Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

Attorneys from Morgan, Lewis & Bockius, in the seventh installment in a series of articles examining trade secrets issues in the U.S., review in detail the 10 cases prosecuted under the Economic Espionage Act related to foreign government espionage.

Reviewing the First Foreign Economic Espionage Cases

BY MARK L. KROTOSKI AND JENNY HARRISON

Mark L. Krotoski is a Litigation Partner in the Privacy and Cybersecurity and Antitrust practices of Morgan, Lewis & Bockius. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.

Jenny Harrison is an associate in the Litigation Group of Morgan, Lewis & Bockius, and is resident in the San Francisco office. Her practice includes all types of litigation matters, with a focus on securities litigation, specifically government investigations and enforcement.

The Economic Espionage Act of 1996 (EEA) provides for the criminal prosecution of the theft or misappropriation of trade secrets.[1] The statute was enacted to protect and promote national and economic security by filling in gaps under the law which previously allowed this conduct to go unpunished.[2] Congress is presently considering an amendment to the EEA which would establish a federal civil private right of action for the theft of trade secrets.[3]

One key part of the EEA involves foreign economic espionage, which involves the misappropriation of a trade secret with the intent to benefit a foreign government, instrumentality or agent. In the past two decades, some challenging foreign economic espionage cases have been prosecuted involving a diverse range of scientific research, technology and military application trade secrets. This article reviews the 10 cases that have been authorized and prosecuted under the statute.

[1] Pub. L. No. 104-294, 110 Stat. 3488 (Oct. 11, 1996) (codified as amended 18 U.S.C. § § 1831–1839). All case information is based upon publicly available sources.

[2] *See, e.g.*, H. Rep. No. 788, 104th Cong., Sess. 4 (1996) [hereinafter ''1996 House Report''] (noting ''the nation's economic interests are part of its national security interests'' and ''threats to the nation's economic interest are threats to the nation's vital security interests''); *id.* at 6-7 (noting gaps under federal law).

[3] *See, e.g.*, M. Krotoski, The Time Is Ripe for a New Federal Civil Trade Secret Law, BNA's Patent, Trademark & Copyright Journal, 89 PTCJ 28 (Nov. 7, 2014) (identifying several reasons warranting a federal trade secret private right of action) (89 PTCJ 28, 11/7/14).

EEA Overview

Under the EEA, two distinct criminal offenses address the theft or misappropriation of a trade secret. The offenses are often referred to by their statutory sections: Section 1832 (trade secret theft) or Section 1831 (foreign economic espionage).

The two offenses focus on different forms of intent. Section 1832, involving traditional trade secret theft or misappropriation, requires proof of the ''intent to convert a trade secret . . . to the economic benefit of anyone other than the owner'' and ''intending or knowing that the offense will, injure any owner of that trade secret.'' The maximum sentence for a Section 1832 conviction is 10 years and a fine of $250,000. An organization may be fined up to $5,000,000.[4] Approximately 25 Section 1832 cases have been prosecuted in the last year.[5]

A Section 1831 offense, known as foreign economic espionage, involves the misappropriation of a trade secret with the intent to benefit a foreign government, foreign instrumentality or foreign agent. Under the U.S. Attorney's Manual, a federal prosecutor may not charge a Section 1831 offense without prior review and approval by the Assistant Attorney General for the National Security Division.[6] The review process includes an assessment of foreign policy, strength of the evidence and other relevant factors.

The maximum sentence for a Section 1831 conviction is fifteen years and a fine of $5,000,000. An organization may be fined up to $10,000,000 or ''3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.''[7] At sentencing, under the Sentencing Guidelines, the court may impose a four-level enhancement if ''the defendant knew or intended . . . that the offense would benefit a foreign government, foreign instrumentality, or foreign agent,'' and a two-level enhancement may result if ''the defendant knew or intended that the trade secret would be transported or transmitted out of the United States.''[8]

Proving an Intent to Benefit a Foreign Government, Instrumentality or Agent

Some unique issues arise under Section 1831 cases. First the focus is on the defendant's *intent* to benefit a foreign government, instrumentality or agent. As the Ninth Circuit has observed, although evidence of the foreign government's role may be relevant under other statutes, ''criminal liability under the EEA may be established on the basis of Defendant's intent alone.''[9] While foreign government action is not required, it may provide circumstantial evidence of the defendant's intent.

The EEA does not define ''foreign government.'' However, it is generally understood elsewhere to include ''the government of a foreign country, irrespective of recognition by the United States.''[10]

The EEA defines ''foreign instrumentality'' as ''any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government.''[11] In other words, it may be a shell entity that is ''substantially'' controlled by a foreign government. The legislative history clarifies that the term ''substantially'' does not mean complete control, but refers to ''material or significant'' control, not ''technical or tenuous.'' The test is not meant to be ''mechanistic or mathematical.'' The ''pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.''[12]

Finally, the term ''benefit'' is construed broadly. Under the EEA, ''benefit means not only an economic benefit but also reputational, strategic, or tactical benefit.''[13]

First 10 Foreign Economic Espionage Cases

Since 1996, 10 foreign economic espionage cases have been authorized and prosecuted.[14] These cases present unique challenges including:

- Seeking to identify and recover trade secrets that may have been taken outside the United States;

[4] 18 U.S.C. § 1832.

[5] Press Release, Senator Coons, Hatch Introduce Bill to Combat Theft of Trade Secrets and Protect Jobs, April 29, 2014, http://www.coons.senate.gov/newsroom/releases/release/senators-coons-hatch-introduce-bill-to-combat-theft-of-tradesecrets-and-protect-jobs (noting ''the Department of Justice brought only 25 trade secret theft cases last year'') (88 PTCJ 41, 5/2/14).

