ECONOMIC ESPIONAGE AND TRADE SECRET THEFT:

AN OVERVIEW OF THE LEGAL LANDSCAPE AND POLICY RESPONSES

September 2013

KURT CALIA, COVINGTON & BURLING LLP

DAVID FAGAN, COVINGTON & BURLING LLP

JOHN VERONEAU, COVINGTON & BURLING LLP

GINA VETERE, COVINGTON & BURLING LLP

KRISTEN EICHENSEHR, COVINGTON & BURLING LLP

FRANK CILLUFFO, GW CYBERSECURITY INITIATIVE

CHRISTIAN BECKNER, GW CYBERSECURITY INITIATIVE

COVINGTON

COVINGTON & BURLING LLP

GW CYBERSECURITY INITIATIVE

INTRODUCTION AND EXECUTIVE SUMMARY

Concern about cyberespionage and intellectual property (IP) theft, particularly trade secrets, has intensified—and with good reason. While these threats are not new, rapid technological advances resulting in greater connectivity and data storage and more globalized supply chains have increased the opportunity—and potentially the payoff—to breach corporate networks and acquire sensitive corporate data. In short, the same technologies responsible for accelerating global growth are also being used to steal proprietary information and harm economies.

These threats strike directly at the core value of many businesses—and a core vulnerability. Trade secrets comprise an average of two-thirds of the value of firms' information portfolios, and that percentage rises to 70 to 80% for knowledge-intensive industries, such as manufacturing, information services, and professional, scientific, and technical services.[1] This value, however, can be tenuous; once a trade secret is made public or obtained by a competitor, its value may be substantially or entirely lost—a loss that may not be recoverable.

Indeed, the aggregate amount of intellectual property lost to cyberespionage each year is staggering. The U.S. Department of Defense has noted that "[e]very year, an amount of intellectual property larger than that contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government departments and agencies."[2] In a 2012 speech, General Keith Alexander, the head of the National Security Agency and U.S. Cyber Command, stated that IP theft due to cyber espionage is the "greatest transfer of wealth in history," and he estimated that U.S. companies lose $250 billion per year due to IP theft.[3] Put differently, the annual theft of intellectual property from U.S. businesses and other entities is "likely . . . comparable to the current level of U.S. exports to Asia—over $300 billion."[4] Of course, the problem is not just limited to cyberespionage; trade secret theft is growing in various forms. In the United States, federal cases of trade secret theft doubled between 1988 and 1995, doubled again between 1995 and 2004, and are projected to double again by 2017.[5]

This is hardly just a U.S. issue. Economic espionage and trade secret theft are carried out in countries around the globe and affect companies worldwide. Although data from Europe is inconsistent across jurisdictions, a significant increase in claims in the United Kingdom, for

---

[1] Forrester Consulting, The Value of Corporate Secrets, at 4-5 (Mar. 2010), available at http://www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20Secrets.pdf.

[2] Dep't of Defense, *Strategy for Operating in Cyberspace*, at 4 (July 2011), *available at* http://www.defense.gov/news/d20110714cyber.pdf.

[3] Josh Rogin, *NSA Chief: Cybercrime Constitutes the "Greatest Transfer of Wealth in History"*, The Cable, July 9, 2012, *available at* http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history.

[4] *The Report of the Commission on the Theft of American Intellectual Property*, at 2 (Feb. 2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf [hereinafter IP Comm'n Report].

[5] David S. Almeling, et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 293 (2010).

example, suggests that trade secret cases are also on the rise in Europe.[6] A recent survey conducted for the European Commission demonstrates the significant scope of this problem: over the past 10 years, approximately one in five respondents experienced at least one attempt or act of misappropriation within EU countries and nearly 40 percent of respondents believe that risk has increased during the same period.[7] Similarly, in a study by the Japanese government, more than 35 percent of respondent manufacturing firms reported some form of technology loss.[8] Meanwhile, South Korea estimates that costs from economic espionage more than tripled between 2004 and 2008.[9]

The number and nature of attacks is also troubling. The 2013 Verizon Data Breach Investigation Report tracked 621 confirmed data breaches in the preceding year, of which 92% were perpetrated by outsiders.[10] Nineteen percent of the breaches were attributed to state-affiliated actors,[11] and Chinese state-affiliated actors' "comprise about one-fifth of all breaches" and 96% of all espionage-related breaches.[12] State-sponsored espionage often involves use of "social tactics," such as spear phishing, and the percentage of breaches using "social tactics" was four times higher in 2012 than in 2011, composing 29% of all breaches in 2012.[13] In addition, 52% of breaches involved hacking, and 40% involved malware.[14] Another recent study estimated that the largest global organizations could face on average $35 million in losses over a two-year period from evolving attacks on cryptographic keys and digital certificates.[15] Although government and private sector capabilities to trace the origin of attacks are improving, attributing attacks to particular perpetrators and determining whether perpetrators are state-sponsored remain challenging as a technical matter.

---

[6] Robert Anderson & Sarah Turner, *Report on Trade Secrets for the European Commission* (Jan. 2012), 6, 41, *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/trade/201201-study_en.pdf [hereinafter 2012 EC Trade Secrets Study].

[7] European Commission, *Study on Trade Secrets and Confidential Business Information in the Internal Market* (April 2013), 13, *available at* http://ec.europa.eu/internal_market/iprenforcement/docs/20130711/final-study_en.pdf [hereinafter 2013 EC Trade Secrets Study].

[8] Office of the National Counterintelligence Executive, *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage*, 2009-2011, at B-1 (Oct. 2011) [hereinafter ONCIX Report].

