE

U.S. CHAMBER OF COMMERCE

THE CASE FOR ENHANCED PROTECTION OF TRADE SECRETS IN THE TRANS-PACIFIC PARTNERSHIP AGREEMENT

COVINGTON

COVINGTON & BURLING LLP

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The ability to innovate and protect one's intellectual property (IP) helps drive economic and cultural growth, development, and investment. However, today's businesses face increasing threats to one of their most valuable intellectual property assets: trade secrets. By today's estimates, theft of trade secrets and other critical business information costs businesses billions of dollars in annual losses.

Economic studies and surveys demonstrate that robust protection and effective enforcement of trade secrets and other intellectual property is critical to a company's ability to innovate, grow, and invest in markets around the globe. The strength of a country's IP protection (including, in many cases, the robustness of trade secret protection) correlates directly with investment, increased R&D expenditures, and technology transfer to a country. Studies also demonstrate the key role that effective protection of trade secrets plays in the development of particular industries in emerging markets and the growth of small businesses.

Trade secrets are increasingly valuable to today's businesses. As detailed in this report, trade secrets can comprise up to 80% of the value of a company's information portfolio. Yet as the value of trade secrets continues to increase, studies also illuminate how vulnerable these assets can be. A variety of studies show that the impact of trade secrets theft and espionage are felt by companies operating in countries of every income level and in every region. Given the proliferation of digital devices, greater workforce mobility, increasing global competitiveness, and the rise of cyber theft, it is not unreasonable to expect trade secrets theft and the losses caused by such theft to be on the rise.

This paper also examines recent cases of trade secret theft and the remedies available to combat this theft. In a number of cases, these examples shine a spotlight on the lack of or insufficient remedies and deterrents to deal with this growing threat. Overall, these cases, which show significant trade secret vulnerability in the Asia Pacific region, suggest that a combination of effective criminal remedies and robust civil enforcement are important for curbing the growing scourge of trade secret theft.

The twelve countries[1] continuing to negotiate a high standard, 21st century Trans-Pacific Partnership (TPP) Agreement should seize the opportunity to address the growing threat of trade secrets theft in the Asia Pacific region. Current laws protecting trade secrets and/or efforts to enforce them in many TPP countries remain relatively weak. Securing advances in trade secret protection and enforcement among the TPP parties would not only promote innovation, investment and economic growth in the region, but would also set an important model for future trade agreements, both for TPP countries and otherwise.

Specifically and ideally, national laws and policies within TPP countries would

[1] Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, the United States, and Vietnam.

(i) expressly recognize the IP nature of trade secrets, and their critical importance to economic growth, development, and investment;

(ii) provide strong, statutory and cost-efficient protection of trade secrets for all its members, including both criminal and civil protection; and

(iii) commit the parties to work closely together to combat all forms of trade secret misappropriation, espionage, and theft by sharing information and trade secret theft reporting and intelligence among TPP parties.

We recognize, however, that TPP negotiations are far along and that in some countries, cyber theft and other forms of trade secret misappropriation have only recently become a serious issue. Accordingly, at a minimum, TPP countries should include firm commitments to provide robust trade secret protection, with criminal penalties designed to sufficiently deter a growing problem. The value of trade secrets to national economies, businesses and innovation is too great to be ignored in these negotiations.

OVERVIEW

This policy paper presents the case for why enhanced legal protections for trade secrets, including criminalization of willful misappropriation and unauthorized disclosure of trade secrets, should be elevated on the TPP agenda. Although the legal definition of a trade secret varies from jurisdiction to jurisdiction, broadly speaking, trade secrets may be thought of as commercially valuable confidential information whose value derives from not being generally known and which is subject to reasonable efforts to maintain its confidentiality. As a result, any disclosure, however temporary and to whichever party, carries substantial risk to the actual or potential commercial and economic value of the trade secret and may, in fact, devalue it altogether. This is particularly true in the case of trade secrets related to production processes, business, or marketing strategies and other forms of trade secrets not physically represented in the end-product.

Generally speaking, trade secret theft can be broken down into three categories: (1) ordinary theft by an individual, (2) corporate espionage, and (3) state-sponsored espionage. The remedies discussed in this paper are intended to cover all three of these categories.

STRONG PROTECTION FOR TRADE SECRETS FOSTERS INVESTMENT AND INNOVATION

It is well established that robust protection for intellectual property rights benefits countries' economic performance. As explained below, trade secrets are a significant category of intellectual property, and strong trade secret protection benefits economies in a number of critical and documented ways. Strong trade secret protection—coupled with effective and credible enforcement—affects firms' investment decisions in ways that benefit a country's economy as a whole. Such protection has also been shown to spur the development of particular sectors and industries that depend on trade secrets, including in TPP member countries. Finally, trade secret protection benefits individual enterprises, including small businesses, allowing for more efficient hiring, investment, and deployment of resources.

The Economic Benefits of Strong Intellectual Property Protection

Studies assessing the effect of patent, trade secret, copyright, trademark, and other intellectual property protections have documented the impact of such policies on foreign direct investment and voluntary technology transfer. The World Bank reported, for example, that "since 1980, the world's greatest economic gains have been achieved by developing nations that aggressively opened their economies to foreign technologies and business methods and *protected the intellectual property rights of their developers*."[2]

This effect is particularly salient in industries that rely on complex technology, and in sectors at a high level of the value chain, including manufacturing and R&D. In each of these areas, strong trade secret protection is critical for companies to actualize the value of their

[2] Robert J. Shapiro and Kevin A. Hassett, "The Economic Value of Intellectual Property," at 5 (2005) (citing World Bank, *World Development Indicators*, Washington, DC: World Bank, 2005).

investment, stimulate further investment, and spur further innovation. A pioneering study surveyed 100 U.S. firms regarding their view of the strength of intellectual property protections available in fourteen countries, including Chile, Indonesia, Mexico, and Singapore. Using data on U.S. investment in these countries, it found the strength of a country's intellectual property protection, as measured by these perceptions, to be positively correlated with the volume of foreign direct investment (FDI) flowing into that country from the United States.[3]

The strength of intellectual property protection also influences the kinds of technology that firms are willing to transfer to a country, and such protections become more important the higher one moves up the value chain. Another survey of businesses showed that intellectual property protection was of importance to only 20 percent of firms investing in sales or distribution outlets, but that it mattered to 50-60 percent of firms investing in manufacturing of components or complete products, and to 80 percent of firms investing in R&D facilities.[4]

Other research confirms the trend. A 2010 Organization for Economic Cooperation and Development (OECD) study established that increases in the strength of intellectual property protection were associated with increases in FDI inflows, service imports, and domestic R&D.[5] Firm-level data from Eastern Europe and the former Soviet Union, meanwhile, shows that relatively weak intellectual property rights in a potential host country deter investors from sectors that rely heavily on such protections, and dampen investment more generally. Weak intellectual property protection also discourages firms from investing in and undertaking local manufacturing, thus hampering job creation.[6]

The Key Role of Trade Secrets: Macro-Level Benefits

Trade secrets are a critical part of intellectual property protections. One often-cited index compiled to measure the strength of intellectual property protection in emerging markets located largely in Latin America, including Chile and Mexico, ranked trade secrets just below patents, and above copyright, trademark, and other protections in terms of their importance.[7] The strength of trade secret protection bears directly on investment decisions. For instance, weak protection for trade secrets, or unreliable enforcement of relevant laws, may prompt companies to make excessive investments in ensuring physical protection for their secrets, rather than in

---

[3] Jeong-Yeon Lee and Edwin Mansfield, "Intellectual Property Protection and U.S. Foreign Direct Investment," *Review of Economics and Statistics* 78, 181-86 (1996).

[4] Edwin Mansfield, "Intellectual Property Protection, Foreign Direct Investment, and Technology Transfer," World Bank Discussion Paper No. 19 (1994).

[5] Cavazos-Cepeda, R. et al., "Policy Complements to the Strengthening of IPRs in Developing Countries," OECD Trade Policy Working Papers, No. 104, OECD Publishing (2010).

[6] Beata Smarzynska Javorcik, *European Economic Review* 48, 39-62 (2004).

[7] Robert M. Sherwood, "Intellectual Property Systems and Investment Stimulation: the Rating of Systems in Eighteen Developing Countries," 37 *IDEA* 261, 265 (1996).

innovation.[8] Or it may limit firms' investments altogether. As a survey respondent explained, his company made investments in a large developing country but had not "implemented manufacturing operations there that use our highest level of technology due to uncertainty over adequacy of trade secret protection."[9] Empirical work bears out these insights. One such study examined the relationship between the historical development of trade secret protection in the United States and concurrent levels of R&D investment.[10] It found more stringent trade secret protection to be positively correlated with increased R&D investment in high-tech and other R&D-intensive industries.[11]

Robust trade secret laws, however, must be complemented by equally strong enforcement. Multiple studies have shown a clear, positive relationship between the degree of IP *enforcement* in developing countries and FDI flowing into those countries.[12] An OECD study analyzed this relationship using an index of "legal effectiveness," which assigned countries "a composite score of judicial independence, impartial courts, security of property rights, and integrity of the legal system."[13] This study concluded that IP protection has the greatest influence on FDI when complemented by an effective legal system.[14]

Robert Sherwood's comparative work on the trade secret protection systems of Brazil and the United States further illustrates this relationship.[15] Sherwood determined that trade secret protection was vital for ensuring the commercial success of new innovations.[16] Ultimately, Sherwood concluded that economic development in Brazil has been hampered by weak trade secret protection and ineffective enforcement relative to the United States. Even though Brazil "does good science," Sherwood argues, an inefficient judiciary and weak enforcement of trade secret laws undermine the potential economic benefits of that science.[17] As a result, Brazilian

---

[8] *See* Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 Stanford L. Rev. 311, 332-37 (2008).

[9] Mansfield, *supra* note 4, at 27.