[6] U.S. Attorney's Manual § 9-59.100 (Economic Espionage Act of 1996 (18 U.S.C. § § 1831-1837)—Prosecutive Policy), http://www.justice.gov/usam/usam-9-59000-economic-espionage, § 9-90.020 (National Security Matters Prior Approval, Consultation, and Notification Requirements), http://www.justice.gov/usam/usam-9-90000-national-security#9-90.020; *see generally* Thomas Reilly, Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and The ''Foreign Instrumentality'' Element, 57 UNITED STATES ATTORNEYS' BULLETIN 24-26 (Nov. 2009) (explaining the approval process), http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[7] 18 U.S.C. § 1831.

[8] U.S.S.G. § 2B1.1(b)(13).

[9] *United States v. Chung*, 659 F.3d 815, 828, 2011 BL 244585 (9th Cir. 2011).

[10] 18 U.S.C. § 1116(b)(2).

[11] 18 U.S.C. § 1839(1).

[12] 142 CONG. REC. S12201, S12212 (daily ed. Oct. 2, 1996) (Sen. Kohl remarks).

[13] 1996 House Report, *supra* note 2, at 11 (emphasis added).

[14] Statement of Randall Coleman, Assistant Director, Counterintelligence Division, Federal Bureau Of Investigation, before the Senate Judiciary Subcommittee On Crime And Terrorism, ''Economic Espionage And Trade Secret Theft: Are Our Laws Adequate For Today's Threats?'' (May 13, 2014) (''Since the law was passed in 1996, there have been 10 economic espionage'' cases under Section 1831.), http://www.judiciary.senate.gov/imo/media/doc/05-13-14ColemanTestimony.pdf ; *see also* M. Krotoski, Common Issues and Challenges In Prosecuting Trade Secret and Economic Espionage Act Cases, 57 UNITED STATES ATTORNEYS' BULLETIN 8 (Nov. 2009) [hereinafter ''Common Issues and Challenges''] (summarizing the first six EEA prosecutions), http://www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

  PTCJ ISSN 0148-7965

- Proving conduct that likely occurred outside the country;
- Investigating a ''highly reactive case scenario with largely historical and most likely limited evidence'' without knowing whether the full scope of the conduct can be uncovered and the number of misappropriated trade secrets can be identified;[15]
- Establishing that the defendant intended to benefit a foreign government, instrumentality or agent by expert and other forms of evidence;
- Preserving and obtaining electronic evidence including from other countries;
- Handling and understanding evidence in other languages;
- Maintaining the confidentiality of the trade secrets; and
- Requesting and obtaining DOJ approval to charge a Section 1831 offense.

Of the 10 foreign economic espionage cases, six cases involving eight individuals have resulted in Section 1831 convictions while other counts of conviction have also been obtained in other cases. There have been four trials, including two jury and two bench trials, with varied results. Each case is reviewed including the facts, types of trade secrets, foreign government and foreign instrumentality issues, and disposition.

1. *United States v. Takashi Okamoto* (N.D. Ohio)

The first foreign economic espionage case involved the misappropriation of DNA and cell line reagents trade secrets related to the cause and treatment of the Alzheimer's Disease. Takashi Okamoto, a Japanese national, was the lead investigator (or researcher) of this work at the Lerner Research Institute of the Cleveland Clinic Foundation in Cleveland, Ohio. The government alleged that in 1999 he accepted a position at the Institute of Physical and Chemical Research (RIKEN), a government funded laboratory in Japan. In July 1999, he allegedly misappropriated trade secrets from the Cleveland Clinic Foundation and also destroyed trade secrets at the lab to thwart completion of the research projects. He sent four boxes of stolen DNA and cell line reagents to a Hiroaki Serizawa, a research associate at the Kansas University Medical Center in Kansas City, Kansas, for holding until he could later retrieve them while enroute to Japan. At the end of July 1999, Okamoto resigned from his research position at the Clinic Foundation in Cleveland and started his new research position at RIKEN in Japan the next month. The government's theory was that he intended to benefit RIKEN as a foreign instrumentality as it received nearly all of its funding from the Ministry of Science and Technology.[16]

In May 2001, Okamoto and Serizawa were charged in a four-count indictment in the Northern District of Ohio which included one conspiracy count, two Section 1831 counts and one count of interstate transportation of stolen property. Over the next few years, the government pursued Okamoto's extradition from Japan to the United States to face the charges. The government presented the case to Japan's Ministry of Justice and Okamoto was incarcerated pending the final ruling on extradition. However, in March 2004, the Tokyo High Court ultimately declined the request to extradite Okamoto to the United States ''because industrial espionage is not a crime in Japan.''[17]

In May 2002, Serizawa pled guilty to one count of making false statements to the government concerning his relationship and contacts with Okamoto, the quantity of research materials taken and the position Okamoto took with RIKEN. He was sentenced to serve three years of probation, perform 150 hours of community service and pay a $500 fine.[18]

2. *United States v. Fei Ye and Ming Zhong* (N.D. Cal.)