[9] *Id.*

[10] Verizon, *2013 Data Breach Investigations Report*, at 4-5, *available at* http://www.verizonenterprise.com/DBIR/2013/.

[11] *Id.* at 5.

[12] *Id.* at 5, 21.

[13] *Id.* at 6.

[14] *Id.*

[15] Ponemon Institute and Venafi, *2013 Annual Cost of Failed Trust Report: Threats & Attacks,* at 4, *available at* http://www.venafi.com/wpcontent/uploads/2013/02/Ponemon_Cost_of_Failed_Trust_Report.pdf.

The accelerating rise of cyber theft of corporate data is receiving policymaker attention in the United States. In February 2013, the Obama Administration released a "Strategy to Mitigate the Theft of U.S. Trade Secrets,"[16] and the release of the Strategy followed the issuance earlier in the month of Executive Order 13636 on Improving Critical Infrastructure Cybersecurity.[17]

However, the threat to intellectual property borne from cyber-based attacks requires ongoing attention, and there is room for a greater connection between cybersecurity-related policy efforts and efforts to protect trade secrets. In fact, the Executive Order on Cybersecurity is focused principally on protecting critical infrastructure, not necessarily protecting intellectual property that may be held more broadly by U.S. businesses.

To assist in the public policy discussion, the authors from Covington & Burling LLP have partnered with the George Washington University Cybersecurity Initiative to produce this issue brief. The brief provides an overview of U.S. laws and policy reforms being considered in the European Union to prevent trade secret theft and economic espionage, reviews challenges in trade secrets enforcement in select markets overseas, and explores ways for the private sector and governments to improve trade secret protection and enforcement internationally. Specifically, as described further below:

- Trade secret protection in the United States is relatively more advanced than in most of the rest of the world. Both civil and criminal provisions address trade secret theft. On the civil side, many U.S. states have adopted the Uniform Trade Secrets Act. On the criminal side, the federal Economic Espionage Act of 1996 criminalizes misappropriation of trade secrets intended to benefit foreign governments or for economic gain. Cyber-based attacks on corporate networks may also implicate federal computer crime laws, including the Computer Fraud and Abuse Act and the Electronic Communications Privacy Act, as well as analogous state laws.
- At the national level, the European Union lags the United States in providing consistent and robust trade secret protection across its Member States. However, the EU is currently evaluating potential policy responses at the EU level to improve trade secret protection.
- Much of the rest of the world has very weak laws or enforcement practices, with the issue particularly acute in many of the largest emerging economies, such as China, Brazil, Russia, and India. Thus, as supply chains and operations expand globally, a company's ability to protect its trade secrets may be significantly diminished by weak rule of law and ineffective or non-existent enforcement in a number of countries.
- In light of these global challenges to protecting and enforcing trade secret protections, companies should be proactive in investing in trade secret protection; such expenditures should not be viewed as sunk costs, but rather important investments to preserve and enhance value.

---

[16] *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (Feb. 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf [hereinafter U.S. Administration Trade Secrets Strategy].

[17] Exec. Order No. 13,636, 78 Fed. Reg. 11,739 (Feb. 12, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

- In addition, trade policy tools should be utilized to elevate the importance of trade secrets protection, raise global standards, and promote more effective deterrence. In particular, U.S. negotiations on the Trans-Pacific Partnership ("TPP") Agreement with eleven other Asian-Pacific nations and the Trans-Atlantic Trade and Investment Partnership (T-TIP) with the European Union, along with negotiations toward a bilateral investment treaty with China, provide important opportunities to secure advances in protecting trade secrets. Trade secret protection should also be considered in other fora, including regional organizations and the World Trade Organization ("WTO") TRIPS Council. The U.S. should also consider using more enhanced enforcement tools, including through highlighting trade secret protection deficiencies of its trading partners in its annual Special 301 Report.
- The U.S. government should also improve internal coordination among agencies with responsibility for cybersecurity and the protection of trade secrets.

In sum, combating the growing threat of economic espionage and trade secret theft will require concerted efforts by companies to deter such threats and more robust policy responses and cooperation at the international level.

DISCUSSION: ADDRESSING ECONOMIC ESPIONAGE AND TRADE SECRET THEFT: THE LEGAL LANDSCAPE IN THE UNITED STATES AND EUROPEAN UNION

In the face of increasing threats of cyberespionage and theft of trade secrets, the United States is taking, and the European Union is actively considering, steps to update their respective laws, policies and practices. Below is an overview of the United States' trade secret protection and enforcement system, a summary of the inconsistencies of trade secret protection across EU Member States, and brief discussions of perceived deficiencies and efforts to address them in both systems.

TRADE SECRET PROTECTION IN THE UNITED STATES

General Information on U.S. Trade Secret Law

A trade secret is useful commercial information that gives a competitive advantage to its owner by being kept secret. Common examples of trade secrets include confidential formulae, customer lists, and manufacturing or other industrial techniques. Unlike patents and copyrights, which do not protect ideas, trade secrets also protect ideas, but only if their secrecy is preserved. Also unlike patents and copyrights, trade secret protection lasts as long as secrecy is maintained. For example, one of the world's most famous trade secrets—the formula for Coca-Cola®—is well over 100 years old.

An owner of a trade secret has rights only against those who (a) have agreed, either explicitly or implicitly, not to disclose the secret information, or (b) have obtained the secret information by misappropriation. Anyone else who has lawfully gained access to the information can benefit from using the trade secret information.