[10] Png, Ivan P. L., "Law and Innovation: Evidence from State Trade Secrets Laws" (June 15, 2012), *available at* SSRN: http://ssrn.com/abstract=1755284 or http://dx.doi.org/10.2139/ssrn.1755284

[11] *Id.*

[12] Cavazos-Cepeda, et al., *supra* note 5; L. Branstetter and K. Saggi, "Intellectual Property Rights, Foreign Direct Investment, and Industrial Development," NBER Working Papers 15393, National Bureau of Economic Research (2009).

[13] Cavazos-Cepeda, *supra* note 5, at 12.

[14] *Id.*

[15] Robert M. Sherwood, *Trade Secret Protection: Help for a Treacherous Journey*, 48 WASHBURN L.J. 67, 105 (2009). Sherwood chooses these two countries for comparison due to similarities in length of active history, early economic importance of agriculture, and population size.

[16] *Id.* at 83.

[17] *Id.* at 105.

businesses "cannot rely on the judicial system to adequately support the law regarding trade secret protection."[18]

In his earlier work, Sherwood also found trade secret protection wanting in a number of other Latin American countries, including Mexico and Chile. In Chile, for instance, he noted that "[s]cattered statutory provisions provide only limited and largely ineffectual trade secret protection."[19] In Mexico, meanwhile, Sherwood observed that while laws criminalizing trade secret misappropriation existed, "fines and jail terms have been seldom used and therefore lack credibility."[20]

The Key Role of Trade Secrets: Benefits to Business

As the above studies show, the benefits of strong trade secret protection benefit entire economies. However, the positive effects of such laws are also felt at a micro or lower level, by particular sectors and industries. For instance, the World Intellectual Property Organization (WIPO) highlights several case studies of trade secret protection playing a key role in the development of particular industries in emerging markets.[21] Businesses in Singapore's food products industry have relied heavily on trade secret protection for know-how such as recipes and specialty coffees.[22] The rubber industry of Thailand, meanwhile, has used trade secret protection to safeguard know-how of the rubber recovery process. Due to the nature of the industry, the IP Management Group of Thailand's National Science and Technology Development Agency found trade secret protection to be "vital to the successful commercialization of the [rubber recovery] technology."[23]

Strong trade secret protection also promotes the growth of small businesses, which have been empirically shown to play a substantial role in innovation.[24] To protect their innovations, small businesses rely disproportionately on trade secrets, which are much less expensive to obtain, keep, and enforce than patents.[25] This is particularly true of innovative small businesses

---

[18] *Id.* at 75.

[19] Sherwood, *supra* note 7, at 300.

[20] *Id.* at 315

[21] *See, e.g.*, World Intellectual Property Association, "From a Lone Stall to International Success," *available at* http://www.wipo.int/ipadvantage/en/details.jsp?id=2573

[22] *Id.*

[23] World Intellectual Property Association, "Bridging the Gap from the Laboratory to the Market," *available at* http://www.wipo.int/ipadvantage/en/details.jsp?id=3246

[24] Small Bus. Admin., "The Small Business Economy, for Data Year 2006: A Report to the President" 1, 9 (2007), *available at* http://www.sba.gov/advo/research/sbecon2007.pdf

[25] David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L. J. 769, 786-87 (2009).

in high technology sectors. Survey evidence shows that such businesses show a marked preference for trade secrets over patents.[26]

While enforcement of trade secrets does involve litigation expenses, these expenses are significantly lower than the costs of patent litigation and this difference can affect how small businesses choose to protect their intellectual property. Data from high-stakes litigation in 2009 show that on average, patent litigation cost businesses 2.5 times as much as trade secret disputes.[27] More important, survey data has shown that small businesses are more threatened by trade secret misappropriation than large businesses.[28] Intellectual property litigator David Almeling has advanced two potential reasons for this finding. First, small businesses tend to be less stable and have higher rates of employee turnover,[29] and most cases of trade secret theft involve current or former employees. Additionally, small businesses have fewer assets that would allow them to withstand the loss of trade secret information.[30]

Finally, strong trade secret laws benefit not only individual enterprises, large and small, but their employees as well. Stanford Law School Professor Mark Lemley argues that trade secret laws act "as a substitute for the physical and contractual restrictions [that] companies would otherwise impose in an effort to prevent a competitor from acquiring their information."[31] With strong trade secret protection, employers can hire for skill rather than for loyalty, and assign employees where their talents would be most beneficial to the business rather than keeping them away from projects involving confidential information.[32] Similarly, strong trade secret protection allows businesses to undertake joint ventures or collaborations involving sensitive information—deals that may well constitute promising investments but would be viewed as too risky absent strong legal protections for the information involved. Employees, meanwhile, benefit from the greater freedom that comes with increased inter-company mobility.[33]

---

[26] Joseph J. Cordes et al., "A Survey of High Technology Firms," February 1999, *available at* http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.202.514&rep=rep1&type=pdf

[27] Am. Intell. Prop. Law Ass'n, Report of Economic Survey 29-30 (2009).

[28] *See* Steven Fink, *Sticky Fingers: Managing the Global Risk of Economic Espionage* 198 (2002) (finding that "small-sized to medium-sized businesses suffer the most significant losses").

[29] Almeling, *supra* note 25, at 788.

[30] *Id.*

[31] Lemley, *supra* note 8, at 335.

[32] *Id.* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 39 (2007).

[33] Almeling, *supra* note 25, at 786.

TRADE SECRETS HOLD IMMENSE VALUE BUT REMAIN HIGHLY VULNERABLE

Studies at the enterprise level confirm the great value of trade secrets to businesses. A 2010 study by Forrester Consulting surveyed Australian, European, and U.S. companies regarding their data security practices. The study found that trade secrets comprise an average of two-thirds of the value of firms' information portfolios. In knowledge-intensive industries like manufacturing, information services, and professional, scientific, and technical services, that percentage increases to some 70 to 80%.[34] In the aggregate, this value is immense. Publicly traded U.S. companies own an estimated $5 trillion worth of trade secrets.[35]

Survey evidence also consistently shows that many businesses view trade secret protection as more critical than any other form of intellectual property protection—including patents. A survey of 650 managers in the U.S. manufacturing sector, for instance, discovered that trade secrecy was largely viewed as more effective than patents for protection of process innovations.[36] Another survey of nearly 1,500 R&D labs in the United States asked what measures each firm takes to capture the gains from their investments in innovation. The authors learned that firms placed the greatest emphasis on secrecy and lead time and, for the most part, far less emphasis on patent protection.[37]

In 2008, the National Science Foundation conducted a survey asking United States businesses to report on the importance of various forms of intellectual property protection to their companies.[38] As summarized in the below table, companies with significant R&D activity reported trade secrets to be the most important form of intellectual property protection.[39]

Table 1. Importance of Various Forms of IP Protection to U.S. Businesses with R&D Activity

	Very	**Somewhat**	**Not**
Trade secrets	45%	22%	33%
Trademarks	33%	27%	40%
Utility patents	26%	15%	60%

[34] Forrester Consulting, "The Value of Corporate Secrets" at 4-5, *available at* http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf

[35] Elizabeth A. Rowe, "Contributory Negligence, Technology, and Trade Secrets," 17 *George Mason L. Rev.* 1, 5 (2009).

[36] Richard C. Levin et al., "Appropriating the Returns from Industrial Research and Development," *Brookings Papers on Economic Activity*, Vol. 1987, No. 3, pp. 783-831 (1987).

[37] Wesley M. Cohen et al., "Protecting their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)," NBER Working Paper No. 7552 (2000).

[38] National Science Foundation, "Business Use of Intellectual Property Protection Documented in NSF Survey" (2012), *available at* http://www.nsf.gov/statistics/infbrief/nsf12307/. This survey specifically sought responses regarding utility patents, design patents, trademarks, copyrights, trade secrets, and mask works.

[39] *Id.*

	Very	Somewhat	Not
Design patents	15%	18%	67%
Copyrights	25%	25%	49%
Mask works	4%	6%	90%

Source: National Science Foundation

Even among companies without R&D activity, trade secrets ranked as the second most important form of intellectual property protection, only slightly behind trademarks and ahead of copyrights and patents.[40]

Results from other parts of the world are largely consistent. One survey of Swiss R&D executives concluded that secrecy was considered a particularly effective protection mechanism in the electronics, chemicals, food, synthetics, and paper sectors.[41] A broader survey of European firms also found that a high percentage of firms rated secrecy as a more valuable form of protection for R&D investments than patents.[42]

The value of trade secrets is matched only by their vulnerability. Lackluster legal protection for these assets gives businesses significant cause for concern. Government and private-sector data alike show the extent of the threat. U.S. litigation statistics, for instance, show a sharp increase in cases of trade secret theft: the number of such cases doubled between 1988 and 1995, doubled again between 1995 to 2004, and is expected to double yet again by 2017.[43]

Similarly, a McAfee survey of more than 1,000 senior IT executives from companies in Brazil, China, Japan, the Middle East, the United Kingdom, and the U.S. determined that companies lost an average of $4.6 million worth of intellectual property in 2008 due to security breaches.[44] While this survey provides a snapshot of 2008, there is no reason to believe that the losses in other years are less—indeed, as shown above, with ever-increasing threats, it seems clear that these average intellectual property losses are also on the rise. Because unauthorized disclosure, such as one stemming from a security breach, does not negate the potential to seek enforcement of other forms of intellectual property protection that may cover the disclosed material, such as patents and copyrights, it would appear that the estimated losses from the McAfee survey primarily involve trade secrets.

---

[40] *Id.*

[41] Najib Harabi, "Appropriability of Technical Innovations: An Empirical Analysis," *Research Policy*, Vol. 24, No. 6, (1995) pp. 981-992.

[42] Anthony Arundel, "The Relative Effectiveness of Patents and Secrecy for Appropriation," *Research Policy*, Vol. 30, No. 4, (2001) pp. 611-624.