In the second indictment and first Section 1831 case conviction, Fei Ye, a naturalized U.S. citizen who was born in China, and Ming Zhong, a Chinese national, pled guilty to possessing stolen trade secrets regarding the design and manufacture of computer microprocessors and admitted they intended to use these secrets at their PRC-funded company, Supervision. Supervision, founded in 2001 by the defendants, received funding from Chinese provincial governments in exchange for Supervision's promise to provide a share of its profits, repay the funding and locate facilities in that region. Supervision also applied for funding from the National High Technology Research and Development Program of China.[19] In November 2001, the defendants were arrested at the San Francisco International Airport as they attempted to board a flight destined for China. A search of their luggage led to the discovery of the microprocessor design trade secrets belonging to their former employers, Transmeta Corporation and Sun Microsystems.[20]

In December 2002, the defendants were charged with 10 counts, including two for foreign economic espio-

---

[15] Common Issues and Challenges, *supra* note 14, at 13.

[16] Indictment ¶¶19, 22-25, *United States v. Okamoto & Serizawa*, No. 01-CR-00210 (N.D. Ohio May 8, 2001) (No. 1).

[17] Tokyo High Court refuses US extradition, UPI (March 30, 2004), http://www.upi.com/Top_News/2004/03/30/Tokyo-High-Court-refuses-US-extradition/36271080689113/; *see also* Court rejects U.S. request for extradition in industrial spy case, The Japan Times (March 30, 2004), http://www.japantimes.co.jp/news/2004/03/30/national/court-rejects-u-s-request-for-extradition-in-industrial-spy-case/#.VROVM-9FCP8.

[18] Judgment and Minute Order, *United States v. Serizawa*, No. 01-CR-00210 (N.D. Ohio May 28 & 30, 2003) (Nos. 162, 164); *see also* Scientist Pleads Guilty to Providing False Statements Regarding Trade Secret Theft from Cleveland Clinic Foundation (May 1, 2002), http://www.justice.gov/criminal/cybercrime/press-releases/2002/serizawaPlea.htm; Japanese scientist admits deceiving FBI, USA Today (May 1, 2002), http://usatoday30.usatoday.com/news/world/2002/05/01/japanese-scientist.htm.

[19] *See generally* National High-tech R&D Program (863 Program), Ministry of Science and Technology of the PRC, http://www.most.gov.cn/eng/programmes1/.

[20] Press Release, U.S. Dep't of Justice, Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China (Dec. 14, 2006), http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm; *see also United States v. Fei Ye*, 436 F. 3d 1117, 1119, 77 U.S.P.Q.2d 1942 (9th Cir. 2006) (noting that the defendants were arrested ''while attempting to board a flight to China at the San Francisco International Airport'' and alleged trade secrets were ''simultaneously seized various . . . from defendants' personal luggage, homes, and offices'').

nage.[21] In December 2006, both defendants pled guilty to the two foreign economic espionage counts and admitted possessing the stolen trade secrets with the intent to benefit the PRC.[22] At sentencing, the Probation Officer recommended a sentence of 37 months in prison for Zhong and 46 months for Ye. While acknowledging the seriousness of the offense, the government requested a downward departure from the sentencing guidelines based largely on the cooperation provided by the defendants. The court granted the government's request for a lower sentence and imposed a term of one year and one day in prison and a three-year period of supervised release for each defendant.[23]

3. *United States v. Xiaodong Sheldon Meng* (N.D. Cal.)

The third foreign economic espionage case involved the misappropriation of a visual simulation software program trade secret used for training military fighter pilots and export of a prohibited munition list item that were both taken to the PRC. The trade secret was displayed at a demonstration project at the PRC Navy Research Center in Beijing.[24] According to the government, the defendant also was ''developing at least two proposals for two separate Air Forces in Southeast Asia involving visual simulation equipment and source code'' which would have involved ''the transfer and use of source code for the visual simulation products so the military customers could build, maintain and upgrade the simulators in the future.''[25] The case resulted in two significant national security convictions: the second conviction and first sentencing for foreign economic espionage and the first conviction involving ''source code'' under the Arms Export Control Act.[26]

In 2003, Xiaodong Sheldon Meng, a naturalized Canadian born in China, took trade secrets from his former employer, Quantum3D, to the PRC. In December 2004, while he was en route to an industry trade show in Orlando, customs agents at the Minneapolis airport discovered Quantum3D material on his laptop. Meng was allowed to travel to Orlando, but was arrested two days later for international/interstate transport of stolen property.[27] In a superseding indictment in December 2004, Meng was charged with 36 counts including three Section 1831 counts involving multiple foreign governments, such as the Thai Air Force, Malaysian Air Force and various PRC instrumentalities.[28]

In August 2007, Meng pled guilty to two national security violations: committing foreign economic espionage with the intent to benefit the PRC Navy Research Center and violating the AECA and the International Traffic in Arms Regulations. He admitted to misappropriating trade secrets to profit from them.[29] Meng was sentenced to 24 months and one day in prison, a three-year supervised release, and was ordered to pay $10,200 and forfeit computer equipment.[30]

4. *United States v. Lan Lee and Yuefei Ge* (N.D. Cal.)

The fourth case charging economic espionage—and only one to result in a post-trial acquittal and dismissal on all charges—involved the alleged misappropriation of computer chip designs and manufacturing information from NetLogic Microsystems (NLM) and Taiwan Semi-Conductor Company (TSMC) in 2003. Co-defendants Lan Lee and Yuefei Ge were indicted in September 2007 for five counts under Sections 1831 and 1832. The government alleged that the defendants intended to use the misappropriated information at their corporation, SICO Microsystems Inc., and that the defendants sought funding for SICO from the PRC's 863

[21] Indictment, *United States v. Fei Ye*, No. 02-CR-20145 (N.D. Cal. Dec. 4, 2002) (No. 31). The 10 counts included one count of conspiracy, two counts of economic espionage, five counts of possession of stolen trade secrets, and two counts of foreign transportation of stolen property. *See also* Press Release, U.S. Dep't of Justice, Pair from Cupertino and San Jose, California, Indicted for Economic Espionage and Theft of Trade Secrets From Silicon Valley Companies (Dec. 4, 2002), http://www.justice.gov/criminal/cybercrime/press-releases/2002/yeIndict.htm.

