## BNA's Patent, Trademark & Copyright Journal<sup>®</sup>

Reproduced with permission from BNA's Patent, Trademark & Copyright Journal, 90 PTCJ 2233, 10/23/2015. Copyright © 2015 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

### TRADE SECRETS

The author provides a comparative analysis of trade secret law in the U.S., Europe, the BRIC countries and Japan.

### **International Protection of Trade Secrets**

Bloomberg BNA



### By John W. Harbin

n the late 1700s and early 1800s, leaders of the fledgling United States encouraged others to take industrial secrets from abroad. In his *Report on Manufactures* in 1791, Alexander Hamilton recommended rewarding those who brought "improvements and secrets of extraordinary value" from abroad. George Washington praised the "activity and zeal" of Thomas Digges in his industrial espionage efforts (for which Digges was repeatedly jailed by Great Britain, then the world's leading industrial power).<sup>1</sup>

Now, the United States is the world's leading economic power, and U.S. businesses are regularly sub-

John Harbin, principal at Meunier, Carlin, & Curfman LLC, is a renowned trial attorney with three decades of experience in intellectual property and complex business cases, having tried more than 30 jury and bench trials in jurisdictions throughout the country, as well as at the ITC and in several arbitrations. jected to trade secret theft. The U.S. and many other countries are attempting to enhance the protection of this unique form of intellectual property. This article will review the status of protection efforts in the U.S. and major markets abroad.

# A. U.S. Efforts to Strengthen Trade Secret Protection

In recent years, the U.S. government has improved trade secret protection by executive order, increased criminal prosecutions, new legislation and trade agreements, and in one case the federal judiciary has done the same.

### **1.** Orders from the White House

On Feb. 2, 2013, the Administration announced its "Strategy on Mitigating the Theft of U.S. Trade Secrets," which listed several steps it planned to take, including:

1. Focusing diplomatic efforts to protect trade secrets overseas, stating that U.S. trading partners must treat trade secret theft seriously. This would include using trade policy tools to increase international enforcement against trade secret theft, including deeper cooperation with like-minded trading partners and targeting weakness in protections through enhanced use of the annual Special 301 process,<sup>2</sup> raising trade secret issues in bilateral negotiations and negotiating free trade agreements

<sup>&</sup>lt;sup>1</sup> Doron S. Ben-Atar, *Trade Secrets: Intellectual Piracy and the Origins of American Industrial Power*, Yale University Press (2004), p. 146.

<sup>&</sup>lt;sup>2</sup> The Special 301 process evaluates the degree to which the U.S.'s trading partners are protecting intellectual property. A key part is the Special 301 Report, which is an annual publication by the Office of the U.S. Trade Representative under Section 301 of the 1974 Trade Act to identify trade barriers to U.S. companies because of intellectual property issues. As part of the Report, the USTR must identify countries that do not provide "adequate and effective" IP protection and those deemed worst are put on the "Priority Watch List."

with firm obligations on trade secret protection (such as the just-concluded Trans-Pacific Partnership negotiations, discussed below);

- 2. Promoting best practices by private industry to protect trade secrets;
- 3. Enhancing domestic law enforcement operations;
- 4. Improving domestic legislation; and
- 5. Increasing public awareness and stakeholder outreach.

On Feb. 12, 2013, the White House issued its Executive Order on Improving Critical Infrastructure Cybersecurity, the purpose of which is to increase policy coordination and information-sharing about cybersecurity threats and incidents and "to assist the owners and operators of critical infrastructure in protecting their systems from unauthorized access, exploitation, or harm ...." This Order calls for developing (a) a "Cybersecurity Framework," including standards, procedures and processes to reduce cybersecurity risks, and (b) a voluntary program for owners and operators of critical infrastructure to adopt the Framework.

