Trade Secrets and Economic Espionage:

Legal Risks in Advancing Technology between the U.S. and China



September 16, 2015 Brian A. Sun



Introduction

- Historical Racism and Bias Against Chinese Americans
- Geopolitical Situation between the U.S. and China
- Current Legal Environment
- Recent Federal Prosecutions
- Take-Away Guidance



The Chinese in America

- Despite major economic contributions to America over 160 years, Chinese in America have often faced racism, misunderstanding, bias – even death
- In context of current U.S.-China tensions and competition,
 Chinese Americans today face unique scrutiny, suspicions
- In recent years, a spate of criminal prosecutions have been brought against Chinese Americans focused on trade secrets fact and unlawful acknowledging transfers to China
- These cases have raised serious questions about racial profiling and due process and damage the image of Chinese Americans and their loyalty to the United States of America



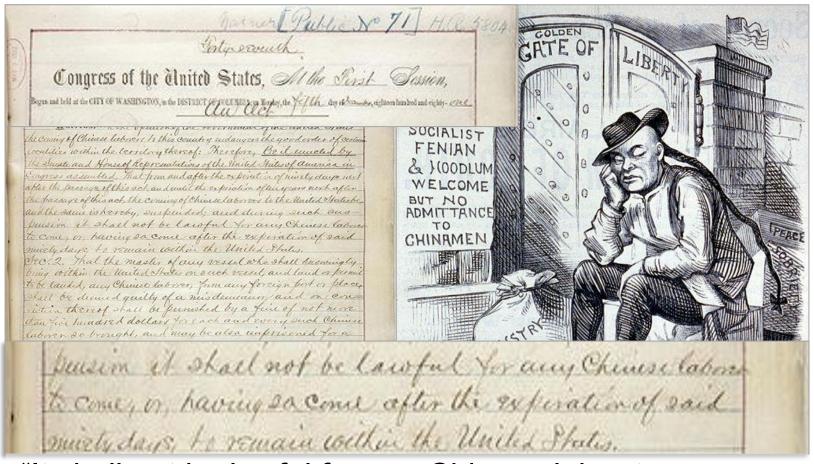
Historical Racism and Bias Against Chinese Americans







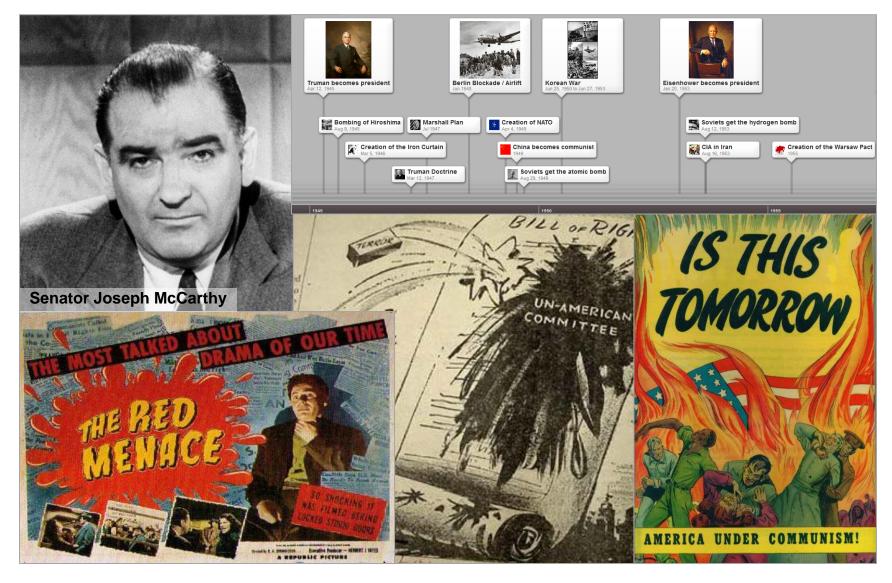
1882 Chinese Exclusion Act



"It shall not be lawful for any Chinese labor to come, or ... to remain within the United States."



The Red Scare





CAMPAIGNSer Scruting



THE NUNS

September 4, 1997

Transcript





One of the beneficiaries of the

rockets could launch America company, Liu Chaoying, is sa military intelligence to the Da

Ms. Liu's involvement was de

nytimes.com/1998/.../how-chinese-wo

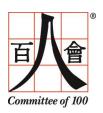
HOW CHINESE WON RIGHTS TO LAUNCH SATELLITES FOR U.S.