[22] Press Release, U.S. Dep't of Justice, Two Men Plead Guilty to Stealing Trade Secrets from Silicon Valley Companies to Benefit China (Dec. 14, 2006), http://www.justice.gov/criminal/cybercrime/press-releases/2006/yePlea.htm; Fei Ye Government's Sentencing Memorandum, at 3-4, 6 (June 17, 2008) (No. 247).

[23] Fei Ye Sentencing Hearing Transcript, at 12, 31-32, 39 (No. 272) (probation officer's sentencing recommendation); *id*. 7-8, 10, 12, 39-46 (government sentencing recommendation); *see also* Fei Ye Government's Sentencing Memorandum, at 7 (No. 247); Fei Ye Judgment (Nov. 25, 2008) (No. 268); Zhong Judgment (Nov. 25, 2008) (No. 270).

[24] Redacted Plea Agreement ¶ 2, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Aug. 29, 2007) (Nos. 76, 77); Meng Government's Sentencing Memorandum, at 5, 10-11 (June 11, 2008) (No. 94). *Disclosure*: Co-author Mark Krotoski was the prosecutor on the *Meng* case working with a team of dedicated FBI and ICE agents.

[25] Meng Government's Sentencing Memorandum, at 6.

[26] Arms Export Control Act (AECA) and the International Traffic in Arms Regulations (ITAR), 22 U.S.C. § § 2778(b)(2), 2778(c), and 22 C.F.R. § 120.2; *see generally* Press Release, U.S. Dep't of Justice, Former Chinese National Convicted of Economic Espionage to Benefit China Navy Research Center (Aug. 2, 2007), http://www.justice.gov/archive/opa/pr/2007/August/07_nsd_572.html; Press Release, U.S. Dep't of Justice, Chinese National Sentenced For Committing Economic Espionage With The Intent To Benefit China Navy Research Center (June 18, 2008) [hereinafter ''Meng Sentencing Press Release''], http://www.justice.gov/criminal/cybercrime/press-releases/2008/mengSent.pdf.

[27] Complaint, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Dec. 9, 2004) (No. 1).

[28] Superseding Indictment ¶ ¶ 28, 40, *United States v. Meng*, No. 04-CR-20216 (N.D. Cal. Dec. 17, 2004) (No. 57); Meng Redacted Plea Agreement ¶ 2 (Aug. 29, 2007) (Nos. 76, 77); Meng Government's Sentencing Memorandum, at 8 (June 11, 2008) (No. 94). The superseding indictment charged ''three conspiracy counts; three counts of economic espionage and attempted economic espionage; two counts of violations of the Arms Export Control Act; twelve counts of theft of trade secrets and attempted theft of trade secrets; fifteen counts of foreign and interstate transportation of stolen property; and three counts of making false statements to a government agency.'' Press Release, U.S. Dep't of Justice, Former Chinese National Charged with Stealing Military Application Trade Secrets from Silicon Valley Firm to Benefit Governments of Thailand, Malaysia, and China (Dec. 14, 2006), http://www.justice.gov/criminal/cybercrime/press-releases/2006/mengCharge.htm.

[29] Meng Redacted Plea Agreement ¶ 2 (Aug. 29, 2007) (Nos. 76, 77).

[30] Meng Judgment (June 24, 2008) (No. 103); *see also* Meng Plea Agreement ¶ 9 (forfeiture provision); Meng Sentencing Press Release, *supra* note 26. According to court records, the sentence included a reduction based on substantial assistance provided under U.S.S.G. § 5K1.1. *See* Meng Sentencing Hearing Transcript, at 10-11, 17-18 (June 18, 2008).

  PTCJ ISSN 0148-7965

Program and the People's Liberation Army's General Armaments Department.[31]

After a three week trial in late 2009, the jury found the defendants were not guilty of two charges related to TSMC's trade secrets, including foreign economic espionage and theft of trade secrets.[32] The jury was unable to reach a verdict on three other counts: conspiracy to commit foreign economic espionage, foreign economic espionage or attempted foreign economic espionage and theft of trade secrets belonging to NLM. Ultimately the court declared a mistrial,[33] and later acquitted the defendants on the foreign economic espionage counts regarding NLM's trade secrets since the ''government did not present any evidence that Defendants intended to enter into a venture capital relationship with an agent or instrumentality of the PRC'' and ''there was no evidence that Defendants intended to or were required as a condition of the grant to transfer any technology to the PRC or to any instrumentality or agent or to operate on behalf of a foreign government.''[34] The court granted the government's post-trial motion to dismiss the superseding indictment with prejudice.[35]

5. *United States v. Dongfan Chung* (C.D. Cal.)

The fifth EEA case involved the theft of space shuttle and Delta IV Rocket trade secrets by a Boeing and Rockwell engineer. The case was the first foreign economic espionage prosecution that went to trial (preceding the *Lee* jury trial by just four months) and also to result in a bench trial conviction.

Dongfan Chung, who was born in China and became a naturalized U.S. citizen, worked at Boeing and Rockwell as a civil engineer since the 1960s. After his retirement in 2002, he started working at Boeing as a contractor in 2003. Based in part on information obtained in another investigation, in 2006 FBI agents executed a search warrant at his residence and discovered approximately ''300,000 pages of Boeing and Rockwell documents, many of which related to the space shuttle, Delta IV Rocket, F–15 Fighter, B–52 Bomber and Chinook Helicopter.''[36] The records included six trade secrets: four documents about a phased array antenna project for the space shuttle and two documents concerning the Delta IV Rocket, which was a booster rocket designed to launch manned space vehicles.