[43] Almeling, *supra* note 25, at 292.

[44] McAfee, "Unsecured Economies: Protecting Vital Information" at 7 (2009), *available at* http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

Significant numbers of businesses are at risk. In 2007, Japan's Ministry of Economy, Trade, and Industry surveyed 625 manufacturing firms and learned that more than 35% had suffered from some form of technology loss. The Canadian Government discovered in 2010 that this was true of 86% of Canada's large corporations, and that the rate of cyber espionage in the private sector had doubled since 2008. This trend appears consistent across economies with extensive high-tech sectors: South Korea reported in 2008 that its firms had lost $82 billion due to foreign economic espionage; that number is up from $26 billion in 2004.[45] Likewise, the United Kingdom estimates that theft of trade secrets accounts for over 40% of the $34 billion annual cost of industrial espionage to its private sector.[46]

In February 2013, the White House unveiled its "Strategy on Mitigating the Theft of U.S. Trade Secrets." The Strategy noted that there are "multiple vectors of attack" for governments and persons to steal trade secrets.[47] Likewise, the U.S. Department of Defense has said that U.S. businesses, universities, and governments annually lose "an amount of intellectual property larger than that contained in the Library of Congress" (whose collections include more than 34.5 million catalogued books) as a result of cyber espionage. Legislation in the U.S. Senate last year ascribed the value of the intellectual property stolen from American businesses at over $1 trillion.

Along similar lines, another McAfee study recently established the annual economic losses resulting from cybercrime alone to be $24 to $120 billion in the United States, and between $300 billion and $1 trillion globally.[48] The latter figure represents 0.4 to 1.4% of global GDP. The study describes the theft of intellectual property and confidential business information as the most important area of such losses. It stresses that such losses may be particularly difficult to calculate and prone to underestimation, because of the potentially long-lasting effects of unfair competition resulting from the theft of trade secrets. Moreover, the estimates of losses do not include the increased cost of security that the proliferation of such theft necessitates.[49] This would be of particular concern where businesses cannot rely on the law to deter and punish breaches effectively.

The McAfee study also captures the broad range of industries and technologies vulnerable to trade secret theft. These include not only know-how in "strategic industries" but

---

[45] "Administration Strategy on Mitigating the Theft of U.S. Trade Secrets," *available at* http://www.whitehouse.gov//sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf

[46] *Id.*

[47] "Administration Strategy," *supra* note 45, at 1.

[48] McAfee, "The Economic Impact of Cybercrime and Cyber Espionage," July 2013, *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

[49] *Id.* at 12.

information as varied as "breakfast cereal recipes, running shoe designs, automobile part technologies, and soft drink formulas."[50]

Even with the increasing risk of misappropriation from afar through cybercrimes, the greatest threat to a company's trade secrets may still be its own employees. In over 85% of federal trade secret cases in the United States, the alleged misappropriator worked for or with the trade secret owner, either as an employee or a business partner.[51] Statistics from the Economic Espionage Act ("EEA") database also indicate that 76% of the defendants in EEA cases were current or previous employees of the company bringing claims of misappropriation.[52]

Greater job mobility increases that risk, creating more opportunities for employees to use a previous employer's trade secrets in subsequent employment--whether accidentally or intentionally. As employee mobility continues to rise, companies will face greater challenges protecting their trade secrets. The increasingly mobile employee base is a global trend, affecting developed and developing countries alike. Many developing countries in Asia have very high employee turnover rates.[53] For example, Malaysia's annual employee turnover rate has in past years reached over 12%.[54] One study reasons that rapid economic growth in these developing countries is fueling the rise in employee mobility.[55] While such growth is, of course, highly desirable, strong measures are needed to counter the attendant rise in trade secret misappropriation due to that mobility.

RECENT CASES OF TRADE SECRET THEFT HIGHLIGHT THE NEED FOR STRONG AND CREDIBLE DETERRENTS

Recent cases of trade secret theft show significant activity in the Asia Pacific region. These cases tend to involve theft by current or former employees, and highlight the overwhelming need for a strong deterrent, including the credible threat of criminal liability. While the civil damages awards in some of these cases may be significant, that is not true for others. Moreover, the continued increase in trade secret theft detailed above suggests that they may not suffice to curb the problem, and that a combination of robust civil enforcement as well as criminal penalties is important for protection of trade secrets.

---

[50] *Id.* at 10.

[51] Almeling, et al., *supra* note 3, at 294.

[52] Nicola C. Searle, "The Economics of Trade Secrets: Evidence from the Economic Espionage Act," University of St. Andrews 1, 84 (2010).

[53] Qin Yang and Crystal X. Jiang, "Location advantages and subsidiaries' R&D activities in emerging economies: Exploring the effect of employee mobility," *Asia Pacific J. Manage.* 24, 341-358 (2007). This study reports on employee mobility in the Philippines, Taiwan, China, Thailand, India, Singapore, and Malaysia.

[54] *Id.* at 345.

[55] *Id.* at 350.

Cases Showing Weak Remedies and Procedural Obstacles Undermine Civil Enforcement

An initial group of cases illustrates that limitations on the availability of damages, the difficulties of conclusively establishing such damages, as well as various procedural obstacles, such as the lack of adequate discovery mechanisms, can render civil trade secret protections alone an insufficient deterrent:

- **Australia:** In 2010, Australian catering company Spotless Group won its lawsuit against a former employee for misuse of confidential information but received less than 1/10th of the damages requested.

  From 2007 to 2009, Paul Reynolds was an employee of Spotless. While employed at Spotless, Mr. Reynolds began exploring other opportunities and began communications with Blanco Catering, a rival catering company. Mr. Reynolds acquired an interest in Blanco and began providing Blanco with detailed confidential information, including customer and supplier information, proprietary financial models, and sensitive financial data. In particular, while Spotless was in the process of bidding for a significant long-term catering contract to support conference facilities at the Adelaide Zoo, Mr. Reynolds assisted Blanco in bidding for the same project. Blanco's final rental proposal was identical to Spotless's final rental proposal, and Blanco won the Zoo contract.

  The Federal Court of Australia held that Mr. Reynolds had breached the duties he owed to Spotless but found that Spotless had not proven that it would have won the Zoo contract if Mr. Reynolds had not misappropriated Spotless's confidential information. Accordingly, the Court found it difficult to determine the appropriate amount of damages to award Spotless. Spotless had sought over $1 million in damages for lost profits from the Zoo project. The Court awarded only $100,000 – an amount it conceded had no mathematical basis.[56] This case illustrates the difficulty in proving lost profits and recovering damages sufficient to deter misconduct even when there is a clear case of misappropriation of trade secrets, and helps underscore the need for potential criminal enforcement of trade secrets to complement civil enforcement. (As noted in the Appendix, Australian law currently does not include criminal penalties for trade secret theft.)

- **Canada:** In 2004, Canadian airline Air Canada sued WestJet, a smaller rival airline, for $220 million, alleging that WestJet stole confidential data on a massive scale from an internal Air Canada website.

  WestJet gained access to the internal Air Canada website through Jeffrey Lafond, a former Air Canada financial analyst who joined WestJet in 2003. Mr. Lafond had access to the password-protected website because his separation package from Air Canada gave him the right to book five free flights a year. This internal website allowed employees to check seat availability before booking personal flights. The website also contained load factor data for individual flights almost a year in advance. Load factor is the percentage

[56] *Spotless Group Ltd. v. Blanco Catering Pty Ltd.*, 93 I.P.R. 235 (FCA 2011).

of an airline's seats that are occupied. This data provides key insights into which Air Canada flights were popular and profitable.[57] Mr. Lafond requested and received legal indemnity for giving WestJet his password to this internal Air Canada website. WestJet used Mr. Lafond's password to access this website over 240,000 times between May 2003 and March 2004.[58] WestJet stopped gathering load factor data from this website only after Air Canada had discovered its actions.

After receiving a tip that WestJet had gained access to confidential Air Canada data, Air Canada hired private investigators who dressed as garbage collectors and took garbage left at the curb outside of the home of a WestJet executive. Shredded documents from the garbage were reconstructed, showing that the WestJet executive had regularly logged onto Air Canada's internal website and had created a software program to automate the collection of data.[59]

Air Canada filed suit against WestJet in April 2004, seeking $220 million in damages. Air Canada alleged that the confidential data on its internal website was used by WestJet to adjust its schedule, fares, and expansion strategy.[60] WestJet countersued, alleging that Air Canada unlawfully seized confidential financial information from the garbage of the WestJet executive.[61] Air Canada litigated its case for over two years, spending $5.5 million in investigation and legal fees, before the parties settled.[62]

As part of the settlement, WestJet donated $10 million to children's charities across Canada and paid Air Canada's investigation and legal fees. In addition, WestJet issued a press release admitting that it had "engaged in an extensive practice of covertly accessing a password-protected proprietary employee Web site maintained by Air Canada to download detailed and commercially sensitive information without authorization or consent from Air Canada."[63] WestJet further admitted that "[t]his practice was

---

[57] David L. Blenkhorn, "The Air Canada/WestJet Saga: Spy vs. Spy," 2007, http://www.wlu.ca/documents/22081/3_Air_Canada_WestJet_case.pdf.

[58] Katherine Macklem, "Spies in the Skies," Sept. 20, 2004, http://www.macleans.ca/business/companies/article.jsp?content=20040920_88645_88645.

[59] Ian Austen, "WestJet Settles Spy Case with Rival Air Canada," *The New York Times*, May 30, 2006, *available at* http://www.nytimes.com/2006/05/30/business/worldbusiness/30iht-canair.1846630.html?_r=0.

[60] *Id.*

[61] "WestJet Counter-Sues Air Canada," *CBC News*, June 30, 2004, http://www.cbc.ca/news/canada/story/2004/06/29/westjet040629.html.

[62] Blenkhorn, *supra* note 57.