By JEFF GERTH and DAVID E. SANGER The New Hork Times SATELLITES FOR U.S. By JEFF GERTH and DAVID E. SANGER What's Popular Now Correction Appended My Man Newt Surge in Free WASHINGTON, May 16-Warren Christopher ended a Administration by initialing a A reconstruction of Mr. Clinton's decision to change the export control rules, based on Department's sharp limits on made satellites aboard Chine Both American industry and interviews and documents, shows that it followed a turf war between the State and been lobbying for years to get inventory of America's most: Mr. Christopher sided with th Commerce Departments, and a broader debate over how to balance America's security his own advisers, who noted could jeopardize "significant concerns and commercial competition in the hottest of all the emerging markets. There was one more reason 1 memorandum. Doing so wot sanctions" imposed when the which is what happened in 10 It also illustrates the intersection of the interests of both large American donors and The Secretary of State's decisi for them to be exported, did r the unusual step of reversing surreptitious foreign donors to the 1996 campaign. Control of export licensing fo Department, then run by Roi American businesses oversea raising strategists. Several lice Both American satellite makers and the Chinese were delighted with the decision because A reconstruction of Mr. Clint interviews and documents, sl the Commerce Department has dual responsibilities: licensing sensitive exports and Commerce Departments, and concerns and commercial cou promoting sales of American goods around the world. It also illustrates the intersect surreptitious foreign donors t Both American satellite make the Commerce Department h One of the beneficiaries of that decision, it now turns out, was China Aerospace because its promoting sales of American

rockets could launch American satellites. An executive of the state-owned Chinese

military intelligence to the Democratic Party in the summer of 1996.

company, Liu Chaoying, is said to have provided tens of thousands of dollars from Chinese



1999 Cox Report

105TH CONGRESS 2d Session

HOUSE OF REPRESENTATIVES

REPORT 105-851

REPORT

OF THE

SELECT COMMITTEE ON U.S. NATIONAL SECURITY AND MILITARY/COMMERCIAL CONCERNS WITH THE PEOPLE'S REPUBLIC OF CHINA

SUBMITTED BY MR. COX OF CALIFORNIA, CHAIRMAN

January 3, 1999 — Committed to the Committee of the Whole House on the State of the Union and ordered to be printed (subject to declassification review)

May 25, 1999 — Declassified, in part, pursuant to House Resolution 5, as amended, 106th Congress, 1st Session

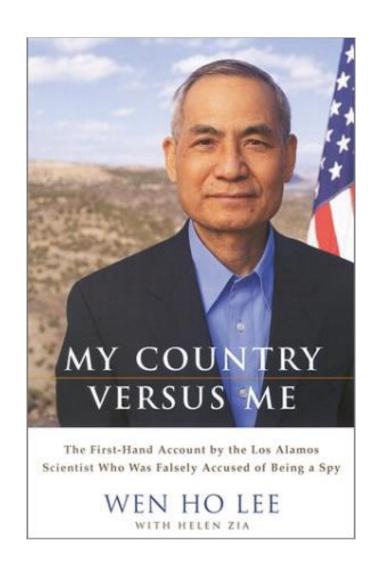
U.S. GOVERNMENT PRINTING OFFICE WASHINGTON: 1999

09-006

A



Dr. Wen Ho Lee, former physicist, Los Alamos National Laboratory, New Mexico





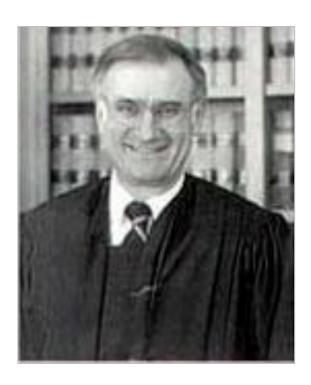
Decision Nears on the Fate Of Ex-Los Alamos Scientist

By JAMES RISEN and DAVID JOHNSTON

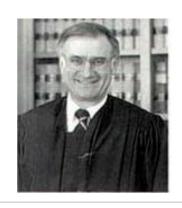
Published: December 8, 1999

ublisied:	December 6, 1999
	Decision Nears on the Fate Of Ex-Los Alamos Scientist By JAMES RISEN and DAVID JOHNSTON Published: 1989 WASHINGTON, Dec. 7— The Federal authorities have intensified their deliberations about whether to prosecute a nuclear weapons scientist at the Los Alamos National Laboratory on charges of PRINT Description to see what your friends are sharing on retires on the PRINT Log In With Facebook What's Popular Now What's Popular Now 10 Best Books of 2011 Central Banks Take Joint
	mishandling highly clatoday. A decision on whether expected within days, 1 Saturday at the White Security, law enforcem The participants conche General Janet Reno de criminal trial would no Among those present is the F.B.I.; George J. Tederal prosecutor in A Law-enforcement offic against Mr. Lee, said the security, alw enforcement offic against Mr. Lee, said the security and
	statutory authority to the officials said. But they seem that the same with the officials said substituted and that she had not given prosecutors final approval. Mr. Lee, his lawyers and his supporters have repeatedly said that he has done nothing wrong and that no one has ever been criminally charged for similar conduct, for example, transferring classified information into a nonclassified computer. Mark Holscher, Mr. Lee's lawyer in Los Angeles, did not return telephone calls today.
	Americal Among those present in addition to Ms. Reno were Samuel R. Berger, President Clinton's country's was inno The high stakes in national security adviser; Energy Secretary Bill Richardson; Louis J. Freeh, the director of Republication of
nytimes.com	As expect which we to a forest serior of federal prosecutor in Albuquerque, who has jurisdiction in the case.





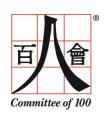




Dr. Lee, I tell you with great sadness that I feel I was led astray last December by the executive branch of our government through its Department of Justice, by its Federal Bureau of Investigation and by its United States attorney for the district of New Mexico, who held the office at that time.

I am sad for you and your family because of the way in which you were kept in custody while you were presumed under the law to be innocent of the charges the executive branch brought against you.