Beginning in the 1980s, states began to adopt the American Law Institute's Uniform Trade Secrets Act ("UTSA"). The UTSA largely codified common law but added a few features, including enhanced damages and discretionary attorneys' fees. Civil trade secret enforcement is a creature of state law, and thus to understand the applicable trade secret laws that will govern a particular actual or potential trade secret dispute, it is necessary to look to the law of the particular state in which the actual or potential dispute has arisen. However, because

most states model their individual trade secret laws from at least some portion of the UTSA, it is instructive to understand its basic provisions.

The UTSA defines a trade secret as information, including formula, pattern, compilation, program, device, method, technique, or process that: (1) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[18]

Civil Trade Secret Misappropriation

Misappropriation is the wrongful acquisition, disclosure or use of a trade secret. The UTSA defines it as (a) acquiring a trade secret through improper means or from another person knowing that the person acquired the secret by improper means, or (b) disclosing or using the secret without consent when the circumstances create a duty not to disclose or use it. Under the UTSA, such circumstances exist when the trade secret has been acquired:

- improperly;
- under an obligation not to disclose or use it;
- from someone who had an obligation not to disclose it; or
- by accident or mistake, for example, through misdirected email or facsimile transmission, if before using or disclosing the trade secret the person who acquired it learns that it is trade secret.

The two principal claims that are asserted in misappropriation civil cases are breach of contract and breach of confidence. Under the UTSA, a trade secret owner whose trade secret rights have been breached under an express contract also may, by reason of the contractually prohibited and hence unauthorized use and/or disclosure, have a claim for misappropriation.[19]

The UTSA imposes civil rather than criminal liability for misappropriation of trade secrets and creates a private cause of action for the victim. Remedies for misappropriation of trade secrets under the UTSA are injunctions including preliminary injunctive relief for both

---

[18] In instances in which there is some question as to whether the disputed subject matter is in fact a trade secret, in applying the UTSA, courts typically consider six factors: (1) the extent to which information is known outside a trade secret claimant's business and (2) by employees and others involved in the business, (3) secrecy measures, (4) the value of the information to the claimant and his competitors, (5) the effort or investment to develop the information, and (6) the ease or difficulty with which the information could be properly acquired or duplicated by others. (The fifth factor is infrequently applied.)

[19] In addition to UTSA-based trade secret misappropriation claims, plaintiffs often assert other tort claims, including conversion, restraint of trade and unfair competition. However, it is not uncommon for such claims to be preempted if these causes of action flow from a common set of operative facts as those that would support the trade secret claim. However, the UTSA does not preempt contract claims, irrespective of whether such claims are based upon common facts.

threatened and actual misappropriation,[20] damages (actual losses as well as unjust enrichment), including "exemplary" (punitive) damages, and, in cases of bad faith or willful and malicious misappropriation, reasonable attorney's fees.[21]

Criminal Trade Secret Statutes and Computer Crime Laws

a) Economic Espionage Act of 1996

The Economic Espionage Act of 1996 ("EEA")[22] is the federal law criminalizing misappropriation of trade secrets intended to benefit foreign governments or agents.[23] It also outlaws misappropriation of trade secrets for economic gain: "[w]hoever, with intent to convert a trade secret, that is related to a product or service used or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly" does one of three things—"(1) steals, or without authorization appropriates [or] takes . . . such information"; "(2) without authorization copies, . . . photographs, . . . replicates, . . . or conveys such information"; or "(3) receives, buys, or possesses such information, knowing the same to have been [misappropriated]," is subject to a fine or imprisonment.[24] Organizations are subject to fines not to exceed $10 million or three times the value of the misappropriated trade secret; fines for individuals cannot exceed $5 million.[25]

The EEA tracks the UTSA and defines "trade secret" as "all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, . . . methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing" if two conditions are met: first, "the owner thereof has taken reasonable measures to keep such information secret," and second, "the

---

[20] Injunctions will be discontinued once the disputed trade secret is no longer confidential, however, it is possible to extend injunctive relief for a reasonable period beyond that in order to eliminate the commercial advantage that would otherwise result from the misappropriation—i.e., the "head start" that the misappropriator would have gained over others who obtained lawful access, such as through reverse engineering.

[21] The UTSA also permits courts to grant protective orders to ensure the secrecy of trade secret during discovery and to prevent disclosure by witnesses. In addition, the UTSA authorizes in camera hearings to take testimony, although there is significant variation in the application of this principle across jurisdictions.

[22] 18 U.S.C. §§ 1831-39.

[23] *Id.* § 1831.

[24] 18 U.S.C. § 1832(a). Several courts have held that the Act does not create a private cause of action. *See, e.g.*, *Barnes v. J.C. Penney Co.*, No. 3-04-CV-577-N, 2004 U.S. Dist. LEXIS 17557 (N.D. Tex. 2004).

[25] 18 U.S.C. § 1832(a).

information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."[26]

One important potential difference between the criminal provisions of the EEA and civil liability under state law is the lawfulness of reverse-engineering. In civil cases under state law, reverse-engineering is generally lawful, but its legality under the Act is in question.[27]

Another important difference is that the EEA punishes attempt and conspiracy.[28] It has been held that "legal impossibility is not a defense to a charge of attempted misappropriation of trade secrets in violation of [the Act]," and that "the government need not prove that an actual trade secret was used"; "[t]he government can satisfy its burden under § 1832(a)(4) by proving beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such."[29] The same principle has been applied to conspiracy.[30]

b) Federal Computer Crime Laws

In addition to the EEA, cyber-based attacks against corporate networks also may implicate federal computer crime laws.

