November
2009
Volume 57
Number 5

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Law Clerk
Elizabeth Gailey

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Managing Editor,
United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

Economic Espionage and Trade Secrets

In This Issue

Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases 2
By Mark L. Krotoski

Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and The "Foreign Instrumentality" Element 24
By Thomas Reilly

Common Defenses in Theft of Trade Secret Cases 27
By Thomas Dougherty

Parallel Proceedings in Trade Secret and Economic Espionage Cases . . . 34
By Tyler G. Newby

Identifying and Using Electronic Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases 41
By Mark L. Krotoski

Border Searches In Trade Secret and Other Cases 52
By Evan Williams

Addressing Sentencing Issues in Trade Secret and Economic Espionage Cases. 62
By Christopher S. Merriam

Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases

Mark L. Krotoski
National Computer Hacking and Intellectual Property (CHIP) Coordinator
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

Trade secrets represent one form of intellectual property and are a key part of the innovation process. Trade secrets are important to protect the development of new ideas as well as established information that derives value from not being publicly known. A trade secret can be the product of years of research and development and possibly hundreds of thousands to millions of dollars in production costs. A substantial portion of the United States economy continues to be based on innovation and the development of new technologies and knowledge-based ideas. *See generally*, *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 180 (7th Cir. 1991) (noting "trade secret protection is an important part of intellectual property, a form of property that is of growing importance to the competitiveness of American industry" and that "[t]he future of the nation depends in no small part on the efficiency of industry, and the efficiency of industry depends in no small part on the protection of intellectual property").

A trade secret may take a wide variety of forms. One classic trade secret example is the Coca-Cola soft drink formula. If the formula is revealed, the company could lose its competitive advantage in marketing, producing, and selling the drink product. For software companies, trade secrets may include source codes for the software. If a source code becomes available to others, then third parties can produce the software, or other versions of it, either in the same domestic market or around the world.

The misappropriation of trade secrets can impose severe economic and other harm not only to the owner of the trade secret but on many others. The adverse consequences may affect company employees whose livelihood is based on the continued success of the company, a community dependent on the company contributions to the local economy, or even the health of a particular industry or the national economy.

In other cases, disclosure of a trade secret can harm our national security. Misappropriated technology such as U.S. munitions list materials, which also qualify as trade secrets, in the hands of adversaries may provide a previously unattainable advantage against the United States. Recent convictions have involved misappropriated trade secrets involving military application technology. *See, e.g.*, *United States v. Cotton*, Case No. CR S-08-0042-EJG (E.D. Cal. Feb. 29, 2008) (trade secret plea agreement factual basis noting that "[t]he military applications of these technologies include enhancing navigation and guidance capabilities, radar jamming, electronic countermeasures, and the ability to locate and pin-point enemy signals during warfare"); *United States v. Meng*, Case No. CR 04-20216-JF (N.D. Cal. Aug. 1, 2007) (economic espionage plea agreement factual basis noting misappropriated materials

included "a visual simulation software program used for training military fighter pilots who were utilizing night visual sensor equipment, including thermal imaging"); *see also United States v. Chung*, Case No. SA CR 08-024-CJC (CDCA) ("Under the direction and control of the PRC, Mr. Chung misappropriated sensitive aerospace and military information belonging to his employer, The Boeing Company ('Boeing'), to assist the PRC in developing its own programs.") (bench trial conviction July 16, 2009). As the United States continues its leadership in technology, the protection of trade secrets remains a vital aspect of promoting economic and national security.

In many cases, trade secret misappropriation may be redressed through civil remedies. Most states have enacted some form of the Uniform Trade Secret Act, which was drafted by the National Conference of Commissioners on Uniform State Laws (UTSA). Only four states (Massachusetts, New Jersey, New York, and Texas) have not enacted the UTSA. For a review of issues arising from parallel civil and criminal investigations and cases, see Tyler G. Newby's article, *Parallel Proceedings in Trade Secret and Economic Espionage Cases,* in this issue of the *Bulletin.*

In appropriate cases involving aggravated conduct, criminal prosecution is necessary to deter and punish the misappropriation of a trade secret. Each of the following case scenarios, which are based on prior cases and investigations, highlight different trade secret misappropriation scenarios that a federal prosecutor may be called upon to consider:

- State-sponsored targeting of trade secrets and technology misappropriated with the intent to benefit a foreign government or an instrumentality of a foreign government.
- A trusted employee with access to valuable company information who, after becoming disgruntled, downloads and transmits the information to others outside the company who offer it to the "highest bidder."
- An employee, who after learning how a new prototype is made, decides to form his own company and use the trade secret and other proprietary information to launch his own competing product.
- A competitor who devises a scheme to gain access to company information for use in fulfilling an international contract.
- Employees who execute a plan to steal proprietary information and take it to another country and are stopped at the airport.
- After being offered a senior position with a direct competitor, and before tendering his resignation, an employee uses his supervisory position to request and obtain proprietary information he would not normally be entitled to access. After taking as much proprietary information as he can, he submits his resignation and takes the materials of his former employer to his new position and employer.

This article provides an overview of some of the common issues and challenges in prosecuting trade secret and economic espionage cases. The article reviews the primary objectives of the Economic Espionage Act of 1996; the distinctions between the two offenses under the statute, including economic espionage under § 1831 and trade secret theft under § 1832; the three components of a trade secret; two common investigative scenarios for trade secret and economic espionage; the importance of protective orders during each phase of the prosecution; and some best practices to consider in charging and proving a trade secret case.