[63] Joaquim P. Menezes, "WestJet Accepts Blame, Settles with Air Canada in Espionage Case," *IT World Canada*, May 28, 2006, http://www.itworldcanada.com/news/westjet-accepts-blame-settles-with-air-canada-in-espionage-case/99049.

undertaken with the knowledge and direction of the highest management levels of WestJet" and apologized to Air Canada for its misconduct.[64]

In cases like this, where the stolen trade secrets were used to make strategic decisions about pricing, what services or products to offer, and how to expand a business, the damage to the trade secret owner is often irreparable. It is not possible to "unring the bell" to make the competitor forget the confidential information it has learned and to prevent it from using what it has learned going forward. Moreover, it is extremely difficult for the trade secret owner to prove the amount of lost profits resulting from lost market share or price erosion, which can continue indefinitely into the future. In circumstances like these, criminal sanctions would be particularly helpful in deterring misconduct—especially in cases where the executives, who tend to set the ethical compass of their companies, are the ones who have misappropriated and misused proprietary information. Canadian law currently does not provide for such sanctions, as explained in the Appendix.

The fact that Mr. Lafond sought out legal indemnity from WestJet further illustrates the deterrent effect that criminal sanctions can provide. Mr. Lafond clearly recognized that his conduct was probably illegal. In this case, Mr. Lafond was able to take comfort in the fact that WestJet would pay any damages from a civil suit against him. If criminal liability were on the table, however, WestJet could not offer him such blanket protection, and he may have chosen not to disclose Air Canada's trade secrets as a result.

- **Japan:** In 2002, Japanese precision machine and mold manufacturer Dai-ichi Seiko K.K. won a landmark trade secret misappropriation case against a company formed by its former employees.

  Dai-ichi's semiconductor department designed, manufactured, and sold auto molding systems and molds for semiconductors' plastic encapsulation. In 1997, managers from Dai-ichi's semiconductor division left Dai-ichi and founded a new company, Asahi Engineering K. K. Asahi sought to create and sell the same type of products sold by Dai-ichi. Within six months, Asahi had hired over 70 employees from Dai-ichi.[65]

  After obtaining some evidence that Asahi had misappropriated its trade secrets, Dai-ichi sought pre-suit discovery in 1998. The Fukuoka District Court ordered Asahi to produce all documents showing the design of its products, but Asahi refused to produce any documents, claiming that they contained Asahi's trade secrets. Under Japan's Unfair Competition Prevention Law (UCPL), there is no general duty to produce documents containing trade secrets. The court may hold an in-camera hearing to view the disputed

[64] "Air Canada, WestJet Settle Spying Lawsuit," *CBC News*, May 30, 2006, http://www.cbc.ca/news/business/story/2006/05/29/westjet-aircansettle.html.

[65] Takamitsu Shigetomi, "Is Legal Protection of Trade Secrets in Japan Enough?" *Center for Advanced Study & Research on Intellectual Property Newsletter*, Winter 2003, *available at* http://www.law.washington.edu/casrip/Newsletter/2003/newsv10i1jp2.PDF.

documents to determine whether they truly contain the withholding party's trade secrets. In this case, however, the Fukuoka District Court chose not to hold an in-camera hearing, and pre-suit discovery proceedings ended without Asahi producing any documents.[66]

In 1999, Asahi filed a declaratory judgment action against Dai-ichi, and Dai-ichi counterclaimed, alleging misappropriation of trade secrets. Despite Asahi's withholding of documents during discovery, Dai-ichi was able to prove that Asahi's employees misappropriated Dai-ichi's trade secrets, including 90,000 drawings of auto molding systems and molds. The Court found that Asahi used Dai-ichi's drawings in designing its products, knowing that this information had been misappropriated by Dai-ichi's former employees.[67]

To prove damages, Dai-ichi provided evidence that its market share, which had been relatively constant for a number of years, dropped 5 to 6% after Asahi stole its trade secrets. The Court concluded that at least a portion of this loss in market share was attributable to Asahi's misappropriation of trade secrets and awarded Dai-ichi over 400 million yen (approximately 3.87 million USD). The Court also ordered an injunction and disposal of all drawings, auto molding systems, and molds based on misappropriated information.[68]

While Dai-ichi ultimately prevailed in its suit, the time and expense of proving its case and the amount of damages was multiplied by the difficulties it encountered in seeking discovery. At the time of this case, the UCPL had already provided Japanese courts with the ability to hold in-camera proceedings to review documents that allegedly contained trade secrets. However, such in-camera hearings only pertained to documents and had its limitations. For example, courts could not issue protective orders to prevent a party from disclosing trade secret information that it acquired in the course of litigation. In light of these limitations, courts may have been reluctant to order parties to produce documents that may contain trade secrets.

Recognizing the need for further protective measures to aid trade secret litigation, Japan amended the UCPL in 2005. The 2005 amendments gave Japanese courts the authority to "implement protective orders, closed hearings, and other procedural safeguards to protect trade secret information divulged in litigation." These new powers enable courts to require the production of information necessary to prove trade secret misappropriation while also protecting the disclosing party's trade secrets.[69]

---

[66] Dario A. Machleidt, "Japanese Trade Secret Protection: Litigations Can Feel Secure Bringing Misappropriation Claims in Japanese Courts," *Center for Advanced Study & Research on Intellectual Property Newsletter*, Winter/Spring 2008, *available at* http://www.law.washington.edu/Casrip/Newsletter/default.aspx?year=2008&article=newsv15i1TradeSecret.

[67] Shigetomi, *supra* note 65.

[68] *Id*.

[69] Machleidt, *supra* note 66.

In this case, Dai-ichi finally obtained civil remedies against Asahi five years after its trade secrets had been stolen. If there had been a prompt criminal investigation at the time Dai-ichi first learned of the trade secret misappropriation, much of the harm to Dai-ichi could have been reduced or prevented, and this case could have been concluded much earlier.[70]

- **Chile:** In 2008, American Express Bank sued Credit Suisse in U.S. federal court, alleging that an agent of Credit Suisse working with American Express employees had stolen trade secrets and proprietary customer information from American Express's Chile offices as part of a scheme to lure away customers. American Express alleged that a month after the scheme was launched, $127 million of its assets in Chile had been or were being transferred away, largely to Credit Suisse.[71] The parties stipulated to joint dismissal of the lawsuit shortly after filing, presumably having reached a settlement.[72] That American Express chose to bring this lawsuit in a U.S. court points up the deficiencies in Chile's own trade secret protections, as detailed in the Appendix.

- **South Korea:** In 2009, South Korea's GM Daewoo sued Russian automaker TagAZ after several former Daewoo employees handed over some 6,000 computer files containing car engine and component designs to the Russian firm. GM Daewoo sought an injunction to stop TagAZ from selling a sedan allegedly manufactured using the stolen information. According to GM Daewoo officials, it cost about 300 billion won (approximately $245 million USD) to develop the model for which information was stolen. The court granted Daewoo's request for an injunction banning TagAZ from using or disclosing the trade secrets, and from producing or selling the engines or components at issue.[73] While such injunctive relief does provide some assurance that the trade secret at issue will not be misused further, it does little, if anything, to deter future theft. This is particularly so where the theft involves the acts of individual employees, who may be compensated for their role well before the stolen information is exploited. The prospect of a future injunction, without more, would have little impact on such individuals' decision-making.

Cases Establishing Criminal Sanction Complement to Civil Enforcement

A second group of recent cases illustrates how the availability of strong criminal sanctions can both complement and fill gaps in existing civil remedies:

---

[70] Shigetomi, *supra* note 65.

[71] *Am. Express Bank, Ltd. v. Credit Suisse*, Case No. 1:08-cv-21391 (S.D. Fl. 2008), Complaint and Demand for Jury Trial, Dkt. No. 1, May 13, 2008.

[72] *Id.*, Dkt. No. 41, July 11, 2008.

[73] Jane Han, "GM Daewoo Takes Action Against TagAZ," *Korea Times*, Sept. 22, 2009, http://www.koreatimes.co.kr/www/news/biz/2009/09/123_52284.html; Peter Alpern, "Court Bans Russian Carmaker from 'Copying' GM Daewoo Models," *IndustryWeek*, Oct. 28, 2009, http://www.industryweek.com/regulations/court-bans-russian-carmaker-copying-gm-daewoo-models.

- **Taiwan:** In January 2013, Taiwan amended its Trade Secrets Act, increasing civil penalties and introducing criminal liability for trade secret theft. Under the amended Act, offenders face prison terms of up to 10 years for the theft and transfer of trade secrets to other countries as well as fines of up to NT $50 million (approximately $1.7 million USD). Moreover, where the offender's personal gain exceeds this maximum, courts can increase the fine up to 10 times the amount of the gain.[74] This move came in response to a number of high-profile cases of trade secret theft.

  In one such case, Taiwan Semiconductor Manufacturing Company (TSMC) sued mainland chipmaker Semiconductor Manufacturing International Corporation (SMIC) in a U.S. court for hiring away more than 100 of its employees and asking them to divulge TSMC's trade secrets. According to TSMC, these employees collectively had access to virtually all of TSMC's proprietary technology and business trade secrets.[75] In 2005, the parties reached an out-of-court settlement where SMIC agreed to pay TSMC $175 million USD and to refrain from using TSMC's trade secrets.[76] Just one year later, TSMC sued SMIC in a U.S. court again, alleging breach of the settlement agreement. In 2009, a jury found SMIC liable for both trade secret theft and breach of the prior agreement.[77] Shortly after this finding of liability, the parties settled the case, with SMIC paying TSMC a combination of cash, stock, and warrants having an estimated value of $290 million USD.[78]

  This increase in cross-border corporate espionage and trade secret theft is believed to have undermined Taiwanese companies' research and development and affected their international competitiveness.[79] The amendments to the Trade Secrets Act are intended to reverse these negative effects and to encourage international collaboration and foreign

---

[74] "Taiwan Gets Tough on Trade Secrets Act Violators," *Taiwan Today*, Jan. 14, 2013, *available at* http://taiwantoday.tw/ct.asp?xItem=200777&ctNode=421; U.S. Trade Representative, "2013 Special 301 Report" at 13, *available at* http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf.