The Computer Fraud and Abuse Act ("CFAA") is the principal federal statute creating criminal and civil liability for unauthorized access to computers that are used in the United States in interstate commerce—which, as a practical matter, means any computing device connected to the Internet.[31] Among other acts, the CFAA prohibits:

- "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any" computer used in or affecting interstate commerce;[32]
- "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value";[33] and

---

[26] *Id.* § 1839(3). The Act does not define what it means for a trade secret to be "related to or included in a product that is produced for or placed in interstate or foreign commerce." *Id.* § 1832(a).

[27] *See* Samuelson & Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1576-77 & n. 6, 1582 (May 2002); *cf. United States v. Lange*, 312 F.3d 263 (7th Cir. 2002) (holding that defendant who sold reverse-engineered aircraft data sold trade secrets under the Act; not suggesting that reverse-engineering itself was improper).

[28] 18 U.S.C. § 1832(a).

[29] *United States v. Hsu*, 155 F.3d 189, 202-03 (3d Cir. 1998).

[30] *Id.* at 203. *Hsu* has been followed by other courts. *See, e.g.*, *United States v. Yang*, 281 F.3d 534, 544 (6th Cir. 2002).

[31] *See Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000) ("[T]he CFAA was intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature.")

[32] 18 U.S.C. § 1030(a)(2); *see also id.* § 1030(e)(2) (defining "protected computer" to include any computer "used in or affecting interstate or foreign commerce or communication").

- accessing a computer "without authorization," and causing damage.[34]

While the CFAA does not define "without authorization," it is generally understood the phrase pertains to outside intruders without any access rights, whereas "exceeds authorized access" pertains to unlawful access to a protected computer by an insider, such as an employee who steals trade secrets.[35] In either case, the CFAA has become a major legal weapon of the federal government in protecting computer systems and networks from hackers and thieves. The CFAA, as amended, provides sufficient breadth to capture most online criminal conduct. The challenge is that it often is difficult to establish the damages necessary to secure a felony violation.

Depending on the nature of the cyber intrusion, other federal laws that can be implicated in cyberespionage attacks include the federal Wiretap Act and the Stored Communications Act ("SCA"), which together comprise the Electronic Communications Privacy Act. Specifically, the Wiretap Act provides for possible criminal prosecution of anyone who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[36] The SCA governs unauthorized access to stored communications and makes it unlawful to: "(1) intentionally access[] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[] an authorization to access that facility; and thereby obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage in such system."[37]

c) State laws

There also can be state law analogs to these federal criminal laws. For example, the New York Penal Code contains an offense for "unlawful use of secret scientific material." A person is guilty of this offense "when, with intent to appropriate to himself or another the use of secret scientific material, and having no right to do so and no reasonable ground to believe that he has such right, he makes a tangible reproduction or representation of such secret scientific

---

[33] *Id*. § 1030(a)(4).

[34] *Id.* §§ 1030(a)(5)(B), (C) (prohibiting intentionally accessing a protected computer "without authorization" and recklessly causing damage or simply causing damage and loss).

[35] *See* U.S. Dep't of Justice, *Prosecuting Computer Crimes*, at 5-6, *available at* http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf (last visited Sept. 6, 2013) (citing S. Rep. No. 99-432, at 10 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479; S. Rep. No. 104-357, at 11 (1996)); *see also Diamond Power Int'l, Inc., v. Davidson*, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007) ("Under the more reasoned view, a violation for accessing a computer 'without authorization' occurs only where initial access is not permitted. And a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted."). *But see United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (finding access without authorization where graduate student with explicit authorization to use computers at Cornell propagated a virus that spread to other protected computers through "password guessing" and finding "holes" in programs, which used the computer systems not "in any way related to their intended function").

[36] 18 U.S.C. § 2511(1)(a).

[37] 18 U.S.C. § 2701(a).

material by means of writing, photographing, drawing, mechanically or electronically reproducing or recording such secret scientific material."[38] "Secret scientific material" is defined broadly to mean:

> a sample, culture, micro-organism, specimen, record, recording, document, drawing or any other article, material, device or substance which constitutes, represents, evidences, reflects, or records a scientific or technical process, invention or formula or any part or phase thereof, and which is not, and is not intended to be, available to anyone other than the person or persons rightfully in possession thereof or selected persons having access thereto with his or their consent, and when it accords or may accord such rightful possessors an advantage over competitors or other persons who do not have knowledge or the benefit thereof.[39]

New York state also has a section of its Penal Law—Article 156—that addresses various offenses involving access to or the misuse of computers. New York law criminalizes both the unauthorized use of a computer and trespass to a computer. An individual is guilty of "unauthorized use of a computer," which is a misdemeanor, when "he or she knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization."[40] A person is guilty of "computer trespass," a felony under New York law, when he or she "knowingly uses, causes to be used, or accesses a computer, computer service, or computer network without authorization and: (1) he or she does so with an intent to commit or attempt to commit or further the commission of any felony; or (2) he or she thereby knowingly gains access to computer material." [41]

Recent Developments in U.S. Trade Secrets Law

Both the U.S. Administration and Congress are rigorously exploring efforts to combat trade secret theft. Late last year, the U.S. Congress passed two pieces of legislation to address inadequacies in U.S. law. The first piece of legislation closed a loophole in the EEA by expanding coverage of the act to computer source code.[42] The second increased criminal penalties for economic espionage and directed the U.S. Sentencing Commission to also consider increasing offense levels for theft of trade secrets to reflect the significant economic harm caused to U.S. businesses.[43] Legislative proposals have also been offered both last year and earlier this year aimed at further enhancing deterrence, including by introducing a civil cause of action at the federal level.[44]

---

[38] N.Y. Penal Law § 165.07.