II. Primary objectives

A. Closing prior offense gaps

Until 1996, for a substantial class of cases, prosecutors lacked an effective tool to prosecute trade secret misappropriation either committed for personal benefit within the country or for the benefit of a foreign government. A House report described the inability of prior law to reach this conduct:

> The principal problem appears to be that there is no federal statute directly addressing economic espionage or which otherwise protects proprietary information in a thorough, systematic manner. The statute that federal prosecutors principally rely upon to combat this type of crime, the Interstate Transportation of Stolen Property Act (18 U.S.C. § 2314), was passed in the 1930s in an effort to prevent the movement of stolen property across State lines by criminals attempting to evade the jurisdiction of State and local law enforcement officials. That statute relates to "goods, wares, or merchandise." Consequently, prosecutors have found it not particularly well suited to deal with situations involving "intellectual property," property which by its nature is not physically transported from place to place. . . . Other statutes on which the government relies to prosecute this type of crime, such as the mail fraud statute or the fraud by wire statute, have also proved limited in their use. The mail fraud statute is only applicable when the mails are used to commit the criminal act and the fraud by wire statute requires proof that wire, radio, or television technology was used to commit the crime.
>
> State laws also do not fill the gaps left by federal law. While the majority of States have some form of civil remedy for the theft of proprietary economic information, either by recognizing a tort for the misappropriation of the information or by enforcing contracts governing the use of the information, these civil remedies often are insufficient.

H.R. Rep. No. 788, 104th Cong., 2d Sess. 6-7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021. The Economic Espionage Act of 1996 was enacted to close these gaps in the law by providing a new tool for prosecuting the misappropriation of trade secrets in appropriate cases. *See* Pub. L. No. 104-294, 110 Stat. 3488; *see also United States v. Hsu*, 155 F.3d 189, 194 (3d Cir. 1998) (noting before the Economic Espionage Act, "the absence of any comprehensive federal remedy targeting the theft of trade secrets, compelling prosecutors to shoehorn economic espionage crimes into statutes directed at other offenses").

B. Protecting and promoting national and economic security

The Economic Espionage Act of 1996 advances two primary objectives: the protection and promotion of national and economic security.

First, on the national security side, the statute prohibits the misappropriation of trade secrets with the intent to benefit a foreign government, foreign agent, or foreign instrumentality. *See, e.g.*, Hearing before the House Judiciary Subcommittee On Crime, 104th Cong., 2d Sess., at 13-14 (May 9, 1996) (testimony of FBI Director Louis J. Freeh) (noting the inability of existing law to counter state-sponsored targeting of "persons, firms, and industries in the United States and the U.S. Government itself, to steal or wrongfully obtain critical technologies, data, and information in order to provide their own industrial sectors with a competitive advantage" and that "[c]losing these gaps requires a federal statute to specifically proscribe the various acts defined under economic espionage and to address the national security aspects of this crime"); H.R. Rep. No. 788, 104th Cong., 2d Sess. 4 (1996) (noting "threats to the nation's economic interest are threats to the nation's vital security interests").

Second, the statute protects and promotes the nation's economic security. The United States remains a leader in innovation. Trade secrets constitute important innovation assets that are critical to the U.S. economy and to national security. The statute promotes innovation by rewarding protections to trade secret owners who pursue reasonable means to safeguard their trade secrets, and punishing, in appropriate cases, those who misappropriate trade secretes.

In his Senate testimony, then-FBI Director Louis J. Freeh, a key early proponent and architect of the statute, aptly described the significance of promoting and protecting the innovation process to the economic growth of the United States:

> The development and production of intellectual property and advanced technologies is an integral part of virtually every aspect of United States trade, commerce, and business. Intellectual property, that is, government and corporate proprietary economic information, sustains the health, integrity, and competitiveness of the American economy, and has been responsible for earning our nation's place in the world as an economic superpower. The theft, misappropriation, and wrongful receipt of intellectual property and technology, particularly by foreign governments and their agents, directly threatens the development and making of the products that flow from that information. Such conduct deprives its owners-individuals, corporations, and our nation of the corresponding economic and social benefits.

Joint Hearing Senate Select Committee On Intelligence and the Senate Judiciary Subcommittee on Terrorism, Technology, and Government Information, 10-11 (Feb. 28, 1996); *see also* H.R. Rep. No. 788, 104th Cong., 2d Sess. 4 (1996) (noting "the development of proprietary economic information is an integral part of America's economic well-being").

III. Two distinct yet related provisions

The Economic Espionage Act provides two distinct but related offenses. 18 U.S.C. §§ 1831-32 (1996). The first offense, § 1831, applies to economic espionage, which involves the misappropriation of a trade secret with the intent to benefit a foreign government, foreign instrumentality, or foreign agent. Before § 1831 charges may be filed, approval is required by the Assistant Attorney General for the National Security Division. *See* USAM § 9-59.100. For a discussion of the approval process and the necessary factors for prosecution under § 1831, see Thomas Reilly's article, *Economic Espionage Charges Under Title 18. U.S.C. § 1831: Getting Charges Approved and the "Foreign Instrumentality" Element,* in this issue of the *Bulletin*.

The second offense, § 1832, involves the misappropriation of a trade secret with the intent to convert the trade secret to the economic benefit of anyone other than the owner and to injure the owner of the trade secret.