I am sad that I was induced in December to order your detention, since by the terms of the plea agreement that frees you today without conditions, it becomes clear that the executive branch now concedes, or should concede, that it was not necessary to confine you last December or at any time before your trial.

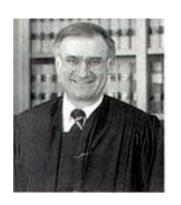




It is only the top decision makers in the executive branch, especially the Department of Justice and the Department of Energy and locally, during December, who have caused embarrassment by the way this case began and was handled. They did not embarrass me alone. They have embarrassed our entire nation and each of us who is a citizen of it.

I might say that I am also sad and troubled because I do not know the real reasons why the executive branch has done all of this. We will not learn why because the plea agreement shields the executive branch from disclosing a lot of information that it was under order to produce that might have supplied the answer.





Although, as I indicated, I have no authority to speak on behalf of the executive branch, the president, the vice president, the attorney general, or the secretary of the Department of Energy, as a member of the third branch of the United States Government, the judiciary, the United States courts, I sincerely apologize to you, Dr. Lee, for the unfair manner you were held in custody by the executive branch.



Geopolitical Situation between the U.S. and China



Chinese Students and the U.S. Science and Technology Workforce



The Chinese in America

- As of 2010 census, approx. four million ethnic Chinese live in the U.S.
- About 25% of all Asian Americans are ethnic Chinese
- Chinese Americans heavily concentrated in 10 major states: CA, NY, HI, TX, NJ. MA, IL, WA, FL, PA
- About 50% of Chinese Americans 1st generation immigrants from China or other Asian countries and 50% born in U.S.
- Almost 40% of adult Chinese Americans have at least bachelor's degree vs. about 22% for U.S. national average



U.S. Colleges and Universities and Foreign Students

- Surging enrollment of Chinese students in U.S. colleges, universities:
 - 2010-11: 157,558 Chinese students (23.5% growth)
 - 2011-12: 194,029 Chinese students (23.1% growth)
 - 2012-13: 235,597 Chinese students (21.4% growth)
- Chinese students currently almost 29% of all foreign students studying in United States (2012-13)

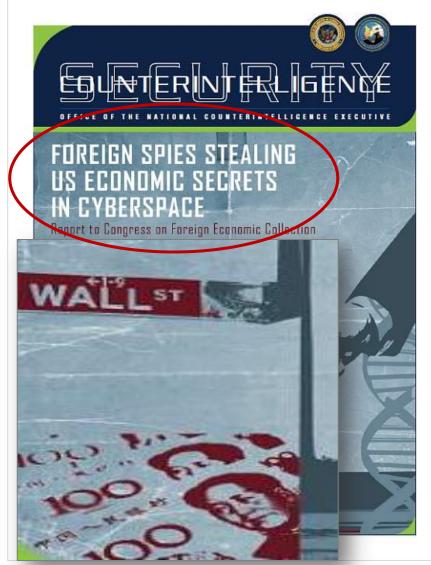


U.S. Colleges and Universities and Foreign Students

- Chinese enrollment now almost evenly divided with 44% in graduate or professional schools, 40% undergraduate
- Chinese students now comprise about 20% of all U.S. engineering students, >11% of all computer/math students

Source: 2011, 2012, 2013 Open Doors Data, Institute of International Education





China: Persistent Collector

Chinese leaders consider the first two decades of the 21st century to be a window of strategic opportunity for their country to focus on economic growth, independent innovation, scientific and technical advancement, and growth of the renewable energy sector.

China's intelligence services, as well as private companies and other entities, frequently seek to exploit Chinese citizens or persons with family ties to China who can use their insider access to corporate networks to steal trade secrets using removable media devices or e-mail. Of the seven cases that were adjudicated under the Economic Espionage Act—both Title 18 USC § 1831 and § 1832—in Fiscal Year 2010, six involved a link to China.



China Singled Out for Cyberspying

U.S. Intelligence Report Labels Chinese 'Most Active' in Economic Espionage; Russia Also Named



Web threats are monitored at Lockheed Martin, also targeted in attacks believed traced to China.

Available to WSJ.com Subscribers



Ford's New SUV Snows Global

Key Obama Backer Off to Slow Start

Bill Burton left the White House with a goal of raising \$100 million for a pro-Obama fund-raising group, alming to mimic the success of recent Sepublican efforts. So far,

WASHINGTON—The U.S. government accused the Chinese of being the world's "most active and persistent" perpetrators of economic spying, an unusual move designed to spur stronger U.S. and international action to combat rampant industrial espionage threatening U.S. economic growth.



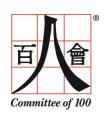


"Many of the organizations comprising China's military industrial complex have both military and civilian research and development functions. This network of government-affiliated companies and research institutes often enables the PLA to access sensitive and dual use technologies or knowledgeable experts under the guise of civilian research and development. The enterprises and institutes accomplish this through technology conferences and symposia, legitimate contracts and joint commercial ventures, partnerships with foreign firms, and joint development of specific technologies."

"As in previous years, China utilized its intelligence services and employed other illicit approaches that involve violations of U.S. laws and export controls to obtain key national security technologies, controlled equipment, and other materials not readily obtainable through commercial means or academia."