[39] *Id.* § 155.00(6).

[40] *Id.* § 156.05.

[41] *Id.* § 156.10.

[42] P.L. 112-236, The Theft of Trade Secrets Clarification Act (S. 3642).

[43] P.L. 112-269, Foreign and Economic Espionage Penalty Enhancement Act (H.R. 6029EH).

[44] *See* S. 3389, "Protecting American Trade Secrets and Innovation Act of 2012" (proposed to add a federal civil cause of action for trade secret misappropriation; no longer pending) and H.R. 2466, "A bill to amend Title 18, United States Code, to provide for strengthened protections against theft

As noted above, in February, the U.S. White House also released its Strategy on Mitigating the Theft of U.S. Trade Secrets. The Strategy recognizes that "the pace of economic espionage and trade secret theft against U.S. corporations is accelerating,"[45] and commits to several actions to address the threat. The action items include: engaging with trading partners to discourage IP theft, including by using trade policy tools; promoting cybersecurity best practices in the private sector; enhancing domestic investigation and prosecution of trade secret theft; strengthening U.S. laws against trade secret theft; and promoting public awareness and outreach efforts.[46]

TRADE SECRET PROTECTION IN THE EUROPEAN UNION

As in the United States, the European Union, which does not have a harmonized trade secret protection system, is actively evaluating the growing threat of trade secret theft and potential policy responses at the EU level.[47] A 2012 study surveying the level of trade secret protection across the 27 EU Member States highlighted that while every State offers some form of protection, the level of protection and effectiveness of that protection varies across Member States.[48] Overall, there are "disparities across the EU in what can be protected, in what circumstances and what the courts can or will do."[49] The report offers a number of suggestions for improving trade secret protection, including: providing consistency as to the types of information that can be protected; addressing difficulties in obtaining evidence of misuse and damage; making available effective preliminary and effective final injunctions; ensuring that courts have the means to protect secret information during proceedings; and the importance of providing for effective civil actions in addition to criminal remedies.[50]

---

of trade secrets, and for other purposes" (also proposed to add a federal civil cause of action for trade secret misappropriation; currently under consideration by various committees in the House of Representatives). In addition, late July saw the introduction of draft legislation by Senators Whitehouse (D-R.I.) and Graham (R–S.C.) to further enhance criminal trade secret laws.

[45] U.S. Administration Trade Secrets Strategy at 1.

[46] *Id.* at 3-12.

[47] *See* European Commission, Roadmap on the Protection of trade secrets/confidential business information from misappropriation and misuse by third parties (Oct. 2012), *available at* http://ec.europa.eu/governance/impact/planned_ia/docs/2013_markt_002_trade_secrets_en.pdf (noting that consistent with its Europe 2020 growth and jobs strategy, the European Commission is exploring policy options to improve trade secret protection at the EU level) [hereinafter EC Roadmap]. The Commission has recently commissioned two studies and held public consultations on trade secret protection.

[48] 2012 EC Trade Secrets Study, *supra* note 6 (emphasizing that "the absence or existence of specific legislation dealing with trade secrets is not necessarily an indication of whether effective action can be taken in a country. Common law countries, such as the UK and the Republic of Ireland, have effective trade secret protection despite having no specific trade secret legislation.").

[49] *Id.* at 44.

[50] *Id.* at 43-44.

A subsequent study prepared for the European Commission indicates that harmonization of trade secrets protection at the EU level is desirable and feasible. This study measured the perception and use of trade secrets, the level of protection and enforcement of trade secrets across Member States, and opinions regarding potential actions at the EU level to improve the protection of trade secrets.[51] Overall, the study found the current fragmented system in the EU has caused harm to innovation, cross-border investment, and growth in the EU.[52]

The vast majority of companies surveyed expressed a need for common legislation to ensure effective and equivalent protection against trade secret misappropriation. The study further noted that the current uncertainty arising from the patchwork of Member State laws has made some businesses reluctant to pursue legal action. Of the companies that reported misappropriation, less than half sought remedies in EU courts. Among the more commonly cited reasons for not doing so were the difficulty in meeting the legal requirements to prove a violation, lack of effective remedies and the inability to quantify damages.[53] Inadequate procedural measures to prevent disclosure of trade secrets in legal proceedings also serve as a barrier to effective enforcement.[54]

Additionally, the study highlighted the importance of criminal and civil remedies for trade secrets violations. For example, more than one third of respondents in the study recognized the strong deterrent effect and resulting benefits to businesses of criminal sanctions based on common rules and applied consistently across the EU.[55]

Another challenge to uniform deterrent-level enforcement in the EU is that many Member States do not recognize trade secrets as an intellectual property right. Such recognition is necessary in order to trigger application of the EU's IPR Enforcement Directive. Nevertheless, as noted in the 2013 study, even if Member States recognized trade secrets as an IP right, this would not automatically lead to the creation of a uniform enforcement system due to the different methods of implementation at the national level.[56]

As of this date, the European Commission has not yet indicated whether and what actions it will take to address trade secret misappropriation. Earlier statements indicate that options being considered are: a new EU Directive, regulation, or recommendation.[57]

---

[51] 2013 EC Trade Secrets Study, *supra* note 7. This study incorporated a survey covering 537 companies and provided a detailed review of the legal frameworks governing trade secrets in the then 27 Member States, the United States, Japan and Switzerland.