According to the U.S. Attorneys' Manual, some of the factors assessed in initiating an economic espionage or trade secret case include

> (a) the scope of the criminal activity, including evidence of involvement by a foreign government, foreign agent, or foreign instrumentality;
>
> (b) the degree of economic injury to the trade secret owner;
>
> (c) the type of trade secret misappropriated;
>
> (d) the effectiveness of available civil remedies; and
>
> (e) the potential deterrent value of the prosecution.

USAM § 9-59.100. Although the two provisions have different intent elements, both require proof of a trade secret. The elements for these two offenses are summarized in the following table, involving the unlawful possession, receipt, or purchase of a trade secret under § 1831(a)(3) and § 1832(a)(3):

Section 1831(a)(3)	**Section 1832(a)(3)**
1. The defendant intended or knew his actions would benefit a foreign government, foreign instrumentality, or foreign agent	1. The defendant intended to convert a trade secret to the economic benefit of anyone other than the owner
2. The defendant knowingly received, bought, or possessed a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization	2. The defendant knowingly received, bought, or possessed a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization
3. The item/information was, in fact, a trade secret	3. The item/information was, in fact, a trade secret
N/A	4. The defendant intended, or knew, the offense would injure the owner of the trade secret
N/A	5. The trade secret was related to or included in a product that is produced for or placed in interstate or foreign commerce

The Economic Espionage Act applies to a broad range of misappropriation conduct. For example, the misappropriation may involve the execution of a fraud scheme, the downloading and copying of information from a network and transmitting it to others, or the possession of a trade secret knowing that it was obtained without authorization. As a general summary, the following table highlights the forms of misappropriation into five categories by subsection:

Summary	**Subsection Conduct**
Steal/Fraud	(1) Steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information
Copy/Share	(2) Without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys
Possess/Buy	(3) Receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization
Attempt	(4) Attempts
Conspire	(5) Conspiracy

There have been well over 100 trade secret prosecutions around the country. It is anticipated that there will be many more trade secret cases opened in the next several years, in part based on more focused investigatory resources in this area.

Since 1996, six cases have been approved for prosecution under § 1831. Three § 1831 cases have resulted in convictions and two remain active. In the first case filed in the Northern District of Ohio, the lead defendant became a fugitive to Japan. The following table summarizes the six § 1831 cases:

Defendant(s)	**Indictment Date / District**	**Status**
Okamoto and Serizawa	First Indictment (May 8, 2001) (N.D. Ohio)	Lead defendant remains a fugitive
Ye and Zhong	Second Indictment (Dec. 4, 2002) (N.D. Cal.) First Case Conviction (Dec. 14, 2006)	Sentenced Nov. 21, 2008 to 1 year and 1 day (includes § 5K1.1 motion for substantial assistance)
Meng	Third Indictment (Dec. 13, 2006) (N.D. Cal.) Second Case Conviction (Aug. 1, 2007)	Sentenced June 18, 2008 to 24 months (includes § 5K1.1 motion for substantial assistance)
Lee and Ge	Fourth Indictment (Sept. 26, 2007) (N.D. Cal.)	Case pending
Chung	Fifth Indictment (Feb. 6, 2008) (C.D. Cal.) First trial conviction (bench trial) (July 16, 2009)	Bench trial June 2009; conviction July 16, 2009
Jin	Sixth Indictment (Dec. 9, 2008) (N.D. Ill.)	Case pending

IV. Three parts to trade secrets

Both § 1831 and § 1832 cases require proof of a trade secret. Consequently, it is important to understand how a trade secret is established under the Economic Espionage Act. A trade secret, as defined under 18 U.S.C. § 1839(3) (A), (B) (1996), has three parts: (1) information; (2) reasonable measures taken to protect the information; and (3) which derives independent economic value from not being publicly known.

A. Information

Under the first part of the definition, information expansively includes: "all forms and types of financial, business, scientific, technical, economic, or engineering information . . . whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing. . . ." These examples included in the statutory definition are merely illustrative as Congress intended that the "definition be read broadly." H.R. Rep. No. 788, 104th Cong., 2d Sess. 12 (1996); *see also United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998) ("[T]he EEA protects a wider variety of technological and intangible information than current civil laws. Trade secrets are no longer restricted to formulas, patterns, and compilations, but now include programs and codes, 'whether tangible or intangible, and whether or how stored.' ") (citation omitted).

Given the breadth of the trade secret definition under § 1839(3), it is not surprising that there have been a wide variety of trade secrets prosecuted in criminal cases. The following table provides a few examples:

Trade Secret Example	**Case/District/Notes**
Cleveland Clinic Foundation DNA and cell line reagents	*United States v. Okamoto and Serizawa*, No. 1:01CR210 (N.D. Ohio) • First EEA § 1831 case charged • Lead defendant fled to Japan and remains a fugitive
Coca Cola marketing information, product sample	*United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008) (per curiam) (N.D. Ga.) • Three defendants convicted, two by plea agreement, and lead defendant insider convicted at jury trial
Transmeta and Sun Microsystems microprocessor schematics, design methodology, technical information	*United States v. Fei Ye*, 436 F.3d 1117 (9th Cir. 2006) (N.D. Cal.) • First case involving EEA § 1831 convictions; two defendants convicted
Visual simulation source code and software for military aircraft training	*United States v. Meng*, No. CR 04-20216-JF (N.D. Cal. 2009) • Second case involving EEA § 1831 conviction; defendant also convicted of violating the Arms Export Control Act
Space Shuttle Phased-Array, Delta IV Rocket, and C-17 cargo plane documents	*United States v. Chung*, No. SACR 08-00024-CJC (C.D. Cal. 2008) • First trial under EEA § 1831 (bench trial); defendant convicted