Current Legal Environment



Espionage Defined

- Merriam-Webster dictionary definition of "espionage": "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company"
- As definition suggests, espionage can occur in two "forms": "public" aimed at government secrets and "economic" or "industrial" aimed at business secrets
 - Term "espionage" often loosely used without distinction between two forms
- Today <u>BOTH</u> forms of espionage are illegal under U.S. laws, each with heavy penalties
 - Separate criminal statutes for each form
 - Different legal consequences for violations



A Complex Legal System

- United States: probably most complex, costly legal environment in the world
 - Criminal prosecutions (by government)
 - Administrative proceedings (by government)
 - Civil litigation (by either government or private parties)
 - Defense costs, reputational damage
 - Severe disruption of normal work, business relationships
 - Possible effects upon U.S. immigration, naturalization status



A Complex Legal System

- U.S. Government's civil and criminal enforcement tools:
 - Government espionage laws
 - Economic espionage laws
 - Export control laws
 - Computer crime laws



Government Espionage Laws

- Several different, somewhat overlapping statutes that date back to Espionage Act of 1917 and have been amended multiple times in past century
- 18 USC § 793: gathering, transmitting or losing defense information "to be used to the injury of the United States, or to the advantage of any foreign nation"
- 18 USC § 794: gathering or delivering defense information "to be used to the injury of the United States, or to the advantage of any foreign nation"
- 18 USC § 798: disclosure of classified cryptography information "prejudicial to the safety or interest of the United States or for benefit of any foreign government to the detriment of the United States"



Economic Espionage Laws

- Since 1996, federal crimes to steal trade secrets:
 - 18 USC § 1831: Economic espionage for benefit of a foreign government; or
 - 18 U.S.C. § 1832: Economic espionage for benefit of anyone other than its lawful owner
- Reflects recognition of corporate value in intellectual assets and focus on international IP enforcement
- New law added public (criminal) protection to private (civil) right in intellectual property (IP), trade secrets
- § 1831 criminal penalties: up to 15 years in prison and/or \$5,000,000 fine for individuals and higher of \$10,000,000 or 3X value of IP for corporations
- § 1832 criminal penalties: up to 10 years in prison and/or \$250,000 fine for individuals or \$5,000,000 for corporations



What Is a "Trade Secret"?

- Generally speaking, any kind of information that:
 - Has independent economic value,
 - Is not generally known to the public or others who can obtain economic value from its disclosure or use, and
 - Is kept secret through reasonable means
- Examples include proprietary drawings, software, blueprints, formulae, specifications, customer or supplier lists, test data, prototypes, etc.
- Trade secret can be found in any form or media: written, electronic, oral or even in human memory
- Often but not always marked as such in documents
- Often implied by security measures taken: nondisclosure agreements (NDAs), badges, passwords, limited distribution, access controls, physical security, etc.



U.S. Export Control Laws

- Trade embargoes (e.g., Cuba, Iran) administered by the U.S.
 Treasury Department's Office of Foreign Assets Control (OFAC)
- Export Administration Regulations (EAR) administered by the U.S. Commerce Department's Bureau of Industry and Security (BIS)
 - Controls exports of "dual use" technologies
 - Many items exportable to China only under BIS license
- International Traffic in Arms Regulations (ITAR) administered by the U.S. State Department's Directorate of Defense Trade Controls (DDTC)
 - Controls exports of "military" technologies
 - "Policy of denial" = total arms embargo against China



U.S. Export Control Penalties

- Most OFAC embargoes and current EAR apply penalties under International Emergency Economic Powers Act (IEEPA)
 - Civil fine: up to greater of US\$250,000 or 2X transaction value (strict liability regime)
 - Criminal fine: up to US\$1,000,000; up to 20 years in federal prison; or both
- ITAR apply penalties under Arms Export Control Act (AECA)
 - Civil fine: up to greater of US\$500,000 or 5X transaction value
 - Criminal fine: up to US\$1,000,000; up to 20 years in federal prison per violation; or both



U.S. Computer Crime Laws

- 18 USC. §1030: Computer Fraud and Abuse Act ("CFAA")
- CFAA intended to reach <u>all</u> forms of computer crime:
 - (a)(1): illicit access to computer to commit espionage
 - (a)(2): computer trespass to access government, financial, credit or commercial information
 - (a)(3): computer trespass to access government computer
 - (a)(4): fraud through computer trespass to access government, financial, credit or commercial computer
 - (a)(5): damaging government, financial, credit or commercial computer
 - (a)(6): trafficking in stolen computer passwords
 - (a)(7): threatening to damage government, financial, credit or commercial computer



U.S. Computer Crime Penalties

- Criminal penalties include:
 - Fines of up to <u>higher</u> of \$100,000 for misdemeanor or \$250,000 for felony or twice value of loss to victim
 - Imprisonment for up to one year for misdemeanor or up to 20 years for felony
 - Or both fine and imprisonment
- Original law amended in 1992 to provide separate right for victim to sue offender privately in a civil action
 - To bring a private civil CFAA action, victim of crime must allege, prove loss of at least \$5,000
 - "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."