[75] Marius Meland, "TSMC Refiles Trade-Secret Suit Vs. Mainland Foundry," July 28, 2004, http://www.law360.com/articles/1857/tsmc-refiles-trade-secret-suit-vs-mainland-foundry.

[76] Marius Meland, "Asian Chip Makers Settle Trade-Secrets, Patent Suit in $175M Deal," Jan. 31, 2005, http://www.law360.com/articles/2941/asian-chip-makers-settle-trade-secrets-patent-suit-in-175m-deal?article_related_content=1.

[77] Zusha Elinson, "TSMC-SMIC Trade Secret Case Settles for $200 Million," *LegalPad*, Nov. 9, 2009, *available at* http://legalpad.typepad.com/my_weblog/2009/11/tsmcsmic-trade-secret-case-settles-for-200-million.html.

[78] Dan Nystedt, "TSMC in US$290M Settlement with China's Biggest Chip Maker," *PCWorld*, Nov. 10, 2009, http://www.pcworld.com/article/181803/article.html.

[79] Amanda Y.S. Liu, "Trade Secret Act Amended," *Managing Intellectual Property*, Mar. 25, 2013, http://www.managingip.com/Article/3177326/Trade-Secret-Act-amended.html.

investment by deterring trade secret theft and making it easier to prove cases of trade secret misappropriation. [80]

Prior to the recent amendments, there was only civil liability for trade secret theft in Taiwan, and the damages awarded were often too low to deter the misconduct. For example, in a case where a former MediaTek employee disclosed trade secrets to a rival semiconductor company, he was fined only NT $270,000 (about $9,210 USD), less than 2% of the damages sought by MediaTek.[81] The increased penalties and imposition of criminal liability under the amended Act provide a much greater deterrent for potential offenders. In addition, the amendments seek to reduce the talent drain that has resulted from the poaching of Taiwan's human resources for the purpose of stealing trade secrets.[82]

The creation of criminal liability also helps to address one of the major difficulties in prosecuting a civil trade secret lawsuit in Taiwan—the absence of discovery procedures. As a civil law jurisdiction, Taiwan does not have any procedure for discovery, and as a result, companies have found it very difficult to prove their claims. Even when there is evidence that a former employee downloaded confidential information, it can be very difficult to prove that this information was used by a competitor without any discovery. The introduction of criminal liability means that companies may now seek assistance from the police in gathering evidence to prove their case.[83]

- **United States:** In 2012, federal prosecutors in the Eastern District of Virginia indicted South Korea-based Kolon Industries, Inc. and several of its executives for allegedly conspiring to steal trade secrets from American firm DuPont and Japanese firm Teijin. DuPont's Kevlar para-aramid fiber and Teijin's Twaron para-aramid fiber had been the only widely commercially available para-aramid fiber products for decades. Para-aramid fiber is used to make body armor, fiberoptic cables, and automotive and industrial products. Kolon sought to develop a para-aramid fiber to compete with Kevlar and Twaron. Between July 2002 and February 2009, Kolon hired current and former employees of the two firms to serve as "consultants" and asked them to reveal proprietary information, including details of the manufacturing process, customer and price lists, costs and profit margins, market trends, and business strategies. The indictment seeks a forfeiture of $225 million. In addition, if found guilty, Kolon executives face up to 30 years in prison for trade secret theft and obstruction of justice.[84]

---

[80] Ted Chen, "Tougher Trade Secrets Act Gets Through," *The China Post*, Jan. 12, 2013, *available at* http://www.chinapost.com.tw/taiwan/national/national-news/2013/01/12/367142/Tougher-Trade.htm.

[81] Peter Leung, "Taiwan Pushes to Improve Law on Trade Secrets," *Managing Intellectual Property*, May 30, 2012, http://www.managingip.com/Article/3038381/Taiwan-pushes-to-improve-law-on-trade-secrets.html.

[82] Chen, *supra* note 80.

[83] Leung, *supra* note 81.

[84] Indictment in Case No. 3-12-CR, Aug. 21, 2012, *available at* http://www.crowell.com/files/US-v-Kolon-Indictment.pdf; "Top Executives at Kolon Industries Indicted for Stealing DuPont's Kevlar Trade Secrets," U.S.

(continued…)

DuPont had also sued Kolon in a related civil case in 2009. Unlike in a criminal case, where prosecutors can get a search warrant to gather evidence, a plaintiff in a civil suit relies upon the defendant's compliance with its duty to preserve and produce relevant evidence. In this case, immediately after DuPont filed its complaint, key Kolon employees deleted a substantial number of emails in violation of the law.[85] Despite this loss of evidence, DuPont was able to prove its case against Kolon, winning a $920 million verdict and an injunction. However, this verdict is being appealed, and in the meantime, Kolon has been permitted to continue selling its para-aramid products.[86]

Cases Showing Growing Global Threat of Trade Secret Theft

Finally, a third set of cases from TPP members in the Asia Pacific region further illustrates the growing prevalence of trade secret theft throughout this part of the world:

- **Japan:** In 2012, Japanese-based Nippon Steel Corp. sued South Korean steelmaker Posco in both the United States and Japan for alleged theft of trade secrets related to electrical steel sheet technology. This technology is used in power plants' electric generators, hybrid cars, and vibration motors in mobile phones. In its damages demand, Nippon Steel alleges that the theft has cost it as much as $1.23 billion. The information was allegedly passed to Posco by a former Nippon Steel employee.[87] The case is still pending.

- **Singapore:** In 2010, Citigroup filed suit in the Singapore High Court, accusing its former Singapore-based director of sending confidential information to competitor Deutsche Bank before joining Deutsche Bank. Gautam Hazarika had worked for Citigroup for 15 years and had access to customer details, business strategies, and other confidential information. Citigroup alleged that Mr. Hazarika sent emails containing trade secrets to Deutsche Bank, Standard Chartered, and his personal account. This suit follows a number of similar cases in 2009, including Merrill Lynch suing Deutsche Bank for misappropriating trade secrets and the Royal Bank of Scotland Group firing its

---

Department of Justice, Oct. 18, 2012, http://www.fbi.gov/richmond/press-releases/2012/top-executives-at-kolon-industries-indicted-for-stealing-duponts-kevlar-trade-secrets.

[85] John Marsh, "DuPont v. Kolon Industries: Deletion of E-mails Leads to Sanctions and Spoliation of Evidence Instruction," *The Trade Secret Litigator*, July 25, 2011, http://hahnlaw.com/tradesecretlitigator/post/2011/07/25/DuPont-v-Kolon-Industries-Deletion-of-E-mails-leads-to-Sanctions-and-Spoliation-of-Evidence-Instruction.aspx.

[86] *E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc.*, No. 3:09-cv-00058 (E.D. Va.), Dkt. No. 1514 (Sept. 14, 2011); "Appeals Court Lifts Ban on Rival to DuPont's Kevlar," Sept. 24, 2012, Reuters, *available at* http://www.reuters.com/article/2012/09/24/dupont-kolon-courtorder-idUSL1E8KO9RQ20120924.

[87] Megan Leonhardt, "Nippon Says Posco Swiped Electrical Steel Secrets," Apr. 25, 2012, http://www.law360.com/articles/334251/nippon-says-posco-swiped-electrical-steel-secrets

Singapore-based chief currency trader for sending emails allegedly containing confidential data.[88]

- **Malaysia:** In 2012, Malaysian plastics company Plastech Industrial Systems sued former employees and a competitor company for unlawfully taking and using its proprietary information and breaching the duty of confidentiality. The former employees had held high management positions at Plastech and thus had full access to Plastech's technical specifications, pricing lists, costs, customer information, and status of on-going negotiations. While still employed at Plastech, they formed a company to compete with Plastech and used Plastech's trade secrets to gain customers and suppliers for this new company. Unlike Plastech, which invested in extensive research to develop its products, the new competing company engaged in no research and development and was only able to produce plastic products identical or similar to Plastech's products by using Plastech's trade secrets. The High Court ordered an injunction, return of all proprietary information and products produced using proprietary information, and an assessment of damages.[89]

CURRENT STATE OF TRADE SECRET PROTECTION VARIES WIDELY ACROSS TPP COUNTRIES, PARTICULARLY IN THE AVAILABILITY OF CRIMINAL SANCTIONS

At present, trade secret protection is far from uniform across the TPP countries, and there is significant room for improvement. TPP should include firm commitments towards strong, statutory and cost-efficient protection of trade secrets, including both criminal and civil protection. As an initial matter, robust enforcement of existing laws is critical. Enforcement can be a matter of capacity as well as political will. For instance, while the United States has had provisions criminalizing trade secret misappropriation since 1996, only within the last five years or so have robust enforcement efforts by federal prosecutors relying on these laws resulted in prosecutions for criminal trade secret theft. Similarly, according to one report, in Mexico, some 97% of cases of trade secret theft go unpunished, and only 56% of those cases that are brought to the attention of authorities result in some form of penalty.[90]

Yet enforcement alone is not going to be enough in light of the existing deficiencies and inconsistencies in applicable laws, and the continued global increase in trade secret theft. For instance, as set forth more fully in the Appendix, which summarizes legal protections for trade secrets throughout the TPP countries, many jurisdictions, including Australia, Brunei, Canada, Malaysia, New Zealand, and Singapore, base civil liability for trade secret misappropriation on common law alone. In each of these jurisdictions, the contours of the law and the available

---

[88] Andrea Tan, "Citigroup Says Ex-Employee Told Deutsche Bank Secrets," *Bloomberg*, May 2, 2010, http://www.bloomberg.com/news/2010-05-03/citigroup-sues-ex-singapore-director-for-giving-secrets-to-deutsche-bank.html.