In 2008, Chung was indicted on fifteen counts including eight foreign economic espionage counts.[37] At his June 2009 bench trial, the government introduced a 1985 ''tasking list'' from the Chinese Ministry of Aviation which asked for ''information concerning methods for determining the fatigue life of aircraft and helicopters, including information regarding United States military specifications.''[38] An FBI agent testified ''that technical documents responsive to the tasking list were found in Defendant's home.''[39]

The defendant was convicted in the bench trial of six EEA counts, one count of conspiring to violate the EEA, one count of acting as an unregistered foreign agent and one count of making a false statement to federal agents.[40] The defendant was sentenced to nearly 16 years in prison (188 months), which is the longest foreign economic espionage sentence to date.[41] The Ninth Circuit affirmed the convictions and sentence in the first appellate decision to consider the merits of a Section 1831 offense.[42]

6. *United States v. Hanjuan Jin* (N.D. Ill.)

The sixth foreign economic espionage case involved the misappropriation of trade secrets related to iDEN (Integrated Digital Enhanced Network) mobile communications technology from Motorola, Inc. by one of the company's software engineers. In February 2007, custom agents stopped Hanjuan Jin at Chicago's O'Hare Airport. Jin had a one-way ticket to China, more than 1,000 sensitive Motorola documents and $30,000 in cash. She had planned to work for Chinese company Sun Kaisens, which develops telecommunications technology for the Chinese military. Jin, a naturalized U.S. citizen who was born in China, was charged in a superseding indictment with three counts of economic espionage and three counts of trade secret misappropriation.

Jin waived her right to a jury trial and proceeded to a five-day bench trial in November 2011. The court convicted her on the three trade secret counts but acquitted

---

[31] Superseding Indictment, at 3, *United States v. Lee*, No. 06-CR-00424 (N.D. Cal. Sep. 26, 2007) (No. 36); *see also* Press Release, U.S. Dep't of Justice, Two Bay Area Men Indicted On Charges Of Economic Espionage (Sep 26, 2007), http://www.justice.gov/criminal/cybercrime/press-releases/2006/liIndict.htm.

[32] Lee Jury Verdict (Nov. 20, 2009) (No. 312); *see also* Lee Judgment of Acquittal (Dec. 2, 2009) (No. 314); Ge Judgment of Acquittal (Dec. 2, 2009) (No. 315).

[33] Lee Criminal Minutes—Jury Trial (Nov. 20, 2009) (No. 309).

[34] Order Granting In Part Defendants' Motion for Judgment of Acquittal, at 6, 13 (May 21, 2010) (No. 327); *id*. at 13 (''The government must present evidence that Defendants intended to confer a benefit on the PRC, not receive a benefit from it. The Court finds evidence that Defendants intended to apply for a grant from the PRC is insufficient to satisfy the statutory requirement that the government prove that the Defendants intended to provide a benefit to the PRC, or one of its instrumentalities or agents.''); *see also* Lee Judgment of Acquittal (June 30, 2010) (No. 338), Ge Judgment of Acquittal (June 30, 2010) (No. 339); Defendants' Motion for Acquittal (Nov. 3, 2009) (No. 280).

[35] Lee and Ge Order Granting Amended Notice of Dismissal (Oct. 27, 2010) (No. 382).

[36] *Chung*, 659 F.3d at 819.

[37] Indictment, *United States v. Chung*, No. 08-CR-00024 (C.D. Cal. Feb. 6, 2008) (No. 1). The charges included one conspiracy count; eight foreign economic espionage counts; one count of acting as an agent of a foreign government without prior notification to the Attorney General; one obstruction of justice count; and three false statement counts. *See* Press Release, U.S. Dep't of Justice, Former Boeing Engineer Charged with Economic Espionage in Theft of Space Shuttle Secrets for China (Feb. 11, 2008), http://www.justice.gov/criminal/cybercrime/press-releases/2008/chungCharge.htm.

[38] *Chung*, 659 F.3d at 820.

[39] *Id*.

[40] *United States v. Chung*, 633 F. Supp. 2d 1134, 1135, 2009 BL 151894 (C.D. Cal. 2009) (Memorandum of Decision); *see also* Press Release, U.S. Dep't of Justice, Former Boeing Engineer Convicted Of Economic Espionage In Theft Of Space Shuttle Secrets For China (July 16, 2009), http://www.justice.gov/criminal/cybercrime/press-releases/2009/chungConvic.pdf.

[41] Press Release, U.S. Dep't of Justice, Former Boeing Engineer Sentenced To Nearly 16 Years In Prison For Stealing Aerospace Secrets For China (Feb. 8, 2010), http://www.justice.gov/criminal/cybercrime/press-releases/2010/chungSent.pdf.

[42] *United States v. Chung*, 659 F.3d 815, 2011 BL 244585 (9th Cir. 2011).

her on the three Section 1831 counts.[43] The district court concluded that ''the government did not prove beyond a reasonable doubt that Jin intended or knew her conduct would benefit the PRC in any way.''[44] The defendant was sentenced to four years in prison and ordered to pay a $20,000 fine.[45] The sentence included a two-level enhancement under U.S.S.G. § 2B1.1(b)(5) (intent that the offense would benefit a foreign government or foreign instrumentality).[46] The Seventh Circuit affirmed the convictions and sentence on appeal.