Recent Federal Prosecutions





Department of Justice

SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, TRADE SECRET AND EMBARGO-RELATED CRIMINAL CASES (January 2008 to the present: updated January 23, 2015)

and Customs Enforcement, (ICE)], the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list of cases is not exhaustive and only represents select cases.

Military-Grade Accelerometers to South Korea — On December 19, 2014, Jae Shik Kim, a citizen of South Korea, had his initial court appearance in the Central District of California pursuant to an Indictment charging the defendant with violations of the Arms Export Control Act and the International Emergency Economic Powers Act. According to the indictment, Kim exported military-grade accelerometers from the U.S. to Iran without first obtaining a license. Kim was the president and CEO of Karham Eng., Corp., a company located in Seoul, South Korea. Beginning in December 2007 to March 2010, Kim and Karham conspired with individuals located in China and Iran to procure U.S.-

Below is a brief description of some of the major export enforcement, economic espionage, theft of trade secrets, and embargo-related criminal prosecutions by the Justice Department since January 2008. These cases resulted from investigations by the Homeland Security Investigations (HSI) [formerly Immigration and Customs Enforcement , (ICE)], the Federal Bureau of Investigation (FBI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list of cases is not exhaustive and only represents select cases.

for nersell and others to the detriment of Orbit. Capetier also anegedly worked with Eu



Some Affected U.S. Companies





2012 Export Control Case

- Jian ("Jason") Liang pled guilty to illegal export of 63 L-3 thermal imaging cameras to China without required Commerce Department EAR export licenses
 - Case filed in Central District of California
- Liang made total of seven shipments of cameras to China over 31-month period
- L-3 had advised Liang of applicable U.S. export controls on its cameras
- Liang's sentence: 46 months in prison; 36 months additional supervised probation after release





IBJNEWS

Lilly scientists stole \$55 million in trade secrets, indictment alleges

J.K. Wall October 8, 2013 KEYWORDS ELI LILLY AND CO., FEDERAL GOVERNMENT, GOVERNMENT, GOVERNMENT & ECONOMIC DEVELOPMENT, HEALTH CARE & INSURANCE, LIFE SCIENCE & BIOTECH, MANUFACTURERS, MANUFACTURING & TECHNOLOGY

RELATED NEWS AND OPINION

TechPoint to focus on IT

Three former employees of Eli Lilly and Co. allegedly transferred trade secrets that Lilly values at more than \$55 million to a competing
Chinese drug company, according to an indictment unsealed Tuesday in

U.S. charges 3 NYU researchers in Chinese bribery case

BY NATE RAYMOND AND JONATHAN STEMPEL

NEW YORK | Mon May 20, 2013 6:34pm EDT

0 COMMENTS Tweet Share Share this 8+1 1 Email

RELATED NEWS

Special Report: The Rise and Fall of China's Sun King

Special Report: U.S. cyberwar strategy stokes fear of blowback

Huge cyber bank theft spans 27 countries

Traders charged in bribe scheme with Venezuelan official

him taken into custod

U.S. brings charges in first criminal case for consumer (Reuters) - U.S. authorities brought criminal charges against three New York University researchers on Monday, alleging they conspired to take bribes from Chinese medical and research outfits for details about NYU research into magnetic resonance imaging technology.

Print

A criminal complaint filed in the U.S. District Court in Manhattan charged Yudong Zhu, 44, Xing Yang, 31, and Ye Li, 31, with commercial bribery conspiracy in connection with NYU research financed by the U.S. government.



Criminal Prosecutions

David Yen Lee Stole Trade Secrets From Valspar To Bring To Chinese Competitor

09/1/10 06:58 PM ET Associated Press^{AP}

React

>

CHICAGO — A New Jersey man who was a chemist for a suburban Chicago-based paint company has pleaded guilty to stealing trade secrets.

Federal prosecutors say 54-year-old David Yen Lee of Jersey City, N.J., pleaded guilty Wednesday. They say he admits to stealing formulas and information that was valued at up to \$20 million. He formerly was a technical director at Valspar Corp.

Prosecutors say Lee stole the information from Valspar as he was preparing to work for a competitor in China. Lee formerly lived in Arlington Heights. Federal officials say he stole secret formulas for paints and coatings from Valspar's offices in Wheeling.

Lee is to be sentenced Nov. 23.

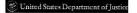


Criminal Prosecutions





Walter Liew Sentenced To Fifteen Years In Prison For Economic Espionage | USAO-ND... Page 1 of 3



THE UNITED STATES ATTORNEYS OFFICE
NORTHERN DISTRICT of CALIFORNIA

Walter Liew Sentenced To Fifteen Years

Northern District of California

FOR IMMEDIATE RELEASE

Friday, July 11, 2014

Walter Liew Sentenced To Fifteen Years In Prison For Economic Espionage

SAN FRANCISCO — Yesterday, Walter Lian-Heen Liew (aka Liu Yuanxuan) was sentenced to serve 15 years in prison, forfeit \$27.8 million in illegal profits, and pay \$511,667.82 in restitution for what the sentencing judge described as a "white collar crime spree" that included violations of the Economic Espionage Act, tax evasion, bankruptcy fraud, and obstruction of justice, announced U.S. Attorney Melinda Haag; John P. Carlin, Assistant Attorney General for National Security at the Department of Justice; David Johnson, Special Agent in Charge of the Federal Bureau of Investigation (FBI), San Francisco Division; and Jose Martinez, Special Agent in Charge of the Oakland Field Office, Internal Revenue Service (IRS), Criminal Investigation.