### 2. Increased Criminal Enforcement

The Justice Department has increasingly used the Economic Espionage Act of 1996, 18 U.S.C. § 1831, et seq., which criminalizes trade secret misappropriation. In June 2013, Sinovel Wind Group, a large wind turbine company in China, was indicted for criminal trade secret theft and copyright infringement for allegedly stealing technology from a Massachusetts company. The case is ongoing; on July 23, 2015, the Seventh Circuit rejected an appeal and mandamus petition by the Chinese Sinovel entity seeking to dismiss the indictment.<sup>3</sup>

In March 2014, a California jury convicted an ex-DuPont engineer of conspiracy to steal DuPont's proprietary process for making titanium dioxide and sell it to a Chinese government-owned business for \$28 million, the first economic espionage conviction by a U.S. jury. In August 2014, the defendant was sentenced to prison. On Sept. 29, 2015, his wife pled guilty to conspiracy to tamper with evidence and was sentenced to probation and restitution of \$6 million.

Also last year, the U.S. charged members of the Chinese military with criminal espionage, the first time such charges have been brought against a state actor. In May 2015, a federal indictment charged six Chinese citizens with conspiracy to steal proprietary technology from two U.S. businesses.

### 3. Strengthening Federal Legislation

Recently, Congress has strengthened the Economic Espionage Act in two ways. First, in the Trade Secret Clarification Act of 2012, Congress closed a loophole in the Act, 18 U.S.C. § 1832(a), so that theft of information a company *uses internally* in its business can be criminally prosecuted, as long as it relates to a product or service used or intended for use in interstate or foreign commerce. This was in response to the Second Circuit's decision in *U.S. v. Aleynikov*,<sup>4</sup> reversing a criminal con-

viction under the EEA because the stolen source code had only been used internally by the victimized business.

Second, the Economic Espionage Penalty Enhancement Act, passed in 2013, increased the maximum fines and penalties under 18 U.S.C. § 1831. Individuals who violate Section 1831(a) (concerning trade secret theft to benefit a foreign government, agent or instrumentality) may now be fined up to \$5 million and imprisoned for up to 15 years. Under Section 1831(b), organizations that violate Section 1831(a) may now be fined up to the greater of \$10 million or three times the value of the stolen trade secret.

Currently, there is a bipartisan effort in Congress to create a federal civil cause of action for trade secret misappropriation. The most recent attempt (after two failed efforts the last two years), the Defend Trade Secrets Act of 2015, introduced on July 29, 2015, would establish a uniform standard for misappropriation; create federal question jurisdiction in federal court; and provide treble damages and injunctive relief to preserve or seize evidence and prevent disclosure or use. Generating some controversy is a provision that would allow for an ex parte seizure order to have the trade secret material brought to and held in court, with the defendant allowed to seek damages and attorneys' fees for wrongful seizure.

### 4. The Trans-Pacific Partnership

As noted, the President has sought to strengthen trade secret regimes through trade agreements. On Oct. 5, 2015, the United States and 11 other Pacific Rim nations<sup>5</sup> announced agreement on The Trans-Pacific Partnership, reportedly the largest regional trade agreement in history.

The text of the agreement will not be available for several weeks (and Congress will later have to vote in favor for it to be adopted here). Reportedly the accord requires the signatories to (a) "comprehensively address the problem of trade secret theft, including theft by state-owned enterprises"; to "establish criminal procedures and penalties for trade secret theft"; and to ensure "the availability of mechanisms to effectively enforce" IP rights.<sup>6</sup>

## **5.** Protecting Trade Secrets At the International Trade Commission

The International Trade Commission has authority to exclude the importation of articles where it finds "[u]nfair methods of competition [or] unfair acts<sup>7</sup> in the importation of" those articles under 19 U.S.C. \$ 1337(a)(1)(A).

In *TianRui Group Co. v. ITC*,<sup>8</sup> the U.S. Court of Appeals for the Federal Circuit affirmed the ITC's authority to remedy trade secret misappropriation that takes place abroad. A complainant must show that the im-

<sup>&</sup>lt;sup>3</sup> U.S. v. Sinovel Wind Grp. Co., 794 F.3d 787, 115 U.S.P.Q.2d 1582 (7th Cir. 2015) (90 PTCJ 2775, 7/31/15).