7. *United States v. Kexue Huang* (S.D. Ind.)

The seventh charged foreign economic espionage case—and fifth individual Section 1831 conviction—involved the misappropriation of trade secrets from the defendant's employer and the transfer of that information to the PRC and Germany for further development.

Between 2007 and 2010, Kexue Huang, a naturalized Canadian born in the PRC, stole proprietary insecticide trade secrets from his employer, Dow AgroSciences, and transferred them to the PRC and Germany for further research.[47] Federal prosecutors successfully recovered some trade secrets in Germany through a Mutual Legal Assistance Treaty request for German law enforcement officials to obtain evidence.[48] Between 2006 and 2010, Huang traveled to the PRC as a part-time professor at Hunan Normal University, where he directed the development of the misappropriated trade secrets. The PRC government also granted funding for this research.[49] After leaving Dow AgroSciences, Huang also misappropriated trade secrets involving ''novel ingredients and process for a food product'' from a subsequent employer, Cargill, Inc.[50]

In June 2010, Huang was indicted on 12 counts of foreign economic espionage and five counts of transportation of stolen property.[51] Huang remained in custody from the time of his arrest through sentencing.[52] In October 2011, two weeks before the scheduled trial, Huang pled guilty to two separate cases filed in two districts: he pled guilty to one count of foreign economic espionage under Section 1831 involving Dow AgroSciences' trade secrets in the Southern District of Indiana, and pled guilty to theft of Cargill's trade secrets under Section 1832 based on charges filed in the District of Minnesota.[53] Huang was sentenced to 87 months in prison—the highest sentence for a negotiated plea agreement for foreign economic espionage to date.

8. *United States v. Elliott W. Doxer* (D. Mass.)

The eighth case is the only foreign economic espionage case involving an undercover sting operation. In June 2006, Elliott Doxer, a Jewish American, emailed the Israeli consulate in Boston, offering to assist the Israeli government in its ''war against our enemies'' by stealing confidential information from his employer, Akamai Technologies, an internet content delivery company handling 15-30% of the world's internet traffic. An undercover agent posing as an Israeli agent contacted Doxer. Doxer never met with the undercover agent in person but communicated with him on multiple occasions. According to court records, Doxer delivered Akamai's confidential information, such as contractual papers, customers and employees over an 18 month period through a ''drop box.''[54]

Doxer was arrested in October 2010 on a wire fraud complaint. He was charged by Information in July 2011, and pled guilty in August 2011 to one count of foreign economic espionage, admitting that he took Akamai's trade secrets without authorization with the intent to benefit the Israeli government.[55] The government asked the court to impose a 36 month sentence and a substantial fine. Instead, the court sentenced Doxer to serve ''a sentence of one year imprisonment'' (which in-

---

[43] *United States v. Jin*, 833 F. Supp.2d 977, 2012 BL 30364 (N.D. Ill. 2012) (No. 08-CR-00192) (Memorandum Opinion and Order).

[44] *Id. at* 1019.

[45] Press Release, U.S. Dep't of Justice, Suburban Chicago Woman Sentenced To Four Years In Prison For Stealing Motorola Trade Secrets Before Boarding Plane For China (Aug. 29, 2012), http://www.justice.gov/usao/iln/pr/chicago/2012/pr0829_01.pdf.

[46] *United States v. Jin*, 733 F.3d 718, 722, 2013 BL 260373 (7th Cir. 2013) (noting sentencing enhancement and affirming sentence; ''Given her egregious conduct, which included repeatedly lying to federal agents (for which she could have been prosecuted but was not), she was fortunate to be the recipient of discretionary sentencing lenity based on her ill health and inability to join her family, now in China.''), *cert. denied*, 134 S.Ct. 1773 (2014).

[47] Huang Sentencing Hearing Transcript, at 17, *United States v. Huang*, No. 10-CR-0102 (S.D. Ind. Dec. 22, 2011) (testimony of Dow AgroSciences managing counsel summarizing investigation); *see also* Press Release, U.S. Dep't of Justice, Chinese National Sentenced to 87 Months in Prison for Economic Espionage and Theft of Trade Secrets (Dec. 21, 2011), http://www.justice.gov/opa/pr/chinese-national-sentenced-87-months-prison-economic-espionage-and-theft-trade-secrets. *Disclosure*: Co-author Mark Krotoski was a member of the prosecution team on the *Huang* case with two other dedicated federal prosecutors and two FBI agents.

[48] *See* Huang Plea Hearing Transcript, at 41-43 (Oct. 18, 2011); Huang Sentencing Hearing Transcript, at 18, 25 (Dec. 22, 2011); and Huang Plea Agreement ¶ 8(D).

[49] Defendant's Memorandum Of Law In Support Of Motion For Revocation Of Detention, 6-7, *United States v. Kexue Huang*, No. 10-CR-0163 (S.D. Ind. Sept. 23, 2010) (No. 42); Huang Plea Agreement ¶ 8(A); Huang Government's Sentencing Memorandum, at 10-11; Huang Sentencing Hearing Transcript, at 23 (Dec. 22, 2011).

[50] Huang Plea Agreement ¶ 9; *United States v. Kexue Huang*, No. 10-CR-312-PAM-AJB (D. Minn.), No. 11-CR-163-WTL-KPF (S.D. Ind.) (as transferred from D. Minn.); Huang Plea Hearing Transcript, at 6-7, 18-19, 47-48 (Oct. 18, 2011).

[51] Press Release, U.S. Dep't of Justice, Chinese National Charged With Economic Espionage Involving Theft Of Trade Secrets From Leading Agricultural Company Based In Indianapolis (Aug. 31, 2010), http://www.justice.gov/criminal/cybercrime/press-releases/2010/huangChar.pdf.