[52] *Id.* at 152.

[53] *Id.* at 151-52 (noting that "apart from the difficulty to quantify damages due to dishomogeneous criteria, damages awards possibly obtained following lengthy litigation can hardly represent an appropriate compensation for the loss of competitive advantage").

[54] *Id.* at 152.

[55] *Id*.

[56] *Id*. at 6.

[57] *See* EC Roadmap.

GLOBAL CHALLENGES FOR PROTECTIONS OF TRADE SECRETS AND ENFORCEMENT

As company operations and supply chains spread throughout the globe, efforts to protect their trade secrets are challenged—by weak rule of law and ineffective or non-existent enforcement in a number of countries. In one survey, global firms indicated that the threat to their digital assets was higher in China, Pakistan, Russia, and India than in the rest of the world. Among the factors cited by respondents as contributing to this high threat level were corruption among law enforcement and legal systems and inadequate intellectual property protections.[58] A 2012 Index benchmarking the intellectual property systems of eleven economically diverse countries supports this finding. In that report, China, India, and Russia all received the lowest score possible on trade secret protection due to inadequate legal frameworks and enforcement against trade secret theft.[59]

In China, for example, although several different laws (including its Anti-Unfair Competition and Criminal Laws) provide for some level of trade secret protection, in practice, the current legal system has not effectively protected trade secrets. According to a survey by the U.S. International Trade Commission (ITC), only 0.6 percent of U.S. firms that reported material losses due to trade secret theft between 2007 and 2009 in China pursued any trade secret misappropriation proceedings in China.[60] Among the challenges highlighted in enforcing trade secrets in China are: constraints on evidence-gathering for use in litigation, difficulties in meeting the criteria for establishing that information constitutes a trade secret, unclear criminal threshold requirements, significant prosecutorial delays, difficulties obtaining preliminary injunctions, and a lack of deterrent penalties.[61] As one study has noted, on average, only 30% of trade secret cases brought in Shanghai Higher People's Court reach conclusions and fewer than half of those result in findings of infringement.[62] However, under China's recently amended Civil Procedure Law, the Shanghai No. 1 People's Court issued the first preliminary injunction by a Chinese court in a trade secrets case,[63] representing a potential positive step forward toward improving trade secrets protection in China.

---

[58] McAfee, *Unsecured Economies: Protecting Vital Information*, at 12-16 (2009), *available at* http://resources.mcafee.com/content/NAUnsecuredEconomiesReport.

[59] Global Intellectual Property Center, *Measuring Momentum - The GIPC International IP Index,* 48, 54, and 65, *available at* http://www.theglobalipcenter.com/measuring-momentum-the-gipc-international-ip-index/ [hereinafter GIPC Index].

[60] U.S. Int'l Trade Comm'n. Pub. 4226, *China: Effects of Intellectual Property Infringement and Indigenous Innovation Policies on the U.S. Economy*, 3-44 (May 2001), *available at* http://www.usitc.gov/publications/332/pub4226.pdf.

[61] *See, e.g.*, Office of the United States Trade Representative, *2013 Special 301 Report*, 33 (May 1, 2013), *available at* http://www.ustr.gov/sites/default/files/05012013%202013%20Special%20301%20Report.pdf [hereinafter USTR Special 301 Report]; GIPC Index, *supra* note 59, at 50.

[62] GIPC Index, *supra* note 59, at 50.

[63] *Ex-employee banned from circulating trade secrets*, Shanghai Daily (Aug. 3, 2013), *available at* http://www.china.org.cn/china/2013-08/03/content_29613779.htm (quoting Judge Liu Junhua:

Studies also highlight ineffective trade secret protection and enforcement in a number of other countries. India's limited trade secret protections under common law and inefficient and backlogged judicial system, for example, are viewed as significant obstacles to effective trade secret enforcement.[64] Similarly, a comparative study highlighted Brazil's inefficient judiciary and weak enforcement of trade secret laws and noted the negative economic impact of such policies on the country.[65] And although Mexico provides for trade secret protection and criminal remedies in its laws, another study highlights that 97% of the industrial espionage cases go unpunished and of the cases that are brought to court only 56% result in damages or fines.[66]

In addition to the challenges posed by a country's inability or unwillingness to enforce its own trade secret laws, some foreign governments are pursuing policies that, inadvertently or not, result in the disclosure of trade secrets and other proprietary data. This is particularly of concern where foreign governments, often in furtherance of domestic innovation policies, require the transfer of technology to local partners as a condition for market access or investment.[67]

RECOMMENDATIONS: ENHANCING PRIVATE SECTOR INVESTMENT AND GLOBAL TRADE AND INVESTMENT MECHANISMS TO RESPOND TO THE GLOBAL THREAT

Given the transnational nature of economic espionage and trade secrets theft, a comprehensive approach must complement existing domestic legal reform efforts, such as those underway in the United States and the European Union, to combat these growing threats. Part of such a comprehensive approach should include investments and enhancements by the private sector in mitigating cyber-based threats to trade secrets. In addition, international trade and investment mechanisms should be used to raise the bar for robust trade secret protections as a means of deterring future theft and to strengthen the capacity and political will to enforce existing trade secret laws. The U.S. government should also improve internal coordination among agencies with responsibility for cybersecurity and the protection of trade secrets.

"The new Civil Procedure Law has filled a gap in protection of trade secrets, and the decision of the court will help the plaintiff hedge risks from secrets being leaked.").