<sup>&</sup>lt;sup>4</sup> U.S. v. Aleynikov, 676 F.3d 71, 102 U.S.P.Q.2d 1458 (2d Cir. 2012) (83 PTCJ 910, 4/20/12).

<sup>&</sup>lt;sup>5</sup> The other nations are Australia, Canada, Japan, Malaysia, Mexico, Peru, Vietnam, Chile, Brunei, Singapore and New Zealand. *See The Trans-Pacific Partnership*, Office of the U.S. Trade Representative.

<sup>&</sup>lt;sup>6</sup> The Trans-Pacific Partnership: Promoting Innovation & Creativity, Office of the U.S. Trade Representative (2015).

<sup>&</sup>lt;sup>7</sup> The unfair acts/methods include violations of intellectual property rights.

<sup>&</sup>lt;sup>8</sup> TianRui Grp. Co. v. Int'l Trade Comm'n, 661 F.3d 1322, 100 U.S.P.Q.2d 1401 (Fed. Cir. 2011) (82 PTCJ 810, 10/14/11).

ported articles were manufactured using the stolen trade secret and that the "threat or effect" of the importation is "to destroy or substantially injure an industry in" or "to prevent the establishment of an industry in" the United States. The case concerned a secret process for making cast steel railway wheels held by a U.S. company, Amsted. The defendant, Chinese company TianRui, had tried to license the process from Amsted. When those efforts failed, TianRui hired former employees of a Chinese licensee of Amsted and began exporting wheels made with the process to the U.S. Amsted sought relief in the ITC. Notably, the Federal Circuit affirmed the ITC's authority even though Amsted was no longer using the secret process to make the wheels it was selling in the U.S.<sup>9</sup>

Since *TianRui*, there have been two notable trade secret cases at the ITC. In *Certain Rubber Resins*, Inv. No. 337-TA-849, complainant SI Group claimed that Chinese tire makers had stolen, via an ex-employee of SI's Chinese subsidiary, trade secrets regarding producing rubber resins. (SI commenced the ITC action after efforts to obtain relief in China failed.). In early 2014, the ITC affirmed the finding by the Administrative Law Judge (ALJ) of a Section 337 violation. The ITC barred the respondents from importing rubber resins made with the trade secrets for 10 years. The case is on appeal.<sup>10</sup>

In Inv. No. 337-TA-88, Manitowoc Cranes claimed that a Chinese company and its U.S. subsidiary stole, via a departing engineer, its design for crawler cranes with stabilizing counterweight systems. It also alleged patent infringement.

On April 16, 2015, the ITC affirmed the ALJ's finding of trade secret misappropriation and infringement and barred the respondents from importing such products for 10 years on the trade secret claim.

Given these developments, U.S. businesses that are the victims of trade secret theft have options beyond the traditional civil court case, such as presenting the information to federal authorities or, in the appropriate circumstances, seeking import relief from the ITC. Businesses should ascertain what information in their operations, from manufacturing to marketing to accounting, constitutes proprietary information and what they are doing to protect the information. An audit of the firm's trade secret protections may be warranted.

### **B. Efforts in the European Union**

The European Union is seeking to buttress trade secret protection by providing a pan-European legal regime. Currently, trade secret laws vary country by country, with uneven protection and enforcement.

The World Trade Organization's TRIPS Agreement, which went into effect on Jan. 1, 1995, contains in Article 39.2 a definition of "Undisclosed Information," including trade secrets. It requires Member States to provide a minimum level of protection, including providing means to obtain and preserve evidence; injunctions against misappropriation and importation; rights to obtain information about third parties' involvement in production and distribution of infringing goods; and damages. But it has not been uniformly adopted and where it has been adopted, implementation often varies.