[52] Huang Detention Order, at 11.

[53] Huang Plea Hearing Transcript (Oct. 18, 2011); Huang Plea Agreement; Order (March 8, 2011) (No. 72); *see also* Press Release, U.S. Dep't of Justice, Chinese National Pleads Guilty to Economic Espionage and Theft of Trade Secrets (Oct. 18, 2011), http://www.justice.gov/opa/pr/chinese-national-pleads-guilty-economic-espionage-and-theft-trade-secrets.

[54] Plea Agreement, Agreed Statement of Facts, at 1, 4, 6-7, *United States v. Doxer*, No. 11-CR-10268 (D. Mass. July 20, 2011); *see also* Criminal Complaint, Cromer Aff. at 9, (Oct. 5, 2010); Press Release, U.S. Dep't of Justice, Employee of High Technology Company Charged with Seeking to Provide Confidential Business Information to a Foreign Government (Oct. 6, 2010), http://www.justice.gov/usao/ma/news/2010/October/DoxerEliotPR.html.

[55] Doxer Plea Agreement, *supra* note 54.

   ISSN 0148-7965

cluded six months in prison and six months in home confinement) and imposed a fine of $25,000.[56]

9. *United States v. Walter Liew, et al.* (N.D. Cal.)

The first jury trial conviction for foreign economic espionage involved the misappropriation of pigment manufacturing trade secrets and their subsequent use at PRC-owned companies. The lead defendant Walter Liew was sentenced to 15 years in prison (180 months), the second longest sentence in a foreign economic espionage case after *Chung*.

When Liew learned of the PRC's interest in developing a clean, efficient process for manufacturing chloride-route titanium dioxide (TiO2), a commercially-valuable pigment, he formed a company and assembled a team, including his co-defendants Tze Chao and Robert Maegerle, who were former employees of E.I. du Pont Nemours & Company (DuPont), the top global producer of TiO2. For 10 years (1998-2008), these defendants misappropriated DuPont's TiO2 trade secrets and used them to obtain TiO2 contracts with PRC-owned companies.[57] Co-defendant Hou Shengdong was vice director of the TiO2 project at one such company.

In February 2012, a superseding indictment charged foreign economic espionage and other counts against five defendants: Walter Liew, Tze Chao, Robert Maegerle, Hou Shengdong and Christina Liew. Chao pled guilty in early March 2012, admitting to providing DuPont's TiO2 production trade secrets to PRC-controlled companies.[58]

Liew and Maegerle were tried in a two month jury trial in early 2014 and were convicted on all counts. They were required to pay restitution as well as forfeit their interests in the $27.8 million of illegal profits. Liew was sentenced to 180 months in prison which was based on DuPont's large loss, Liew's self-interested personality and the need to demonstrate that the theft of trade secrets for a foreign government's benefit is a serious crime that threatens America's national security. Maegerle was sentenced to 18 months in prison, drastically less than Liew's sentence given Maegerle's health, age, lack of prior criminal history, productive career and limited knowledge of Liew's dealings with the Chinese government.[59]

Christina Liew's jury trial is scheduled for June 2015.[60] Hou Shengdong was never arrested and remains a fugitive.[61]

10. *United States v. Wang Dong, et al.* (W.D. Pa.)

The most recent foreign economic espionage case charged five Chinese nationals working for a People's Liberation Army intelligence unit with 31 criminal counts based on their alleged hacking of American companies and theft of proprietary information from 2006 through 2014.[62] Since the May 2014 indictment, the defendants have remained in the PRC, so no arrests have been made. They allegedly targeted the IT systems of American companies involved in ''the U.S. nuclear power, metals and solar products industries.''[63] As Attorney General Eric H. Holder Jr. commented:

> This is a case alleging economic espionage by members of the Chinese military and represents the first ever charges against a state actor for this type of hacking . . . . The range of trade secrets and other sensitive business information stolen in this case is significant and demands an aggressive response.[64]

The defendants allegedly used ''spear phishing'' messages to gain access to recipients' computers and then they stole information including emails regarding business strategies, financial positions and production capabilities. This information was then used by state-owned Chinese companies in their business negotiations or litigation with the American targets.[65]

Summary and Conclusion

Overall, despite the unique challenges in prosecuting foreign economic espionage cases, the government has

---

[56] Doxer Sentencing Hearing Transcript, at 5-8, 9-10, 15 (Dec. 21, 2011) (No. 29); Doxer Docket Clerk's Notes (Dec. 19, 2011) (No. 29); *see also* Press Release, U.S. Dep't of Justice, Brookline Man Sentenced for Foreign Economic Espionage (Dec. 19, 2011), http://www.fbi.gov/boston/press-releases/2011/brookline-man-sentenced-to-for-foreign-economic-espionage; Doxer Governnment's Sentencing Memorandum, at 1, 11 (Dec. 16, 2011) (''Elliot Doxer's crime warrants a substantial prison sentence and a fine.'') (No. 28).

[57] Liew Second Superseding Indictment at 2-13, *United States v. Liew*, No. 11-CR-00573 (N.D. Cal. Mar. 12, 2013) (No. 269).

[58] Press Release, FBI, Former DuPont Scientist Pleads Guilty to Economic Espionage (Mar. 2, 2012), http://www.fbi.gov/sanfrancisco/press-releases/2012/former-dupont-scientist-pleads-guilty-to-economic-espionage. The plea agreement remains under seal. *See also* U.S. and Chinese Defendants Charged with Economic Espionage and Theft of Trade Secrets in Connection with Conspiracy to Sell Trade Secrets to Chinese Companies (Feb. 8, 2012), http://www.justice.gov/opa/pr/us-and-chinese-defendants-charged-economic-espionage-and-theft-trade-secrets-connection.