[89] *Plastech Industrial Systems SDN BHD v. N&C Resources SDN BHD & ORS*, 2012 MLJU 605 (High Court 2012).

[90] Global Intellectual Property Center, "Measuring Momentum - The GIPC International IP Index" at 63, *available at* http://www.theglobalipcenter.com/measuring-momentum-the-gipc-international-ip-index/.

causes of action are different. Some countries, like Malaysia, Australia, and Singapore, allow actions only for breach of contract or breach of confidence; others, like Canada, make available additional legal theories, such as breach of fiduciary duty and unjust enrichment.

The most relevant source of deficiency and inconsistency relates to criminal penalties for misappropriation. Some TPP countries, such as Canada, Australia, Malaysia, and Singapore, have no laws criminalizing traditional trade secret disclosure or misappropriation. Many of these countries have criminal laws targeting computer-related crimes, which may sweep some forms of trade secret infringement into their purview but do not address trade secrets directly.[91] Among those countries that do criminalize trade secret misappropriation or disclosure, the penalties often vary from those that would not provide sufficient deterrent effect to those that would but only if applied consistently. For instance, Peru provides for potential imprisonment of no more than two years, while Mexico contemplates prison terms of two to six years.[92] In contrast, in the U.S., criminal penalties under the Economic Espionage Act range from up to 10 to 15 years.[93] Still others, such as Vietnam, have criminal provisions drafted in very general terms, lacking detail as to the nature of the prohibited offenses.[94]

The low criminal penalties or lack thereof in some TPP jurisdictions are particularly troublesome, as criminal penalties are believed to provide a greater deterrent to the would-be trade secret thief than the prospect of a civil penalty alone. For instance, deterrence was a stated purpose of the U.S. Congress in passing the Economic Espionage Act of 1996 ("EEA"). The House Judiciary Committee recognized that proprietary information was "a prime target for theft precisely because it costs so much to develop independently, because it is so valuable, and because there are virtually no penalties for its theft."[95] The Committee explained that enforcement by federal prosecutors, coupled with the criminal penalties in the new legislation, "will serve as a powerful deterrent" to such theft.[96]

---

[91] *See* Malaysia's Computer Crimes Act (1997), *available at* http://www.commonlii.org/my/legis/consol_act/cca1997185/; Singapore's Computer Misuse and Cybersecurity Act (2013), *available at* http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0.

[92] *Compare* Article 165 of the Peruvian Penal Code *with* Article 224 of Mexico's Industrial Property Law. These examples highlight two distinct problems: (1) that weak criminal penalties undermine the value of trade secrets, and (2) that there is significant variation in criminal penalties across jurisdictions.

[93] *See* 18 U.S.C. § 1831 et seq.

[94] *See* Article 212 of Vietnam's Intellectual Property Law (Law No. 50/2005/QH11), *available at* http://www.wipo.int/wipolex/en/text.jsp?file_id=274445. The McAfee study suggests that precisely drafted laws make for more effective enforcement, particularly in the area of cybersecurity and information crimes. *See* McAfee, *supra* note 44, at 17.

[95] House of Representatives Report 104-788, Sept. 16, 1996, at 5.

[96] *Id*. at 7. *See also* Joseph W. Cormier, Richard Kozell, and Jessica L. McCurdy, *Intellectual Property Crimes*, 46 Am. Crim. L. Rev. 761, 763 (2009) ("The marked increase in intellectual property theft, combined with the ineffective deterrence provided by civil remedies, has led the federal as well as state and local governments to enact criminal statutes to protect intellectual property."); Naomi Fine, *Positively Confidential*, Los Angeles: Reasonable

(continued…)

Finally, and often crucially, procedural inconsistencies and a lack of procedural coherence or mechanisms for procedural cooperation often make enforcement actions for cross-border trade secret infringements exceedingly expensive. Better information sharing between governments of (suspected) trade secrets violations or (repeat) perpetrators; further work to harmonize procedural pathways and provide for better, more efficient evidentiary provisions; and specific provisions aimed at protecting confidentiality of information during and after litigation or enforcement are key. Measures should also be adopted to ensure that governments properly justify any requests for proprietary information as a condition for market access or investment, that they implement strict procedures to protect such information, including sanctions against government officials and others involved for any disclosure of such information without the specific consent of the right holder.

CONCLUSION

The significant value and increasing vulnerability of trade secrets, coupled with demonstrated insufficient legal remedies to combat this growing threat in a number of jurisdictions, provide compelling reasons to secure more robust trade secret protections, particularly criminal penalties, in the TPP. As the examples cited in this report highlight, some countries have started to respond to the impact of trade secret theft on their businesses and economy by creating new or strengthening existing remedies to provide greater deterrence. Other countries' laws remain inadequate.

Even for countries where trade secret theft has not proven to be significant, the data shows that the threat is growing and that countries of all levels of development are affected. For emerging economies in particular, the evidence linking more robust IP systems to increased FDI, R&D and technology transfer demonstrate the importance of seeking improvements before misappropriation causes irreparable harm.

Seeking to create a high standard agreement, TPP countries have a unique opportunity to prevent harm to TPP economies and businesses by promoting more effective deterrence and enforcement of trade secrets theft. Such efforts will not only raise the bar for TPP countries but also serve as a model for the greater region and beyond.

Measures Publishing, 2011, at 299-300 (explaining the consequences of a guilty verdict under the EEA, and describing the goal of the criminal statute as deterrence of trade secret theft).

APPENDIX: EXISTING CIVIL AND CRIMINAL TRADE SECRET PROTECTIONS IN TPP MEMBER COUNTRIES

In order to provide a better understanding of the current state of trade secret protection, or lack thereof, in the various TPP countries, this Appendix outlines the general contours of both civil and criminal liability (to the extent any exists) for trade secret misappropriation and disclosure in each TPP country.

Australia

Civil Liability:

- Australia is a common law country. There is no codified system of law defining and protecting trade secrets.
- Many civil statutes refer to trade secrets or confidential information. For example, provisions in the Corporations Act of 2001 forbid the improper use of information acquired by officers or employees of corporations. However, most of the relevant law, including the determination of what constitutes a trade secret, is found in cases.
- Available causes of action include: breach of confidence and breach of contract.
- Because there is no over-arching statute defining and protecting trade secrets, whether disclosure of confidential information is prohibited depends on the circumstances and relationship of the parties involved. In some circumstances, information that is not a trade secret may be protected, while in other circumstances, disclosure of a trade secret is not prohibited.
- Civil remedies include: (1) an injunction, (2) delivery up and destruction of the fruits of the unlawful conduct, (3) compensatory damages, and (4) an accounting of profits.

Criminal Liability:

- There is no criminal law directly addressing trade secrets.
- Trade secrets are not recognized as property, which poses difficulties in prosecuting trade secret misappropriation under more general crimes, such as theft, fraud, or obtaining by deception. However, if a physical item storing the information, such as a document or computer disk, is stolen, trade secret theft could be prosecuted under these criminal provisions.
- Some forms of trade secret misappropriation may fall within the provisions of statutes criminalizing: (1) secretly listening to or recording telecommunications and divulging information obtained by such means, and (2) unauthorized access to computer programs or data.

Sources: Richard Gough, "Trade Secrets Throughout the World," §§ 2:1, 2:4-2:7, 2:13, 2:17-2:20 (2012); AIPPI, "Question 215: Protection of Trade Secrets Through IPR and Unfair Competition Law (Australia)," Mar. 31, 2010, available at https://www.aippi.org/download/commitees/215/GR215australia.pdf.

Brunei Darussalam

Civil Liability:

- Brunei is a common law country. There is no statutory protection for trade secrets. Trade secrets are protected under the common law.
- Under the Application of Laws Act of 1951, English common law and equity have the force of law in Brunei.
    - Available causes of action under English common law and equity include: breach of confidence, breach of contract, breach of the duty of good faith or fidelity, and breach of fiduciary duty.
    - Civil remedies under English common law and equity include: (1) an injunction, (2) delivery up of property or documents relating to the trade secret, and (3) compensatory damages.

Criminal Liability:

- There is no criminal law directly addressing trade secrets.
- Misappropriation of trade secrets would be difficult to prosecute under more general criminal provisions, which focus on physical property. For example, theft is defined as "to take dishonestly any movable property out of the possession of any person without that person's consent." Stealing trade secrets does not require taking property out of the possession of the trade secret owner.

Sources: Application of Laws Act (1951), Ch. 2, available at http://www.commonlii.org/bn/legis/aol2239/; Brunei Penal Code Ch. 22 § 378 (2001); Trade Policy Review: Brunei Darussalam, Secretariat Report, Jan. 21, 2008, WT/TPR/S/196/Rev.1, p. 64; "IPR Toolkit for Brunei Darussalam," http://brunei.usembassy.gov/uploads/images/FtR_7Z-Jl6W6pmLZkxPlrA/2006IPRTOOLKIT.pdf; "Chapter 2 – Sources of Law," at 4, Legal Systems in ASEAN – Brunei,http://www.aseanlawassociation.org/papers/Brunei_chp2.pdf; Simon Mehigan and Mary Yeadon, "Trade Secrets Throughout the World," §§ 39:1, 39:22-39:23, 39:33, 39:36, 39:37 (2012); Diana P.P. Cheong, "Administrative Accountability and the Law of Brunei Darussalam," Tinjauan, 2000/2001, at 5, available at http://www.csps.org.bn/documents/Administrative_Accountability_and_the_Law_in_Brunei_Darussalam.pdf.

Canada

Civil Liability:

- Canada is a common law country. There is no statutory protection for trade secrets, other than in Quebec, but there is a long history of case law defining and protecting trade secrets and confidential information. In Quebec, trade secrets are protected under the Civil Code of Quebec, but the basic legal principles under this statute are the same as the principles set forth in common law.
- Available causes of action include: breach of confidence, breach of contract, breach of fiduciary duty, and unjust enrichment.