[64] *See, e.g.*, GIPC Index, *supra* note 59, at 56; CREATE.org, *Trade Secret Theft: Managing the Growing Threat in Supply Chains*, 17, 19 (2012), *available at* http://www.create.org/news-resources/resources/trade-secret-theft-supply-chains#/-1/.

[65] Robert M. Sherwood, *Trade Secret Protection: Help for a Treacherous Journey*, 48 WASHBURN L.J. 67, 75 and 105 (2009).

[66] GIPC Index, *supra* note 59, at 63.

[67] The U.S. government, for example, has noted such concerns regarding Chinese government measures and policies that condition market access or investment in China on the transfer of intellectual property from foreign to domestic entities. *See* USTR Special 301 Report, *supra* note 61, at 32.

PRIVATE SECTOR INVESTMENT

The first line of defense against trade secret theft is a company's own protection program. Much like other forms of information security, a comprehensive program to protect trade secrets requires a combination of administrative, technical and physical protections. While certain protections are relatively low cost—in the form of strong policies, sensible protocols controlling information access and storage, training for employees, and compensation-related incentives for security-minded practices—others can require more significant investment, especially in the information technology space, or changes in existing business practices.

Companies often view such investments as too costly or burdensome. There can be significant budgetary pressure on IT departments, with the result that investment in security-related technologies is perceived as costly or unnecessary discretionary expenditures. Those technologies can include, for example, software for mapping and tracking data, software that can help identify security vulnerabilities or detect and manage potential data security breaches, enhanced network perimeter controls, and data loss prevention solutions. Other sound security protocols—such as restricting administrative privileges, limiting what devices can be taken on travel to certain countries, or limiting the use of portable media—also can meet resistance as inconveniences or face cultural challenges in adoption. Such perceptions, however, may reflect a misconception about the costs of such security technologies or protocols. Rather than viewing them as cost centers or burdens on a business, organizations may more appropriately view expenditures on strong security technologies and the adoption of strong security procedures as an investment in the future value of the business, much like investments in research and development. This is particularly true for a business for which much of its value and ability to compete resides in its trade secrets.

A 2012 study by the Ponemon Institute underscores the benefits of investing in security technologies and developing strong security posture, particularly in information-intensive businesses. The study found that companies "using security intelligence technologies were more efficient in detecting and containing cyber attacks," resulting in "an average [annual] cost savings of $1.6 million when compared to companies not deploying security intelligence technologies."[68] Substantial costs savings also were obtained from the use of data loss prevention tools, extensive deployment of encryption, and advanced perimeter controls.[69] Overall, companies that reported obtaining "sufficient budgeted resources" for security saved on average $2.2 million annually.[70] The study also found that the most significant cost from cyber crime for businesses was "information loss."[71]

Thus, companies that rely significantly on trade secrets for their business value would be wise to invest in leading-edge approaches to protecting that information. At the same time, the threat of cyberespionage and the loss of trade secrets is so significant that industry

---

[68] Ponemon Institute, *2012 Cost of Cyber Crime Study: United States*, at 4, *available at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf (Oct. 2012).

[69] *Id.* at 18.

[70] *Id.* at 19.

[71] *Id.* at 14.

cannot—and should not—be solely responsible for efforts to address the risks. Other mechanisms, including international trade tools, should be utilized.

INTERNATIONAL TRADE AND INVESTMENT MECHANISMS

There is no international treaty specifically governing economic espionage. International trade law, however, does provide a baseline for protection of trade secrets as an intellectual property right. Under the WTO's Agreement on Trade-Related Aspects of Intellectual Property Rights ("TRIPS Agreement"), WTO members are required to protect intellectual property rights, which include patents, copyrights, trademarks, and trade secrets. In particular, paragraph 2 of Article 39 requires WTO members to protect undisclosed information that is secret, is commercially valuable because it is secret, and has been subject to reasonable steps to be kept secret. The TRIPS Agreement also requires that members make available civil judicial procedures concerning the enforcement of any intellectual property right covered by the Agreement.[72] In addition, the Agreement allows "criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed willfully and on a commercial scale."[73]

While this framework provides for important minimum levels of protection of trade secrets, the TRIPS provisions related to trade secrets offer enough flexibility that implementation of these provisions has varied across jurisdictions.[74] The challenge, therefore, is how to enhance standards for protecting trade secrets. We believe that existing trade policy tools and laws are essential tools to be used to elevate global standards. In particular, trade negotiations and dialogues can offer effective means to elevating the importance of trade secrets protection, raising global standards, and promoting more effective deterrence. The key role of trade policy in combating cyber theft was highlighted in the U.S. Administration's Trade Secrets Strategy, which included plans for sustained and coordinated engagement with trading partners, the use of trade policy tools, and international diplomatic and law enforcement cooperation. [75]

The U.S. is currently negotiating two trade agreements—the Trans-Pacific Partnership Agreement ("TPP") with 11 other countries in the Asia-Pacific region and the Trans-Atlantic Trade and Investment Partnership ("T-TIP")[76] with the European Union—which both provide

---

[72] TRIPS, art. 42.

[73] *Id*., art. 61.

[74] *See, e.g.*, 2012 EC Trade Secrets Study, *supra* note 6, at 10. As the Study highlights, even across EU Member States, what is protected varies ("In common law countries the law of confidence potentially protects all types of confidential and secret information whether it is commercial, industrial or personal. In some other countries, for example, Belgium and France, there is specific statutory protection against disclosure by employees and former employees of manufacturing or process information but different protection for commercial information.") *Id.* at 2.

[75] U.S. Administration Trade Secrets Strategy, supra note 16, at 3-5.