Computer-assisted drawing software for airplane parts, including aircraft brake assembly and specifications	*United States v. Lange*, 312 F.3d 263 (7th Cir. 2002) • Affirming bench trial conviction
Confidential information about adhesive product	*United States v. Yang*, 281 F.3d 534 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003) (N.D. Ohio) • Affirming trial convictions
Cost information unavailable to the public, confidential business plan, customer list	*United States v. Martin*, 228 F.3d 1 (1st Cir. 2000) • Affirming trial convictions
Processes, methods, and formulas for manufacturing anti-cancer drug Taxol	*United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998) • Reversing district court's discovery order
Windows source code	*United States v. Genovese*, 409 F.Supp.2d 253 (S.D. N.Y. 2005) • Denying motion to dismiss indictment
"[A]n epoxy-based intumescent fireproofing material" used in paint products known as "Chartek"	*United States v. Zeng*, Criminal Case No. H-08-075 (S.D. Tex May 16, 2008) • Defendant pled guilty to possessing trade secret under § 1832(a)(3)
"[P]lans, designs, specifications, and mechanical parts and hardware for the manufacture and testing of detector logarithmic video amplifiers (DLVAs) and successive detection logarithmic video amplifiers (SDLVAs) which are components used in microwave technologies"	*United States v. Cotton*, Case No. CR S-08-0042-EJG (E.D. Cal. Feb. 29, 2008) • Defendant pled guilty to stealing, downloading, and possessing trade secret under § 1832

B. Reasonable measures

Under the second part of the trade secret definition, the trade secret owner must have "taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3) (1996). The federal statute confers special intellectual protection where the trade secret owner takes certain steps to safeguard the trade secret. As explained in the House Report:

> The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it. It is important to note, however, that an owner of this type of information need only take "reasonable" measures to protect this information. While it will be up to the court in each case to determine whether the owner's efforts to protect the information in question were reasonable under the circumstances, it

> is not the Committee's intent that the owner be required to have taken every conceivable step to protect the property from misappropriation.

H.R. Rep. No. 788, 104th Cong., 2d Sess. 7 (1996). What constitutes reasonable measures will vary with each case. Absolute security measures are not required. *See generally id.* at 12-13:

> The bill requires the owner to take only "reasonable measures" to keep such information secret. The fact that the owner did not exhaust every conceivable means by which the information could be kept secure does not mean that the information does not satisfy this requirement. Rather, a determination of the "reasonableness" of the steps taken by the owner to keep the information secret will vary from case to case and be dependent upon the nature of the information in question.

What constitutes "reasonable measures" is a factual issue that depends on the trade secret that is being protected. For example, different steps are employed to safeguard computer source codes rather than a recipe or formula used in a plant.

Reasonable measures may include a layered or tiered approach. One layer may involve physical security, such as isolating the trade secret to a particular area and limiting access on a "need to know" basis; using security cards to monitor and restrict access; or requiring sign-in sheets to record visitors. Another layer may involve computer or electronic limitations, such as multiple passwords, secure laptops, data encryption, and no remote or internet access in the area where the trade secret is used. As another layer, most companies protect trade secrets through employment policies and practices including employee non-disclosure agreements, marking trade secret and proprietary information as "confidential," training and reminders about the importance of protecting the company trade secrets, employment manuals, and exit interviews upon an employee's departure to ensure proprietary materials have been returned and to underscore confidentiality obligations.

Can the absence of any one measure potentially defeat the "reasonable measures" element? For example, if the company does not employ a common measure such as using confidentiality agreements, are the measures unreasonable? Not necessarily. An objective assessment of all the measures is taken. *See* H.R. Rep. No. 788, 104th Cong., 2d Sess. 7 (1996) (quoted above).

In the trade secret bench trial of an employee who misappropriated computer data from his employer to sell to competitors, the defense argued that the company failed to use confidentiality agreements with its vendors, which meant the protective measures were not reasonable. The Seventh Circuit, in affirming the conviction, rejected the defense argument and found the following 10 measures taken by the company were reasonable:

> [Trade secret owner Replacement Aircraft Parts Co.] RAPCO [a] stores all of its drawings and manufacturing data in its CAD room, which is protected by a [b] special lock, [c] an alarm system, and [d] a motion detector. The [e] number of copies of sensitive information is kept to a minimum; [f] surplus copies are shredded. Some information in the plans is [g] coded, and [h] few people know the keys to these codes. Drawings and other manufacturing information contain [h] warnings of RAPCO's intellectual-property rights; [i] every employee receives a notice that the information with which he works is confidential. None of RAPCO's subcontractors receives full copies of the schematics; by [j] dividing the work among vendors, RAPCO ensures that none can replicate the product. This makes it irrelevant that RAPCO does not require vendors to sign confidentiality agreements; it relies on *deeds* (the splitting of tasks) rather than promises to maintain confidentiality.

United States v. Lange, 312 F.3d 263, 266 (7th Cir. 2002) (emphasis in original). Under an objective

view, the measures used to protect the drawings and manufacturing data satisfied the standard of reasonableness.

C. Independent economic value

The third part of the trade secret definition requires that "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3)(B) (1996). Illustratively, some means to establish this element may include showing: (a) competitive advantages for the owner in using the trade secret; (b) the costs for an outsider to duplicate the trade secret; (c) lost advantages to the trade secret owner resulting from disclosure to competitors; or (d) statements by the defendant about the value of the trade secret.