- Civil remedies include: (1) an injunction, (2) compensatory damages, (3) punitive damages, (4) an accounting of profits, (5) imposition of a constructive trust over money and property obtained by the wrongful conduct, and (6) an inquiry to determine the market value of the confidential information in an exchange between a willing buyer and a willing seller.

Criminal Liability:

- There is no criminal law directly addressing trade secrets.
- Trade secrets are not generally recognized as property, which poses difficulties in prosecuting trade secret misappropriation under more general crimes, such as theft, fraud, or mischief.

Sources: R. v. Stewart, [1988] 1 S.C.R. 963; "Measuring Momentum," supra note 90, at 42; John T. Ramsay and Francois Grenier, "Trade Secrets Throughout the World," §§ 6:1-6:2, 6:8, 6:20, 6:41 (2012); AIPPI, "Question 215: Protection of Trade Secrets Through IPR and Unfair Competition Law (Canada)," Mar. 30, 2010, available at https://aippi.org/download/commitees/215/GR215canada.pdf; Abhinav Kumar, Pramit Mohanty, and Rashmi Nandakumar, "Legal Protection of Trade Secrets: Towards a Codified Regime," 11 J. Intell. Prop. L. 397, 401 (2006).

Chile

Civil Liability:

- Chile is a civil law country. Protection of intellectual property, including trade secrets, is guaranteed under article 19 of the Constitution.
- Industrial Property Law No. 19.039 imposes civil liability for the following acts provided these acts are committed with the intent to obtain a benefit or to injure the trade secret owner:
    - Unlawful acquisition of a trade secret
    - Unauthorized disclosure or use of a trade secret
    - Disclosure or use of a trade secret lawfully acquired under an obligation of confidentiality
- The Industrial Property Law has some significant deficiencies. For example, trade secrets that are part of the evidence in court cases are often disclosed to third parties without any penalty.
- Civil remedies include: (1) an injunction; (2) compensatory damages; (3) adoption of the measures necessary to avoid the continuation of the offense; and (4) publication of the decision.

Criminal Liability:

- The Chilean Criminal Code contains various provisions relating to the protection of trade secrets. For example, Article 284 of Title 7 of the Chilean Criminal Code provides criminal liability for wrongfully disclosing trade secrets of a current or former employer that is a manufacturing enterprise.

- Depending on the specific criminal provision that is violated, the penalty ranges from 60 days to five years imprisonment and may include a substantial fine.

Sources: Industrial Property Law No. 19.039 (2006), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=271237; "Measuring Momentum," supra note 90, at 46; Trade Policy Review: Chile, Secretariat Report, Oct. 9, 2009, WT/TPR/S/220, p.78; Pablo Ruiz-Tagle, "Trade Secrets Throughout the World," §§ 7:1-7:5, 7:10, 7:23-7:24 (2012); AIPPI, "Question 215: Protection of Trade Secrets Through IPR and Unfair Competition Law (Chile)," June 18, 2010, available at https://www.aippi.org/download/commitees/215/GR215chile_en.pdf.

Japan

Civil Liability:

- Japan is a civil law country. Article 2 of the Unfair Competition Prevention Law defines the following six acts of unfair competition relating to trade secrets:
    - Wrongful acquisition of a trade secret, or using or disclosing such a wrongfully acquired trade secret.
    - Acquisition of a trade secret with knowledge that it was wrongfully acquired, used, or disclosed (or with gross negligence).
    - Use or disclosure of a trade secret with knowledge that it was wrongfully acquired (or with gross negligence).
    - Using or disclosing a properly acquired trade secret for the purpose of acquiring an illicit gain or causing injury to the trade secret owner.
    - Acquiring a trade secret with knowledge that it was improperly disclosed (or with gross negligence), or using or disclosing a trade secret acquired with such knowledge (or gross negligence).
    - After properly acquiring a trade secret, using or disclosing it with the subsequently gained knowledge that it was improperly disclosed (or with gross negligence).
- Civil remedies include: (1) an injunction, (2) destruction of the infringing articles, and (3) compensatory damages.

Criminal Liability:

- Under Article 21 of the Unfair Competition Prevention Law, wrongful acquisition, use or disclosure of trade secrets is a punishable crime if the offender has the intent to acquire an illicit gain or to cause injury to the trade secret owner.
- The criminal penalty is up to ten years imprisonment with labor, a fine of up to ten million yen, or both.
- While there have only been a few cases in which formal action has been taken, and the defendant found guilty, these cases were widely publicized, such that they likely had a sufficient deterrent effect.

Sources: Kazuko Matsuo, "Trade Secrets Throughout the World," §§ 23:1, 23:6-23:7, 23:9-23:10 23:15-16, Appendix 23B (2012).

Malaysia

Civil Liability:

- Malaysia is a common law country. There is no statutory protection for trade secrets.
- Available causes of action include: breach of confidence and breach of contract under the Malaysian Contracts Act (in instances in which the alleged misappropriator has a contractual relationship with the aggrieved party).
- Civil remedies include: (1) an injunction, (2) delivery or destruction of documents or products incorporating the confidential information, and (3) damages.

Criminal Liability:

- There is no criminal law directly addressing trade secrets.
- Misappropriation of trade secrets would be difficult to prosecute under more general criminal provisions, which focus on tangible property. Trade secrets, being intangible, are not recognized as property.
- Some instances of trade secret theft could be prosecuted under the Computer Crimes Act, which criminalizes unauthorized access to computer programs or data. The penalty for such unauthorized access is up to five years imprisonment, a fine of up to 50,000 ringgit, or both.

Sources: Computer Crimes Act (1997), available at http://www.commonlii.org/my/legis/consol_act/cca1997185/; Sai Fong Wong and Indran Shanmuganathan, "Trade Secrets Throughout the World," §§ 25:1, 25:5, 25:10-13, 25:18, 25:23, 25:26 (2012).

Mexico

Civil Liability:

- Mexico is a civil law country. The Industrial Property Law imposes both civil and criminal liability for the following acts if committed for the purpose of gaining an economic benefit or harming the trade secret owner:
    - Unauthorized disclosure of a trade secret that is known by virtue of a position, knowing its confidentiality.
    - Unauthorized appropriation of a trade secret in order to use or disclose it.
    - Unauthorized use of a trade secret that is known by virtue of a position or due to disclosure by a third party, knowing that the third party disclosed the trade secret without authorization.
- The only civil remedy directly available for trade secrets is compensatory damages. Injunctive relief is not generally available. However, if the trade secret owner is able to: (1) prove an act of unfair competition, (2) demonstrate during an inspection the existence of a trade secret that is being used without consent, (3) establish the possibility of damage, and (4) place a bond, additional remedies are available. In practice, these additional remedies are extremely difficult to obtain.

Criminal Liability:

- The Industrial Property Law imposes both civil and criminal liability for unauthorized disclosure, misappropriation, or use of trade secrets for the purpose of obtaining an economic benefit or harming the trade secret owner.
    - The criminal penalty ranges from two to six years imprisonment and a fine of 100 to 10,000 times the minimum daily wage in Mexico City.
- The Federal Penal Code contains additional provisions that relate to the unauthorized disclosure of confidential information, with penalties including prison time, fines, disqualification from performing a profession, and community service.
    - For example, persons who disclose or use information obtained from a private communication face six to twelve years of imprisonment and a fine of 300 to 600 times the minimum daily wage in Mexico City.
- While laws exist on the books criminalizing trade secret theft, there are low rates of prosecution and sentencing. One report found that although one out of ten companies has suffered from industrial espionage, 97% of cases are unpunished. Moreover, of the cases that are brought to the attention of authorities, only 56% result in damages or fines. Better enforcement is necessary for these statutes to serve as a deterrent.

Sources: Industrial Property Law, Titles III, VII (2012), available at http://www.impi.gob.mx/wb/impi_en/industrial_property_law/_rid/134?idNoticia=10%uriWebPage=impi_en; "Measuring Momentum," supra note 90, at 25, 63; Hector Chagoya, "Trade Secrets Throughout the World," §§ 26:1-26:3, 26:11, 26:15, Appendix 26A (2012).

New Zealand

Civil Liability:

- New Zealand is a common law country. A number of civil statutes make passing reference to trade secrets or confidential information. However, there is no codified system of law defining and protecting trade secrets.
- Available causes of action include: breach of confidence, breach of contract, trespass, conversion, conspiracy, and interference with trade.
- Civil remedies include: (1) an injunction, and (2) compensatory damages.

Criminal Liability:

- The Crimes Act of 1961 (as amended by the Crimes Amendment Act of 2003) imposes criminal liability for unauthorized taking, obtaining, or copying any document, model, or other depiction of a thing or process containing or embodying a trade secret, knowing that it contains or embodies a trade secret.
- The criminal penalty is up to five years imprisonment.

Sources: Crimes Act of 1961 (as amended by the Crimes Amendment Act of 2003), Art. 230, available at http://www.legislation.govt.nz/act/public/2003/0039/latest/DLM200200.html; Paul Sumpter, "Trade Secrets Throughout the World," §§ 29:1-29:7, 29:12-29:13 (2012).