Liew was convicted on March 6, 2014, after a two month jury trial before the Honorable Jeffery S. White, U.S. District Court Judge, on each of the twenty counts with which he was charged. The jury found that Liew, his company, USA Performance Technology, Inc. (USAPTI), and Robert Maegerle conspired to steal trade secrets from E.I. du Pont de Nemours & Company regarding their chloride-route titanium dioxide production technology and sold those secrets for large sums of money to state-owned companies of the People's Republic of China (PRC). The purpose of their conspiracy was to help those companies develop large-scale chloride-route titanium dioxide production capabilities in the PRC, including a planned 100,000-ton titanium dioxide factory in Chongqing. This case marks the first federal jury conviction on charges brought under the Economic Espionage Act of 1996.

The jury also found that Liew, USAPTI, and Maegerle obstructed justice during the course of their conspiracy. The jury found that Liew filed false tax returns for USAPTI and Performance Group, a predecessor company to USAPTI, and made false statements and oaths in bankruptcy proceedings for Performance Group.

Liew, 56, of Walnut Creek, Calif., originally was indicted in August 2011 and the grand jury subsequently returned two superseding indictments. Liew was convicted of conspiracy to commit

http://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-... 8/24/2015



April 10, 2014

HUFF LOS ANGELES

Dongfan "Greg" Chung, Chinese Spy, Gets More Than 15 Years In Prison

GILLIAN FLACCUS | 02/8/10 04:52 PM ET | AP



SANTA ANA, Calif. — A Chinese-born engineer convicted in the United States' first economic espionage trial was sentenced Monday to more than 15 years in prison for stealing sensitive information on the U.S. space program with the intent of passing it to China.



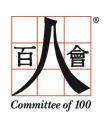
Prosecutors alleged the papers included information about the U.S. space shuttle, a booster rocket and military troop transports.

Before reading the sentence, U.S. District Judge Cormac J. Carney said he didn't know exactly what information Chung had passed to China over a 30-year period. But just taking the "treasure trove of documents" from Boeing Co., a key military contractor, constituted a serious crime, he said.



2010 Economic Espionage Act Conviction

- Dongfan "Greg" Chung, Chinese-born engineer and former Boeing stress analyst possessing high level security clearances, convicted of economic espionage and other charges, for storing allegedly sensitive papers in his home taken from Boeing with the intent to pass it on to China
- The papers in Chung's possession included information related to the space shuttle, booster rockets and military troop transports
- Chung has asserted that he took the information to write books and had no intent to harm national security; no specific evidence was presented what Chung may have sent to China or who received it or how much it "hurt" the United States
- Chung, 74 years old at the time of his sentencing, received a fifteen year jail sentence and has lost his appeals.



2013 "National Security" Case

- Bo Jiang had obtained Ph.D. from Old Dominion University in 2010 and worked as researcher at National Institute of Aerospace (NIA), a research consortium of several southern universities
- After being named by a local Congressman as a potential national security risk, Dr.
 Jiang was terminated by NIA in December 2012 and, with no further work opportunities
 in United States, had purchased one-way ticket home to China in March 2013
- Federal agents arrested him at airport and took him off plane with his laptop computers and digital media
 - Original federal indictment was about Dr. Jiang lying about what he was carrying out of country
- Federal prosecutors then conceded in court he was carrying <u>no</u> classified information, export controlled information or proprietary information – only pornography – on his laptop
- In plea bargain, Jiang pled guilty to misuse of NASA equipment in exchange for dismissal of indictment, so Jiang allowed to leave U.S. within 48 hours



The New Hork Times http://nyti.ms/1P7ACUU

BUSINESS DAY

Accused of Spying for China, Until She Wasn't

ByNICOLE PERLROTH MAY 9, 2015

On Monday, Oct. 20, 2014, Sherry Chen drove, as usual, to her office at the National Weather Service in Wilmington, Ohio, where she forecast flood threats along the Ohio River. She was a bit jet-lagged, having returned a few days earlier from a visit to China. But as she headed to her desk, she says, she had no reason to think it was anything other than an ordinary day. Then her boss summoned her.

Once inside his office, a back door opened and in walked six agents from the Federal Bureau of Investigation.

The agents accused Mrs. Chen, a hydrologist born in China and now a naturalized American citizen, of using a stolen password to download information about the nation's dams and of lying about meeting with a highranking Chinese official.

Mrs. Chen, 59, an adoptive Midwesterner who had received awards for her government service, was now suspected of being a Chinese spy. She was arrested and led in handcuffs past her co-workers to a federal courthouse 40 miles away in Dayton, where she was told she faced 25 years in prison and \$1 million in fines.