In continuing with the *Lange* aircraft parts case noted above, the Seventh Circuit concluded this element was established: Every firm other than the original equipment manufacturer and RAPCO had to pay dearly to devise, test, and win approval of similar parts; and the details unknown to the rivals, and not discoverable with tape measures, had considerable "independent economic value from not being generally known." *Lange*, 312 F.3d at 269 (citation omitted).

V. Contrasting two trade secret investigative approaches

In a broad sense, trade secret cases generally develop in one of two ways. Each is distinct and entails different investigative approaches. Different types of evidence may be gathered depending on which scenario applies. While there may be variations, it helps to consider these two common case scenarios as a guide in developing an investigative and prosecution strategy. The first approach allows for gathering evidence as the offense continues to unfold. The second scenario reacts to an imminent misappropriation and possible removal of the trade secret from the country.

A. First approach: undercover, largely prospective investigation

In the first case scenario, the criminal conduct is generally ongoing, allowing for the acquisition of prospective evidence through the use of an undercover investigation or cooperating witnesses. There may be some useful historical evidence of planning and preparation. This scenario allows investigators to assess and determine the scope of trade secret activity, the number of participants, and their distinct roles in the scheme.

One of the best recent examples of this first case scenario is the Coca-Cola trade secrets case that was prosecuted in the Northern District of Georgia. The case involved the misappropriation of Coca-Cola trade secrets by an executive assistant who stole confidential documents and product samples and gave them to a friend with the hope of mutually profiting from the misappropriated materials. *See United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008) (per curiam). Under the scheme, a letter was sent to a senior vice president at Pepsi offering the information to the "highest bidder." Pepsi was immediately suspicious and provided the letter to Coca-Cola which contacted the FBI. At that point, the FBI commenced an undercover investigation and an agent posed as a Pepsi official. The undercover investigation, which lasted about 60 days, allowed law enforcement to determine how many participants were involved and who misappropriated the information and how. There were three participants, which included one insider. Each served a particular role in the scheme.

The agent contacted the phone number listed on the Pepsi letter and spoke with "Dirk," later identified as defendant Dimson, one of the outsiders working with the insider employee. Dimson reported that he "had almost unlimited ongoing access to more confidential information." After further discussion and the exchange of other Coca-Cola documents, Dimson requested some "good faith money." The investigation led to the identification of Coca-Cola employee, Williams. After security cameras were then installed in her work area, she was filmed placing documents and Coca-Cola product samples into a personal bag. A wiretap was placed on Dimson's cell phone. Recordings were obtained involving three defendants, including Williams, Dimson, and Duhaney (a second outsider working with the co-conspirators). The agent met with Dimson at the airport and the meeting was videotaped. During the meeting, the agent provided a $30,000 payment and agreed to provide an additional $45,000 after testing the materials turned over by Dimson, which included a liquid product sample and confidential documents. Coca-Cola confirmed that the materials given to the agent were trade secrets of the company. Dimson e-mailed a list of 20 items he could provide to the undercover agent and negotiated a price of $1.5 million for the items. He requested an additional $11,000 before meeting again. Instead, $10,000 was wired to Dimson's account. Thereafter, the agent met Dimson at a hotel restaurant. After the agent agreed to buy the other documents and product samples for $1.5 million, Dimson was arrested. Duhaney, who stayed outside in a car, was also arrested. Williams was subsequently arrested. Before trial, Dimson pled guilty, and Duhaney pled and agreed to cooperate. Williams proceeded to trial and was convicted. She was sentenced to 96-months' imprisonment. Dimson received a 60-month term. Duhaney, who cooperated, received a 24-month sentence, which included a supervised release provision.

The *Williams* case is a model example of the first investigative approach, which allows for evidence to be gathered prospectively to augment any historical evidence. Based on evidence introduced at trial, the investigators effectively used a variety of traditional investigative techniques to gather evidence, including e-mail search warrants, Title III court-authorized intercepts, videotapes of meetings, security camera footage of the employee insider's desk, surveillance, and other traditional undercover methods. The case only took about 2 months to develop and the investigators were able to learn about the scope and nature of the scheme and the number of participants.

Other trade secret cases involving undercover investigations or cooperating witnesses include *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998) (undercover investigation to purchase processes, methods, and formulas for anti-cancer drug, Taxol); and *United States v. Yang*, 281 F.3d 534, 540-41 (6th Cir. 2002) (after being confronted by the FBI about industrial espionage, consultant agrees to cooperate and assist in the investigation concerning the misappropriation of information about a new adhesive product; investigation included videotape of meetings with the defendants).

B. Second approach: reactive investigation, largely uncovering past events

Under the second case scenario, which is much more common, law enforcement typically learns that the defendant may have misappropriated trade secrets and is leaving the country in 48 hours or may be leaving the company imminently. The following examples, which are based on past investigations, are typical of this second approach:

- The defendant is at the airport and preparing to leave the country when an experienced U.S. Customs and Border Protection Officer notices something unusual and begins asking appropriate questions, revealing misappropriated trade secrets in the defendant's luggage or on the defendant's laptop. *See United States v. Jin*, Case No. CR 04 20216-JF (N.D. Ill. Dec. 9, 2008) (superseding indictment alleging that the defendant "traveled to O'Hare International Airport in Chicago, Illinois, for the purpose of departing to China" and "had in her possession over 1,000 electronic and paper documents belonging to

Company A containing technical information, certain of which were marked as containing confidential and proprietary information belonging to Company A").