[76] In light of current U.S. and EU efforts to enhance their own respective trade secret enforcement systems, T-TIP provides a timely opportunity to explore opportunities to adopt consistent approaches that could serve as foundation for global standards and be consistent with the agreement's goal to promote greater regulatory harmonization and coherence.

important opportunities to secure advances in protecting trade secrets, including through criminal and civil remedies and commitments to work cooperatively to combat all forms of trade secret theft and economic espionage. Such advances would not only benefit the parties to each agreement but would also contribute to the establishment of more robust global standards.

Similarly, the U.S. and China have recently reinvigorated negotiations on a Bilateral Investment Treaty ("BIT"). BITs provide investors with improved market access, protections from discriminatory or other arbitrary treatment, and a mechanism to pursue international arbitration against a foreign government to protect against expropriation or other violations of the treaty. These negotiations provide an excellent vehicle for ensuring that trade secrets, as a key intellectual property right, are protected against expropriation. In particular, U.S.-China BIT negotiations provide an opportunity to address the discriminatory impact of technology transfer requirements as a condition for market access or investment.

While these negotiations provide the most direct avenue to addressing the threats posed to trade secrets by cyber-based and other forms of industrial espionage, they should not be the exclusive trade-related avenues to pursue the issue. A wide variety of international fora provide opportunities to elevate trade secret protection. For example, at July's high-level U.S.-China Strategic and Economic Dialogue, U.S. Vice President Biden pressed China to halt the cyber theft of trade secrets.[77] In addition, trade dialogues such as those at the Asia Pacific Economic Cooperation (APEC) forum, Organization for Economic Co-Operation and Development (OECD), and the WTO TRIPS Council all provide opportunities to raise trade secret concerns, discuss best practices, and enhance global standards.

Of course, efforts to raise global standards will take time and, even then, they may not be sufficient to stem the growing tide of economic espionage and trade secret theft in the short term. If the U.S. is to deter the most egregious of crimes, particularly by criminal organizations and foreign governments, it should consider more effectively deploying existing enforcement tools and exploring new ones.

For example, the Office of the U.S. Trade Representative's Special 301 report is an important tool for putting trade partners on notice about concerns related to their trade secret protection regimes and to possibly setting the stage for potential enforcement action. For the first time in 2013, USTR included a designated section on trade secret theft in its Special 301 Report. The Trade Act of 1974 requires USTR to identify those countries that deny adequate and effective protection for intellectual property rights or deny fair and equitable market access for persons that rely on IPR protection. The most egregious of offenders are designated as Priority Foreign Country ("PFC"), requiring a Section 301 investigation, which could prompt WTO litigation and the imposition of tariffs or other border measures.[78]

---

[77] Paul Eckert & Anna Yukhananov, *U.S.-China talks cover cyber issues, currency, Chinese reform*, Reuters, *available at* http://www.reuters.com/article/2013/07/10/us-usa-china-dialogue-idUSBRE9690T520130710.

[78] As one author noted regarding the Administration strategy document, WTO enforcement actions were noticeably absent from the strategy. The paper further observes: "However, WTO members have, to date, shown no interest in addressing economic espionage within the WTO despite mounting worries about this practice[,]" citing difficulty establishing responsibility for government-

Given the scope and gravity of the problem, other proposals for more robust enforcement are emerging. These include potential reforms to Section 337 of the Tariff Act of 1930 (19 U.S.C. § 1337) (commonly referred to as "Section 337"), procurement and supply chain reform, and the broader use of sanctions.[79] We are not expressing a view on these; they each are intended to serve a broader public policy purposes, but each also has risk.

U.S. FEDERAL GOVERNMENT COORDINATION

A wide variety of agencies have responsibility for the protection of trade secrets within the federal government. The 2013 Trade Secret Strategy, for example, highlights the role of eight U.S. Government Departments (Commerce, Defense, Homeland Security, Justice, State, Treasury, the Office of the Director of National Intelligence and the United States Trade Representative).

Similarly, responsibility for cybersecurity in the federal government is spread across a variety of agencies, including the Department of Defense, Department of Homeland Security, Federal Bureau of Investigation, National Institute for Standards and Technology, and the National Security Agency.

Within each domain there exist mechanisms to facilitate operational and investigative coordination, including the National Intellectual Property Rights Coordination Center (NIPRCC) for trade secrets and the DHS-led National Cybersecurity and Communications Integration Center (NCCIC) and the FBI-led National Cyber Investigative Joint Task Force (NCIJTF) for cybersecurity.

Efforts should be made to improve the coordination between the NIPRCC and either or both of these cybersecurity centers, including through the exchange of detailees and the establishment of clearer protocols for operational and investigative coordination, consistent with agencies' existing authorities and legal requirements for the protection of relevant information.

Such efforts would strengthen the U.S. government's ability to address each of these important issues and could help to clarify and in some cases deconflict investigations of these matters.

CONCLUSION

The increasing scope in size and impact of economic espionage and trade secret theft merits a multi-pronged approach by the public and private sectors alike. Businesses must do their part to harden their cyber defenses, but to avoid continued, significant and irreversible harm to U.S. companies and the overall economy, robust public policy tools—including in particular trade tools—must also be utilized to raise global standards and enhance deterrence against this growing threat.

---

sponsored espionage as one of the challenges to launching such an enforcement action. David P. Fidler, *Economic Cyber Espionage and International Law: Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies*, American Society of International Law Insights (Mar. 10, 2013), *available at* http://www.asil.org/pdfs/insights/insight130320.pdf.

[79] *See, e.g.*, IP Comm'n Report.