Peru

Civil Liability:

- Peru is a civil law country. The main statutory provisions governing trade secrets are Decision No. 486 (Common Provisions on Industrial Property) and Legislative Decree No. 1044 (Approving the Law on Suppression of Unfair Competition).
- Decision No. 486 prohibits the following acts of unfair competition:
    - Unauthorized use of a trade secret that was acquired under an obligation of confidentiality.
    - Unauthorized disclosure of a trade secret to gain an advantage or harm the trade secret owner.
    - Improper acquisition of a trade secret.
    - Use or disclosure of a trade secret that was improperly acquired.
    - Use of a trade secret obtained from another knowing (or where one should have the known) that the person was not authorized to disclose it.
    - Disclosure of a trade secret to gain an advantage or to harm the trade secret owner when the trade secret was obtained from another, knowing (or where one should have known) that the person was not authorized to disclose it.
- Legislative Decree No. 1044 prohibits:
    - Unauthorized disclosure or use of a trade secret that was either: (1) lawfully acquired with an obligation of confidentiality or (2) unlawfully acquired.
    - Acquisition of a trade secret through spying, instigating breach of an obligation of confidentiality, or other improper means.
- Before bringing an action in civil court based on unfair competition, one must first exhaust administrative proceedings before the National Institute for the Defense of Competition and the Protection of Intellectual Property ("INDECOPI").
    - The Commission for Supervision of Unfair Competition and Commissions of Regional Offices of INDECOPI ("the Commission") can impose the following administrative sanctions: (1) a fine of up to 700 UIT or 10% of the gross income of the infringer, (2) an injunction, (3) confiscation and destruction of products embodying the trade secret, (4) temporary closure of the infringing establishment, (5) preventing the import of products embodying the trade secret, and (6) publication of the conviction decision.
    - After a finding of unfair competition by the Commission, one can seek compensatory damages in court.

Criminal Liability:

- Article 165 of the Peruvian Penal Code imposes criminal liability for the unauthorized use, disclosure, or illicit communication of trade secrets if the offender is an employee, a public functionary in charge of guarding the secret, or a person having a commercial or contractual relationship with the trade secret owner. Otherwise, only civil sanctions are applicable.
- The criminal penalty is up to two years imprisonment and a fine of 60 to 120 times the average income of the offender.

Sources: Decision No. 486 of the Commission of the Cartagena Agreement, Common Provisions on Industrial Property, Title XVI, Ch. I (2000), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=223717; Legislative Decree No. 1044, Approving the Law on Suppression of Unfair Competition, Titles II, VI, VII (2008), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=203601; Rodrigo R. Bermeo, "Trade Secrets Throughout the World," §§ 30:1, 30:7, 30:10 (2012); AIPPI, "Question 215: Protection of Trade Secrets Through IPR and Unfair Competition Law (Peru)," Mar. 31, 2010, available at https://www.aippi.org/download/commitees/215/GR215peru/pdf.

Singapore

Civil Liability:

- Singapore is a common law country. There is no statutory protection for trade secrets.
- Available causes of action include: breach of confidence and breach of contract.
- Civil remedies include: (1) an injunction, (2) an accounting of profits, (3) compensatory damages, (4) delivery up or destruction of all materials and information relevant to the infringement of the trade secret, and (5) imposition of a constructive trust upon any benefits obtained from misuse of the trade secret.

Criminal Liability:

- There is no criminal law directly addressing trade secrets.
- Some instances of trade secret theft could be prosecuted under the Computer Misuse and Cybersecurity Act, which criminalizes unauthorized access to computer programs or data. The penalty for such unauthorized access that results in damage is up to seven years imprisonment, a fine of up to $50,000, or both.

Sources: Computer Misuse and Cybersecurity Act (2013), available at http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=DocId:8a3534de-991c-4e0e-88c5-4ffa712e72af%20%20Status:inforce%20Depth:0;rec=0; Gladys Mirandah and Gerald Samuel, "Trade Secrets Throughout the World," §§ 33:2, 33:5, 33:10-33:12, 33:21-33:22, 33:26, 33:29 (2012).

United States

Civil Liability:

- The United States is a common law country. Trade secrets are protected both under the common law and by statute. In both cases, civil trade secret law is based on state law, not federal law.
- Common law trade secret protection is based primarily on Chapter 4 of the Restatement (Third) of Unfair Competition.
    - Common law provides civil liability for the following acts:
        - Improper acquisition of a trade secret if one knows or has reason to know that it is a trade secret.

        - Unauthorized use or disclosure of a trade secret if one knows or has reason to know that it is a trade secret and that: (1) he acquired the trade secret under a duty of confidence; (2) he improperly acquired the trade secret; (3) he acquired the trade secret from someone who acquired it improperly or breached a duty of confidence in disclosing it; or (4) he acquired the trade secret through an accident or mistake, unless this was due to the trade secret owner's failure to take reasonable precautions to maintain the secrecy of the information.
    - Remedies include: (1) an injunction, (2) compensatory damages, and (3) an accounting of profits.
    - Breach of contract is another cause of action available for some instances of trade secret misappropriation.
- Statutory trade secret protection is based primarily on the Uniform Trade Secrets Act (UTSA).[97]
    - The UTSA provides civil liability for the follow acts:
        - Acquisition of a trade secret if one knows or has reason to know it was improperly acquired.
        - Unauthorized disclosure or use of a trade secret if:
            - It was improperly acquired;
            - One knew or had reason to know that: (1) he acquired the trade secret from someone who improperly acquired it; (2) he acquired the trade secret under a duty of confidence; or (3) he acquired the trade secret from someone who owed the trade secret owner a duty of confidence; or
            - One knew or had reason to know it was a trade secret and had been acquired by accident or mistake.
    - Remedies include: (1) an injunction, (2) compensatory damages, (3) an accounting of profits, (4) a reasonable royalty for the unauthorized disclosure or use of the trade secret, and (5) exemplary damages and attorney's fees in the case of willful and malicious misappropriation.

Criminal Liability:

- About half of the states have statutes criminalizing trade secret theft. These statutes require proving: (1) the act of theft, and (2) that the theft was intentional or that the trade secret was received or used with knowledge that it was stolen. Harm to the trade secret owner is not relevant.
    - Criminal penalties vary depending on the state. For example, in California, the penalty for stealing trade secrets is up to one year imprisonment, a fine of up to $5,000, or both. In Georgia, the penalty is one to five years imprisonment, a fine of up to $50,000, or both.
- The Economic Espionage Act makes theft or misappropriation of trade secrets under certain circumstances a federal crime.

[97] The UTSA is a model statute and is not, by itself, controlling law. However, 44 states and the District of Columbia have enacted statutes based on the UTSA.

- Under 18 U.S.C. § 1831, it is a punishable offense to steal, copy, communicate, receive, buy, or possess a trade secret, as well as to attempt or conspire to commit any of these acts, if done with the intent or knowledge that it will benefit a foreign-controlled entity or a foreign government or its representative.
    - The penalty is up to 15 years imprisonment, a fine of up to ten million dollars or three times the value of the trade secret,[98] or both. In addition, the offender shall: (1) forfeit any property derived from the crime and any property involved in commission of the crime, and (2) pay restitution to the trade secret owner.
- Under 18 U.S.C. § 1832, it is a punishable offense to steal, copy, communicate, receive, buy, or possess a trade secret relating to a product for interstate or foreign commerce, as well as to attempt or conspire to commit any of these acts if done for an economic benefit and with the intent or knowledge that it will injure the trade secret owner.
    - The penalty is up to 10 years imprisonment, a fine of up to five million dollars, or both. In addition, the offender shall: (1) forfeit any property derived from the crime and any property involved in commission of the crime, and (2) pay restitution to the trade secret owner.
- The Economic Espionage Act is not intended to criminalize every case of trade secret theft. Only cases involving very serious criminal activity will be prosecuted, with a focus on cases involving foreign companies or governments.

- Trade secrets are not recognized as property, which poses difficulties in prosecuting trade secret misappropriation under more general criminal provisions, such as the National Stolen Property Act. However, if a physical item storing the information, such as a document or computer disk, is stolen, trade secret theft could be prosecuted under these criminal provisions.

*Sources: Economic Espionage Act, 18 U.S.C. §§ 1831-1834, 1839 (2013); 18 U.S.C. § 2323 (2008); United States v. Agrawal, 2013 WL 3942204, at *13-15 (2d Cir. Aug. 1, 2013); United States v. Aleynikov, 676 F.3d 71, 72-79 (2d Cir. 2012); Cal. Penal Code § 499(c) (2011); O.C.G.A. § 16-8-13(b) (1995); Terence F. MacLaren, "Trade Secrets Throughout the World," §§ 40:1-40:6, 40:10-40:12, 40:16-40:17, 40:35-40:37, 40:41-40:42, Appendix 40A (2012).*

Vietnam

Civil Liability:

- Vietnam is a civil law country. The Intellectual Property Law imposes civil and criminal liability for the following:
    - Acquisition of a trade secret by taking acts against secret-keeping measures.

[98] The fine for individuals is up to five million dollars, while the fine for organizations is up to ten million dollars or three times the value of the stolen trade secret, whichever is greater.

    - Unauthorized disclosure or use of a trade secret.
    - Breaching a secret-keeping contract, using deception, bribery, or other improper means to acquire or disclose a trade secret.
    - Acquiring a trade secret from an applicant for a license by taking acts against an agency's secret-keeping measures.
    - Using or disclosing a trade secret knowing or having an obligation to know that it was improperly acquired.
    - Failing to perform secret-keeping obligations.
- Civil remedies include: (1) an injunction, (2) compelling public apology and rectification, (3) compelling the performance of civil obligations, (4) compensatory damages, and (5) destruction, distribution, or use for non-commercial purposes of the materials and means used for the production of infringing goods.

Criminal Liability:

- The Intellectual Property Law imposes civil and criminal liability for the unauthorized acquisition, disclosure, and use of trade secrets.
- Article 171 of the Vietnam Criminal Code provides criminal penalties for infringement of intellectual property rights. The penalty is re-education without detention for up to two years or a fine of DVN 20 million to 200 million. For especially serious cases, the penalty is six months to three years in prison.

Sources: Intellectual Property Law (Law No. 50/2005/QH11), available at http://www.wipo.int/wipolex/en/text.jsp?file_id=274445; Pham & Associates, "Vietnam Moves to Fill IP System Gaps," Mondaq, July 12, 2000, http://www.mondaq.com/x/8872/Vietnam+Moves+To+Fill+IP+System+Gaps.

U.S. CHAMBER OF COMMERCE

1615 H Street, NW | Washington, DC 20062-2000
www.uschamber.com