- The defendant unexpectedly e-mails his resignation after successfully executing his plan over several prior weeks, unknown to others, to misappropriate trade secrets and other information. The trade secret owner learns just as the employee leaves that he has accessed and downloaded information he was not entitled to have. Law enforcement is contacted.
- The defendant is attending a conference in the United States for 3 days. At the airport, suspected trade secrets are found on his laptop. A decision whether to arrest him or pursue an ongoing investigation must be made before he leaves the country following the conference.
- Based on a tip, investigators learn of the misappropriation just before two defendants are boarding their international plane, requiring a decision on whether to arrest the defendants at the border. A search reveals that the defendants possess suspected trade secrets from four Silicon Valley companies, including technical schematics, information about design methodology, computer aided design (CAD) scripts, microprocessor specifications, and other technology information. *See United States v. Fei Ye*, 436 F.3d 1117 (9th Cir. 2006).

Each of these examples represents a highly reactive case scenario with largely historical and most likely limited evidence. These types of cases present unique challenges. Investigators must respond to a misappropriation that has already occurred when the trade secret has likely left the company or country. There may be little likelihood of obtaining evidence prospectively. As the case unfolds, it is not known whether all of the historical evidence (including planning and preparation) may be uncovered.

In trade secret cases under this scenario, prompt decisions concerning border searches typically are necessary. *See, e.g., Fei Ye*, 436 F.3d at 1119 (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 . . . from defendants' personal luggage, homes, and offices"); *United States v. Meng*, Case No. CR 04 20216-JF (N.D. Cal. Aug. 1, 2007) (plea agreement factual basis stating that after the defendant arrived in the United States "at the Minneapolis St. Paul International Airport on a flight originating from Beijing, the People's Republic of China," with his laptop computer, his "computer was initially viewed by U.S. Customs & Border Protection (CBP) Officers at the airport who noticed that Quantum3D properties were on my laptop," later confirmed to include source code and other company programs and materials "that I had misappropriated from Quantum3D."). For a discussion of legal issues arising in trade secret and other cases involving border searches, please see Evan Williams's article, *Border Searches In Trade Secret and Other Cases*, also found in this issue of the *Bulletin.*

As investigators race to gather evidence, does the unfolding information represent the tip of the iceberg or the whole iceberg? Will a border search be necessary?

C. Contrasting approaches

In sum, these two common scenarios present different investigative and prosecution approaches to trade secret cases. The first scenario may have some useful planning and historical evidence, but there are also opportunities to develop evidence prospectively to learn more about the scope and nature of the misappropriation scheme. Traditional law enforcement techniques, including using an undercover agent or cooperating witness, have proven effective under this first approach. Recorded conversations or video

of key meetings may be important to reveal the defendant's intent to convert a trade secret to the economic benefit of anyone other than the trade secret owner and the intent to injure the owner of the trade secret, required under 18 U.S.C. § 1832(a) (1996), or the intent to benefit a foreign government, necessary under 18 U.S.C. § 1831(a) (1996).

In contrast, under the highly reactive second approach, there may be little opportunity for developing future investigative leads. The misappropriation has typically occurred, and investigators are racing to discover all of the facts. Under this approach, it is often useful to review the defendant's conduct during the preceding weeks. Prior to the misappropriation and departure, a few company officials may have suspected that the defendant was actively engaged in misappropriating trade secrets.

By reviewing the defendant's meetings, phone calls, computer use, and related activity, the plan of misappropriation may be uncovered. Perhaps the defendant engaged in fraud to obtain the trade secrets by making material misrepresentations to access materials he or she was not otherwise entitled to have. The defendant may have asked co-workers to e-mail him trade secrets. A review of his computer may show that he e-mailed the information to an account he controlled outside the company or to co-conspirators outside the company. Review of the defendant's laptop in the weeks prior to his departure may show numerous downloads of information that he was not authorized to have or examination of the computer may reveal that files were downloaded to an external hard drive or thumb drive contrary to company policy.

The strategy for each approach is distinct. While there may be variations of these approaches, these two common scenarios largely highlight the difference between obtaining historical or prospective evidence. There are numerous successful prosecutions around the country under both approaches.

VI. Protective orders

Congress recognized the importance of safeguarding the confidentiality of trade secrets during the investigation and prosecution of trade secret cases. The Economic Espionage Act contains a special provision to protect against the disclosure of trade secret information during the criminal justice process.

Section 1835 provides:

> The court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws. An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret.

See H. Rep. No. 788, 104th Cong., 2d Sess. 13 (1996) ("The intent of this section is to preserve the confidential nature of the information and, hence, its value. Without such a provision, owners may be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth."); *see also United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1998) (noting "the confidentiality provision aims to strike a balance between the protection of proprietary information and the unique considerations inherent in criminal prosecutions").

Protective orders are essential to safeguard the confidentiality of the trade secret during each phase of a criminal case. Three types of protective orders have typically been used, depending on the stage of the prosecution.

- First, a protective order may be required before charges are filed in order to explore a possible pre-indictment resolution of the case.

- Second, after charges are filed but before trial, a protective order is necessary to restrict access to the trade secret solely to the attorneys defending against the charges.
- Third, during a trial, a protective order is used to govern the use of the trade secret during the presentation of the case in a public forum.