Case 1:13-cr-00150-WTL-TAB Document 202 Filed 12/05/14 Page 1 of 2 PageID #: 2097 UNITED STATES DI SOUTHERN DISTRI INDIANAPOLIS UNITED STATES DISTRICT COUF SOUTHERN DISTRICT OF INDIAN 61 INDIANAPOLIS DIVISION UNITED STATES OF AMERICA. proffered for the Court. Plaintiff, UNITED STATES OF AMERICA. If you look at 3142(g)(1), the first factor that Cause 1 Plaintiff. 1:13-CF GUOQING CAO, Indiana SHUYU LI. October Congress has instructed the Court to consider when issuing --2:38 p. Defendants. GUOQING CAO, SHUYU LI, A/K/A "DAN, " ORDER GRANTING LEA When considering the issue of release or detention is the Defendants. This matter having commature and circumstances of the crime. If the superseding Before the Honorable MARK J. DINSMORE Court to dismiss the Second Su OFFICIAL REPORTER'S TRANSCRIP reviewed the motion and being indictment in this case could be wrapped up into one word, the DETENTION HEARING ORDERED AND ADJU dismissal of the Second Supers word would be "traitor." For Plaintiff: Cynthia J. Rid Assistant U.S. United States Suite 2100 The indictment describes individuals who were ORDERED AND ADJUDGED that the Seco 10 West Market 15 entrusted by the company with this work and trusted over the Indianapolis, DISMISSED. course of years, trained by the company over the course of For Guoqing Cao: David J. Hense DONE AND ORDERED in Indianapolis, Ind Pence Hensel, those years to keep these crown jewels, as you heard Mr. Heath Suite 1600 135 N. Pennsyl 18 describe, private, confidential, and restricted, exclusively Indianapolis, WW 19 to Eli Lilly and Company employees and employees with the need For Shuyu Li: Mark L. Newman Hon. Will United St 20 to know. 7722 Susan Dri Southern Indianapolis, 21 What you have before you are individuals who, what Court Reporter: David W. Moxle could be considered traditional intelligence tradecraft, United States 23 carved out a niche and exploited that information that they 46 East Ohio Indianapolis, were entrusted with, exploited the relationships that they garnered through their hosting company, through Eli Lilly's --PROCEEDINGS TAKEN BY AUDIO RECO TRANSCRIPT CREATED BY COMPUTER-AIDED T



The New Hork Times http://nyti.ms/1MhmTct

U.S.

U.S. Drops Charges That Professor Shared **Technology With China**

By MATT APUZZO SEPT. 11, 2015

WASHINGTON - When the Justice Department arrested the chairman of Temple University's physics department this spring and accused him of sharing sensitive American-made technology with China, prosecutors had what seemed like a damning piece of evidence: schematics of sophisticated laboratory equipment sent by the professor, Xi Xiaoxing, to scientists in China.

The schematics, prosecutors said, revealed the design of a device known as a pocket heater. The equipment is used in semiconductor research, and Dr. Xi had signed an agreement promising to keep its design a secret.

But months later, long after federal agents had led Dr. Xi away in handcuffs, independent experts discovered something wrong with the evidence at the heart of the Justice Department's case: The blueprints were not for a pocket heater.

Faced with sworn statements from leading scientists, including an inventor of the pocket heater, the Justice Department on Friday afternoon dropped all charges against Dr. Xi, an American citizen.

It was an embarrassing acknowledgment that prosecutors and F.B.I. agents did not understand — and did not do enough to learn — the science at the heart of the case before bringing charges that jeopardized Dr. Xi's career and left the impression that he was spying for China.



JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE

Tuesday, May 19, 2015

Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China

Chinese Professors Alleged to Have Stolen Valuable Technology from Avago Technologies and Skyworks

Solutions to Benefit a PRC University

On May 16, 2015, Tianjin University Professor Hao Zhang was arrested upon entry into the United States from the People's Republic of China (PRC) in connection with a recent superseding indictment in the Northern District of California, announced Assistant Attorney General for National Security John P. Carlin, U.S. Attorney Melinda Haag of the Northern District of California and Special Agent in Charge David J. Johnson of the FBI's San Francisco Division.

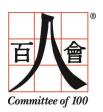
The 32-count indictment, which had previously been sealed, charges a total of six individuals with economic espionage and theft of trade secrets for their roles in a long-running effort to obtain U.S. trade secrets for the benefit of universities and companies controlled by the PRC government.

"According to the charges in the indictment, the defendants leveraged their access to and knowledge of sensitive U.S. technologies to illegally obtain and share U.S. trade secrets with the PRC for economic advantage," said Assistant Attorney General Carlin. "Economic espionage imposes great costs on American businesses, weakens the global marketplace and ultimately harms U.S. interests worldwide. The National Security Division will continue to relentlessly identify, pursue and prosecute offenders wherever the evidence leads. I would like to thank all the agents, analysts and prosecutors who are responsible for this indictment."

"As today's case demonstrates, sensitive technology developed by U.S. companies in Silicon Valley and throughout California continues to be vulnerable to coordinated and complex efforts sponsored by foreign governments to steal that technology," said U.S. Attorney Haag. "Combating economic espionage and trade secret theft remains one of the top priorities of this Office."

"The conduct alleged in this superseding indictment reveals a methodical and relentless effort by foreign interests to obtain and exploit sensitive and valuable U.S. technology through the use of individuals operating within the United States," said Special Agent in Charge Johnson. "Complex foreign-government sponsored schemes, such as the activity identified here, inflict irreversible damage to the economy of the United States and undercut our national security. The FBI is committed to rooting out industrial espionage that puts U.S. companies at a disadvantage in the global market."