The defects of the current state-by-state regime in Europe include (a) the lack of a uniform definition of trade secrets or the means to protect the secrets in court and (b) weak penalties. Just identifying what information is protectable can be difficult. Only 10 of the 28 member states have statutory definitions of trade secrets and only one country, Sweden, has a comprehensive statutory trade secret scheme. Some states protect trade secrets through different civil and criminal legislation, such as unfair competition or industrial property laws. France's Code of Industrial Property protects *manufacturing* trade secrets. Tort law is used in some countries. In common law countries (e.g., the UK), trade secrets are protected by common law and contract law.

Definitions of what constitutes misappropriation vary. Sweden requires competitive damage, Bulgaria requires that the secret serve the interests of the parties, and Slovenia requires the trade secret to be qualified as such by corporate resolution. In most of the larger markets (e.g., Germany, France and the UK), the definition comes from case law.

Most states do not allow enforcement actions against third parties who obtained the information in good faith. Italy requires a showing that the recipient is aware of the misappropriation.

Also, the available remedies differ. Some but not all countries allow for the return, seizure or destruction of pirated items, or for ex parte orders for searching offices and IT systems. There are differing criminal sanctions, with some large markets (e.g., the UK) lacking any criminal statute on trade secret theft. Some states provide for corporate liability, others do not, and criminal sanctions vary. In Greece, the maximum sentence is three months; in Poland, only one month.

Also, means are lacking to protect the secrecy of the information in court proceedings. Civil proceedings in all Member States are public, and the grounds for excluding the public are limited to security, public order and decency. Only a few states allow for a party to request that proceedings be held in private and in practice that request is seldom granted.

As a result, there are few reports of trade secret cases being brought in the Member States and virtually no cross-border actions.

A 2013 survey by the European Commission found overwhelming business support for a pan-EU law. Seventy-five percent of companies stated that trade secrets are important for competitiveness and innovation; 20 percent said they had been victims of misappropriation in the last 10 years. The EC staff found that the current piecemeal protections harm the competitiveness of EU businesses, particularly small manufacturing entities, which rely more on trade secret protection, and that adopting uniform protections would facilitate cross border business and R&D.

The EC's November 2013 draft directive for an EUwide trade secret law would harmonize the definitions of (a) trade secrets (requiring, generally consistent with U.S. definitions, that the information be confidential, of commercial value and the subject of reasonable efforts to maintain confidentiality) and (b) misappropriation, providing protection for reverse engineering and parallel innovation.

<sup>&</sup>lt;sup>9</sup> Id. at 1335-37.

<sup>&</sup>lt;sup>10</sup> Sino Legend (Zhangjiagang) Chem. Co. v. Int'l Trade Comm'n, No. 2014-1478 (Fed. Cir.).

The proposal does not address criminal sanctions but provides civil remedies (i) to stop the unlawful use and further disclosure of trade secrets, including providing remedies against third parties who possess the information; (ii) to remove from the market goods produced by use of illegally acquired secrets; (iii) for compensatory damages; and (iv) to protect the secrecy of the information in court proceedings.<sup>11</sup>

The Council of the European Union responded favorably to the proposal on May 26, 2014. The European Economic and Social Committee, which includes representatives from consumer and environmental groups, trade unions, small and medium-sized companies and social NGOs, also responded favorably. In June 2015, the European Parliament's Legal Affairs Committee voted in support of the Trade Secrets Directive, but backed some changes to protect the rights of workers to use honestly-acquired experience and skills and to prohibit legal actions for some disclosures, such as if the disclosure is to reveal fraud or illegal activity or is otherwise in the public interest. Both the EC and the EP must approve the Directive before it can come into force.

Until such a pan-European law is adopted, entities doing business in Europe should make sure they are familiar with the trade secret laws in each jurisdiction. Non-disclosure agreements are commonly used but again attention needs to be paid to the law of each jurisdiction. And most EU countries have stronger employee and privacy protections than is typical in U.S. jurisdictions (hence the proposed changes to the Trade Secret Directive), and they need to be factored in.

# C. The Status of Trade Secret Protection in the BRIC Countries and Japan

All four BRIC countries (China, India, Russia and Brazil) are members of the WTO and signatories to TRIPS, which as noted requires certain protections for trade secrets. All four have legal protections for trade secrets on the books, but the laws can be weak and enforcement difficult. At least in part because of these issues, there are few trade secret cases in the BRIC countries.