To assist and support the prosecution of trade secret and economic espionage cases, the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division has examples of each of these three versions of protective orders, including many examples used in prior cases.

The last sentence in § 1835 provides for an interlocutory appeal "from a decision or order of a district court authorizing or directing the disclosure of any trade secret." If there is any danger of the disclosure of trade secret information during a prosecution, the government may seek immediate judicial review.

An interlocutory appeal has been taken twice under § 1835 since enactment of the Economic Espionage Act in 1996. Both times the government prevailed, though for different reasons. *See United States v. Hsu*, 155 F.3d 189, 203-04 (3d Cir. 1998) (reversing district court order to "select members of the defense team" with access to the documents since the incomplete crimes of attempt and conspiracy did not require actual proof of the trade secret); *see also United States v. Hsu*, 185 F.R.D. 192, 198 & n.19 (E.D. Pa. 1999) (following remand, concluding the defense was not obligated to receive the unredacted documents); *United States v. Fei Ye*, 436 F.3d 1117, 1121 (9th Cir. 2006) (while concluding that the circuit lacked jurisdiction over the § 1835 interlocutory appeal because "all relevant materials had already been turned over" and "the district court's order does not direct or authorize the 'disclosure' of trade secrets as required by the plain language of § 1835," holding that "exceptional circumstances" were established to issue a writ of mandamus directing the district court to rescind its ruling mandating pretrial depositions concerning the trade secrets).

VII. Best practices in charging and proving a trade secret case

Given the three facets of a trade secret, proof that particular information qualifies as a trade secret can present challenges and likely will be tested during the prosecution of the case. In charging a trade secret case, a variety of issues should be considered. Based on past trade secret cases, there are some suggested practices that may help in charging and establishing the trade secret.

A. Consider minimizing public references to the trade secret

As part of an effort to prevent the disclosure of the trade secret information, some steps can be taken at the beginning of the case to minimize public references to the specific name or nature of the trade secret. At a general level, the public documents may refer to the trade secret without providing the particulars. For example, in indictments or other filings, the trade secret may be designated by a more general reference such as confidential information involving the manufacture of widgets or the defendant transmitted trade secrets, that is, file "xyz" or "127B." The defendant has notice of the particular trade secrets based on the discovery, which is covered by a protective order. The public record merely refers to the trade secret in broad or general terms. If necessary, a bill of particulars can provide greater specificity to the defense under Fed. R. Crim. P. 7(f).

In some cases, it may be appropriate to avoid mentioning the victim company by name. For example, the victim company may wish to avoid excessive publicity concerning the misappropriation. Under these circumstances, the indictment may allege the trade secrets belonging to Company A, or a

Company known to the Grand Jury. *See, e.g., United States v. Jin*, Case No. CR 04 20216-JF (N.D. Ill. Dec. 9, 2008) (superseding indictment referring to "confidential and proprietary information belonging to Company A").

These steps can help limit public disclosure about the true nature of the trade secret. The criminal case may proceed, and the defense will receive all the information and discovery necessary to prepare a defense for the case.

B. Confirming reasonable measures taken to protect the trade secret

Prosecutors should work closely with the trade secret owner to ensure that the reasonable measures in place are properly identified before charges are filed. If reasonable measures cannot be shown under the statutory definition, then a trade secret cannot be established to support the charge.

First, consider who would be the best witnesses, if the case went to trial, to explain the trade secret and the reasonable measures employed to protect it. Depending on the case and nature of the trade secret, potential witnesses may include the chief technology officer, chief engineer, or a comparable person with sufficient personal knowledge about the trade secret and the reasonable measures taken to protect it.

Second, carefully consider whether all of the reasonable measures have been identified. Early interviews with the appropriate company witnesses about the reasonable measures can identify the full range of protections in place to safeguard the trade secret. In some cases, it may be appropriate to ask the company official to testify in the grand jury and provide a complete explanation of the trade secret and protective measures. This process will help identify the reasonable measures and confirm whether company policies to protect the trade secret have been used in practice.

Third, as discussed below, if there are close questions presented concerning the proof of reasonable measures, consider conspiracy, attempt, or alternative charges that may be appropriate for the facts of the case. For example, if a fraud scheme was devised and executed to obtain the proprietary information, then mail and wire fraud counts may be warranted. The proof for these alternative charges will not turn on whether reasonable measures were in effect.

C. Identifying the discrete trade secret

Identifying and defining the trade secrets can be important to keep focus in the case and to avoid other unnecessary challenges and issues. In identifying the trade secret(s) to be charged, consider what is unique about the trade secret. Other pre-charging questions to consider may include

- How many distinct trade secrets were misappropriated?
- How do the separate trade secrets relate to one another?
- Were they misappropriated from different places and at different times?
- Were the trade secrets misappropriated all at once or over a period of time?

The misappropriation of multiple trade secrets may show the scope of the defendant's plan and the necessary intent to convert the trade secret to the economic benefit of someone other than the trade secret owner as well as the intent to injure the owner of the trade secret. *See* 18 U.S.C. § 1832 (1996). Instead of stealing the trade secrets from one area, the defendant may have realized that multiple trade secrets or related proprietary information were required to develop or sell the product and compete

against the owner of the trade secret. If multiple trade secrets were misappropriated from different areas in the company, then the case may highlight the efforts necessary to overcome security measures used in separate buildings or areas of the company.