According to the indictment, PRC nationals Wei Pang and Hao Zhang met at a U.S. university in Southern California during their doctoral studies in electrical engineering. While there, Pang and Zhang conducted research and development on thin-film bulk acoustic resonator (FBAR) technology under funding from U.S.



Criminal Prosecutions



China jails US geologist for stealing state secrets

Xue Feng, 44, was detained in 2007 after negotiating the sale of an oil industry database to his employers, an American consultancy company.

A Chinese-born American geologist has been sentenced to eight years in jail in China for stealing state secrets.

Xue Feng, 44, was detained in 2007 after negotiating the sale of an oil industry database to his employers, an American consultancy company.

Three Chinese nationals were also sentenced for illegally providing intelligence abroad.

The US embassy said it was "dismayed" and called for his immediate release.

The jail term handed down was described by his lawyer as "very heavy". Mr Xue was also fined 200,000 yuan (£19,500; \$30,000).



Turning the Tables: PRC State Secrets Prosecution

- Xue Feng, a trained geologist and naturalized American citizen, born in the PRC, convicted in 2010 of violating China's "state secrets" laws after obtaining an oil industry database for his employer, a Colorado-based consulting company, IHS energy.
- Xue insisted that the information in question was classified as "state secrets" only after he and IHS purchased the database.
- China's state secrets laws are extremely vague and subject to broad interpretation.
- Finally released by PRC authorities earlier this year after seven and a half years in custody.



Unique Challenges and Risks

- Chinese Americans often work in key science, technology, engineering and mathematics (STEM) fields
 - Often deeply involved with valuable, sensitive technical or business information, both in industry and in government
 - Often only vaguely aware of applicable U.S. laws
- U.S. official reports state that Chinese government and some Chinese companies do seek illicit sources of such valuable information
- Numerous successful federal prosecutions of ethnic Chinese working in U.S., including both guilty pleas and convictions after trial
- For these reasons, U.S. government (and some U.S. employers) may become skeptical or even suspicious
 - Constant added hazards of "racial profiling," bias, and misunderstanding of otherwise innocent conduct



Take-Away Guidance

- Understand and comply with all applicable U.S. laws
 - Espionage laws
 - Export control laws
 - Computer crime laws
- Understand and comply with applicable employer or client non-disclosure agreements (NDAs), IP protection policies and rules
- Understand potential use as "evidence" of whatever is sent or taken to China, whether as employee or personally
 - Emails, text messages, faxes
 - Smart phones, tablets, laptops, flash drives, etc.
- Understand that normal 4th Amendment protection against "unreasonable search and seizure" does <u>not</u> apply to border searches of luggage or carry-on items
 - Any electronic devices or storage media
 - Any papers and documents
 - Any travelers, whether outbound or inbound
 - Any nationality travelers, including U.S. citizens and non-citizens



Take-Away Guidance (cont)

- Beware of potential for becoming ensnared in illegal schemes (or what could <u>appear</u> as illegal schemes)
 - Chinese efforts to obtain U.S. technology illicitly
 - "Private" efforts by individuals to make illicit profits
 - o "Official" efforts by Chinese agents to benefit Chinese military
 - U.S. efforts to "sting" those aiding such Chinese efforts
 - Company efforts to protect internal corporate security
 - Over-zealous investigators or security personnel who already have preconceived notions about "Chinese threat" or who engage in "racial profiling" against ethnic Chinese
- If one becomes aware of a potential scheme or investigation, immediately consult personal counsel for independent legal advice
 - Company counsel is NOT "personal counsel" or independent
 - INTENTIONAL MISCONDUCT WILL LIKELY BE INVESTIGATED AND PROSECUTED TO MAXIMUM EXTENT OF APPLICABLE LAW



Take-Away Guidance (cont)

- Grave risks for such legal violations:
 - Fines
 - Imprisonment
 - Loss of reputation and job (including permanent record of previous criminal activity)
 - Civil litigation and potential exposure for further damages
 - Jeopardy to U.S. visa status
 - Jeopardy to naturalization process toward U.S. citizenship
 - Collateral damage to family members, friends
 - Collateral damage to companies, investors, co-workers
- Best course is to be fully aware of one's legal responsibilities under U.S. law and to avoid conduct that would create potential violation risks or appearance of such risks!



Take-Away Guidance (cont)

Committee of 100

257 Park Avenue South, 19th Fl.

New York, NY 10010

Phone: 212-371-6565

Fax: 212-371-9009

www.committee100.org

THESE MATERIALS AND ANY PRESENTATION BASED THEREON ARE SOLELY FOR GENERAL EDUCATIONAL PURPOSES TO PROMOTE PUBLIC DISCUSSION AND UNDERSTANDING. THEY ARE NOT INTENDED TO BE, AND SHOULD NOT BE TAKEN AS, LEGAL ADVICE. ANYONE WITH A SPECIFIC LEGAL QUESTION SHOULD RETAIN AND CONSULT QUALIFIED LEGAL COUNSEL.

© Committee of 100 2015. All rights retained.