#### 1. China

China has a codified civil law system. The main trade secret laws are found in China's Anti-Unfair Competition Law of 1993 (AUCL), which provides for administrative penalties and compensatory damages in civil cases. Chinese criminal law was amended in 1997 to provide for prison terms of up to seven years for persons whose misappropriation is found to cause "serious losses" to the owner.

As a practical matter, however, there are several significant impediments to protecting information in China. Just seeking permission to do business in China can put confidential information at risk. There is often pressure to license the technology to a domestic Chinese partner, and China's extensive licensing requirements often require disclosures of confidential information. Compounding the problem, Chinese competitors often serve as expert advisors to these panels and thus have access to the information disclosed.<sup>12</sup>

Weaknesses in the court system also hinder the ability to protect trade secrets. For example, there are high evidentiary burdens, yet discovery is extremely limited and some evidence is discounted. And, as with licensing entities, courts often use outside expert panels that can include Chinese competitors. Also, there are no clear national laws on protecting the confidentiality of the information in court proceedings.<sup>13</sup>

The U.S.-China Business Council (USCBC) is a nonprofit organization comprised of approximately 220 American companies doing business in China. In its 2012 and 2103 member surveys, trade secret protection was the IP issue of greatest concern. In its 2015 Member Survey Report, the trade secret issues of greatest concern are: enforcing non-disclosure agreements (63 percent), gathering evidence for trade secret cases (54 percent) and administrative hearings (33 percent), lack of regulatory clarity (46 percent) and lack of legal framework (42 percent).

The 2015 Special 301 Report of the USTR states that trade secret theft "remains a particular concern" and a "growing problem" in China, that such theft takes place inside and outside China (it quotes a report from the National Counterintelligence Executive that "Chinese actors are the world's most active and persistent perpetrators of economic espionage") and that conditions are "unlikely to improve as long as those committing such theft, and those benefitting, continue to operate with relative impunity."<sup>14</sup>

In December 2013, in the Joint Commission on Commerce and Trade (JCCT), China pledged to improve trade secret protections, and its December 2014 JCCT commitment was to protect from disclosure trade secrets submitted to the government in regulatory or administrative proceedings. China also stated that it is studying a possible new trade secrets law.<sup>15</sup>

The 2015 Special 301 Report urges China to update and amend the AUCL and related trade secret laws and regulations, and to stop using regulatory pressures to compel the licensing or disclosure of technology or to dissuade IP owners from pursuing available legal remedies.<sup>16</sup>

### 2. India

India has no specific trade secret legislation. Indian courts rely on equitable and common law remedies, including breach of confidence theories, which is essentially a breach of contract claim, though breach of confidence can also constitute a tort.

The civil remedies include injunctions against disclosure, return of the information and compensatory damages. There appears to be no criminal liability in India.

India is on the 2015 301 Priority Watch List. The 2015 Special 301 Report expressed concerns about (i) re-

<sup>&</sup>lt;sup>11</sup> See Proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, European Commission, COD 2013/0813, Nov. 28, 2013, available at http://eurlex.europa.eu/legal-content/EN/TXT/PDF/? uri=CELEX:52013PC0813&from=EN.

 <sup>&</sup>lt;sup>12</sup> See Feb. 7, 2014, letter from U.S.-China Business Council for Special 301 Review, pp. 3-6. China has been on the Priority Watch List for several years.
<sup>13</sup> See Recommendations for Strengthening Trade Secret

<sup>&</sup>lt;sup>13</sup> See Recommendations for Strengthening Trade Secret Protection in China, The U.S.-China Business Council (September 2013).

<sup>&</sup>lt;sup>14</sup> 2015 Special 301 Report, pp. 20, 33 and 36).

<sup>&</sup>lt;sup>15</sup> *Id* at 37.