[59] Liew Fourth Amended Judgment (N.D. Cal. Sept. 2, 2014) (No. 9248); Maegerle Judgment (N.D. Cal. Aug. 28, 2014) (No. 921); *see also* Press Release, U.S. Dep't of Justice, Walter Liew Sentenced to 15 Years in Prison for Economic Espionage (July 11, 2014), http://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage.

[60] Docket Clerk's Notes (N.D. Cal. Sept. 2, 2014).

[61] Press Release, FBI, Two Individuals and Company Found Guilty in Conspiracy to Sell Trade Secrets to Chinese Companies (March 15, 2014), http://www.justice.gov/opa/pr/two-individuals-and-company-found-guilty-conspiracy-sell-trade-secrets-chinese-companies.

[62] Indictment, *United States v. Wang Dong*, No. 14-CR-118 (WDPA May 1, 2014) (No. 1), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf. The 31 counts included one for foreign economic espionage and other counts for conspiring to commit computer fraud and abuse, accessing (or attempting to access) a protected computer without authorization to obtain information for the purpose of commercial advantage and private financial gain, hacking, aggravated identity theft, and trade secret theft. Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014) [hereinafter ''Chinese Military Hackers Press Release''], http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

[63] Indictment, at 3, *United States v. Wang Dong et al.*, No. 14-CR-118 (W.D. Pa. May 1, 2014) (No. 1), http://www.justice.gov/iso/opa/resources/5122014519132358461949.pdf; *see also* Federal Bureau of Investigation, Cyber's Most Wanted, http://www.fbi.gov/wanted/cyber/@@wanted-group-listing.

[64] Chinese Military Hackers Press Release, *supra* note 62.

[65] Dong Indictment, at 9-13.

a strong conviction track record, although it has suffered a few setbacks. Convictions have been obtained in eight of the cases, with six cases resulting in Section 1831 convictions. Two other cases (*Jin* and *Serizawa*) involved convictions on alternative charges including trade secret misappropriation and making false statements. Only one case, the *Lee* case, has resulted in the complete acquittal and dismissal of all charges. In two cases, the first and last (*Okamoto* charged in 2001 and *Dong* charged last year), the primary defendants remain at large.

Out of the six Section 1831 convictions, four were based on plea agreements (in the *Fei Ye*, *Meng*, *Huang* and *Doxer* cases). Four of the 10 cases involved trials, of which two were bench trial convictions (*Chung* and *Jin*), one (*Liew*) was a jury trial conviction, and one resulted in an acquittal and dismissal (*Lee)*.

In five cases (*Okamoto*, *Meng*, *Huang*, *Dong* and *Liew*), the trade secret had already been misappropriated outside the United States. In two cases (*Fei Ye* and *Jin*), defendants were stopped at the airport as they were about to depart the country with the trade secrets.

Of the first 10 Section 1831 cases, eight have involved the foreign government or instrumentalities of the PRC. The two remaining cases involved Japan and Israel (*Okamoto* and *Doxer*). Four have been charged in the Northern District of California, which is not surprising given the concentration of trade secrets in Silicon Valley.

On the intent to benefit a foreign government or instrumentality element, most of the cases have focused on an economic benefit (instead of reputational, strategic or tactical benefits). While the statute focuses on the intent of the defendant to benefit a foreign government, two cases have involved evidence of state-sponsored activity (*Jin* and *Dong*).

There has been a wide range of sentences imposed in the cases resulting in convictions. The sentences imposed by the courts have varied due to many factors, including other charges brought in conjunction with the economic espionage charges, the defendant's age, health and social situation, the defendant's intent, motivation and actual use of the trade secret, whether any cooperation was provided to the government for a reduced sentence, and the level of the foreign government's involvement. The sentences have ranged from about one year in the *Doxer* and *Fei Ye* cases, to the sentence of 87 months in the *Huang* case, to the sentencing following trial in *Liew* (180 months) and *Chung* (188 months).

There has been increased attention in recent years on state sponsored efforts to obtain U.S. trade secrets.[66] Recent congressional hearings have focused on the problem of cyber espionage and attacks on U.S. businesses.[67] Against this background, effective enforcement of the Economic Espionage Act will remain an important tool in prosecuting efforts to steal trade secrets with the intent to benefit a foreign government, instrumentality or agent.

---

[66] *See, e.g.*, Statement of FBI Director James B. Comey, Jr., Senate Judiciary Committee, Oversight Of The Federal Bureau Of Investigation, at 4 (May 21, 2014) (listing ''cyber threats from state-sponsored hackers'' as one threat to obtain ''our state secrets, our trade secrets, our technology, and our ideas—things of incredible value to all of us''), http://www.judiciary.senate.gov/imo/media/doc/05-21-14ComeyTestimony.pdf .

[67] *See, e.g.*, Cyber Espionage And The Theft Of U.S. Intellectual Property And Technology: Hearing before the House Comm. on Energy and Commerce Subcomm. On Oversight and Investigations, 1st. Sess. 113th Cong. (July 9, 2013); Cyber Threats From China, Russia, and Iran: Protecting American Critical Infrastructure: Hearing before the House Comm. on Homeland Security Subcomm. On Cybersecurity, Infrastructure Protection, and Security Technologies, 1st. Sess. 113th Cong. (March 20, 2013).

  PTCJ ISSN 0148-7965