<sup>16</sup> Id. at 33, 34.

ported difficulties in obtaining damages and other remedies; (ii) over-reliance on contract law so that, in other situations, such as theft by a competitor, effective relief may be unavailable; and (iii) India's court system lacking sufficient means to protect confidential information in the course of judicial proceedings. The Report, though, notes that the current administration in India has been examining IP issues and engaging with the U.S. since 2014.<sup>17</sup>

### 3. Russia

Russia has statutory protections for trade and production secrets.

Russian law imposes strict requirements on the trade secret owner to adopt secrecy measures (e.g., stamping of documents, formalizing a list of trade secrets and keeping—and updating—a list of those persons having access to the information). Similarly, the Information Law requires that the holder have implemented a "trade secrecy system." So not only are these requirements strict, they are more detailed than in most countries. The statutory penalties include reprimand, dismissal and damages, but are often viewed as lax.

In 2013, Russia opened a specialized Intellectual Property Court able to hear trade secret cases. Reportedly, 350 IP disputes were filed in the first three months.<sup>18</sup> Russia reportedly amended its Trade Secret Law in 2014 to strengthen the penalties imposed on company executives and also on employees, requiring them to reimburse the company for losses from theft of its trade secrets.<sup>19</sup>

### 4. Brazil

To comply with the TRIPS Agreement, Brazil enacted some trade secret protections in its Industrial Property Act of 1996 (the IPL), which establishes the crime of unfair competition for the unauthorized use or disclosure of confidential information used in industry or commerce that (a) was learned via employment or contractual relationship or (b) was obtained by fraud or improper means. The law provides for compensatory damages, and Articles 844, 927 and 944 of the Brazilian Civil Code also contain damages provisions.

Article 206 of the IPL empowers the court to keeping information confidential during a court proceeding, in-

cluding closing the courtroom. There is a dearth of reported trade secret cases in Brazil, however.

Brazil is on the Watch List in the 2015 Special 301 Report. One concern expressed by the USTR is inadequate protection against unfair commercial use of undisclosed tests and other data generated to obtain marketing approval for pharmaceutical and agricultural chemical products.<sup>20</sup>

For entities doing business in the BRIC countries, particularly China, focus should be given to implementing best practices to protect against the disclosure or misappropriation of the information at the front end, rather than relying on remedies facially available after a trade secret has been stolen. Regarding India, given the focus on contract principles, a recommended practice is to require non-disclosure agreements with employees and third parties. In Russia, entities should focus not just on NDAs, but on complying with Russia's detailed requirements for protecting confidential information.

### 5. Japan

Japan is a civil law country. Article 2 of its Unfair Competition Prevention Law defines six acts of trade secret-related unfair competition, which are similar to U.S. violations (e.g., acquisition, use or disclosure of a trade secret with knowledge it was wrongfully acquired). Critics complain that discovery is too restricted in Japanese courts, making trade secret litigation difficult.

In 2005, Japan amended the UCPL to allow Japanese courts to protect the confidentiality of information divulged in the court proceeding, including by implementing protective orders and holding closed hearings.

Article 21 of the UCPL provides criminal sanctions for trade secret theft where there is intent to acquire an illicit gain or injure the owner of the secret. The crime is punishable by up to 10 years in prison.

Recent reports of trade secret theft have led Japanese lawmakers and other governmental groups to consider reforming Japan's trade secret laws. A Nissan employee was indicted in October 2014 for taking secrets regarding a new car sales plan to a competitor and another Nissan employee was arrested in February 2015 and accused of taking secret documents to a Chinese-affiliated competitor. Japan's signing of the Trans-Pacific Partnership can be expected to accelerate such efforts.

<sup>&</sup>lt;sup>17</sup> 2015 Special 301 Report, pp. 45, 46 and 51.

<sup>&</sup>lt;sup>18</sup> Russia's IP Court: three months on, AIPLA Newsstand (Oct. 3, 2013).

<sup>&</sup>lt;sup>19</sup> Law On "Commercial Secrets" amended, AIPLA Newsstand (March 27, 2014).

<sup>&</sup>lt;sup>20</sup> 2015 Special 301 Report, p. 71.