In some cases, the defense may claim that the trade secret was publicly disclosed in a patent application for a new product or process. If there are separate aspects of the trade secret or multiple trade secrets, it may be possible to identify and separate misappropriated trade secrets that were not part of the patent application.

As these brief examples demonstrate, it is important to identify and define the trade secrets to be charged. By doing so, one is more likely to anticipate and overcome defenses, establish the requisite intent, and avoid other unnecessary issues.

D. Role of "integrated" trade secret evidence

It is not uncommon during the execution of a search warrant for agents to find copies of trade secrets along with other related proprietary information. For example, evidence seized during a search may include trade secrets as well as marketing and strategy materials discussing them. Not surprisingly, the defendant may have taken any and all proprietary information related to the trade secrets in addition to the trade secrets themselves. Not all of the proprietary information may meet the trade secret definition under 18 U.S.C. § 1839(3). However, the non-trade secret items nonetheless may be "integrated" or related to the trade secrets and may be useful in prosecuting the case.

Consider the role of "integrated" trade secret evidence and how it will help in the presentation of the case. Some proprietary information may not qualify as a trade secret but nonetheless may have evidentiary value. The integrated trade secret evidence may be included under alternative legal theories (such as unauthorized computer access or wire and mail fraud) or as overt acts as part of a trade secret conspiracy. For example, if a fraud scheme was executed to steal the trade secrets and non-trade secret materials, mail and wire fraud theories do not hinge on whether any or all of the property qualifies as a trade secret. By including the "integrated" evidence in the indictment, the jury will be able to assess the full scope of misappropriated materials and why they were taken.

E. Consider the benefits of charging conspiracy or attempt

For conspiracy and attempt charges, it is now well-settled that it is not necessary to prove the trade secret as part of the case. Sections 1831(a)(4) and 1832(a)(4) both permit attempt offenses. Sections 1831(a)(5) and 1832(a)(5) provide parallel conspiracy provisions. For these inchoate, or incomplete, crimes proof of the trade secret is not required.

The leading case on this issue is *United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998). In *Hsu*, the defendants were charged with attempting to steal trade secrets and conspiring to steal trade secrets, along with other charges. The case was developed as part of an undercover investigation. The defendants were involved in a scheme to purchase processes, methods, and formulas for an anti-cancer drug known as Taxol. The defendants claimed they required disclosure of the specific trade secrets in order to defend against the charges. The Third Circuit disagreed:

> [T]he crimes charged - attempt and conspiracy - do not require proof of the existence of an actual trade secret, but, rather, proof only of one's attempt or conspiracy with intent to steal a trade secret. The government can satisfy its burden under § 1832(a)(4) by proving beyond a reasonable

> doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such.
>
> [T]he Taxol trade secrets in the Bristol-Myers documents are not "material" to the preparation of the defendants' impossibility defense, because proof that the defendants sought to steal actual trade secrets is not an element of the crimes of attempt or conspiracy under the EEA.

Id. at 198, 203, 204; *see also United States v. Martin*, 228 F.3d 1, 13 (1st Cir. 2000) (rejecting defense argument "that he actually received no trade secrets" as "irrelevant" based on charge of "conspiracy to steal trade secrets, rather than the underlying offense"; "The relevant question to determine whether a conspiracy existed was whether Martin intended to violate the statute.").

This legal theory was also used in the successful Coca-Cola trade secret prosecution. Three defendants were charged with one count of conspiring to commit theft of trade secrets, in violation of 18 U.S.C. § 1832(a)(1), (3), and (5). *See United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008) (per curiam). At trial, relying on *Hsu*, the prosecutors successfully argued that it was unnecessary to present direct evidence of or to prove the trade secret. Three other circuits have applied the *Hsu* rationale in trade secret cases. *See United States v. Lange*, 312 F.3d 263, 268-69 (7th Cir. 2002); *United States v. Yang*, 281 F.3d 534, 542-45 (6th Cir. 2002); *Martin*, 228 F.3d at 13.

Another benefit to a conspiracy or attempt charge, as long as the defendant has the intent to commit trade secret theft, is that impossibility is not a defense. *See, e.g., Hsu*, 155 F.3d at 198 (legal impossibility is not a defense to attempted theft of trade secrets or conspiracy to steal trade secrets).

On conspiracy charges under § 1831(a)(5) or § 1832(a)(5), there is a question whether an overt act is required. As with other comparable statutes, arguably it is not. *See, e.g., United States v. Shabani*, 513 U.S. 10, 15-16 (1994) (proof of an overt act is not necessary to prove a drug conspiracy under 21 U.S.C. § 846); *see also Whitfield v. United States*, 543 U.S. 209 (2005) (proof of an overt act is not necessary to prove a money laundering conspiracy under 18 U.S.C. § 1956(h)). In most cases, it is not difficult to charge overt acts, which may be included in an abundance of caution.

F. Role of alternative legal theories

In many trade secret cases, it is useful to include alternative legal theories. By using alternative charges along with trade secret charges, the jury will have a full picture of the conduct, including each phase of the planning and preparation, misappropriation, and possible intended use or actual use of the trade secret. In some trade secret and economic espionage cases, alternative charges have been used to commence the case while the investigation continues to develop the trade secret facts.

The statute expressly recognizes that other legal remedies may be appropriate. The Economic Espionage Act states that it does not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret." 18 U.S.C. § 1838 (1996).

Another benefit of using alternative charges is that proof of the trade secret is not essential. This may be important, as noted above, where "integrated" trade secret evidence is involved. For example, if the materials were misappropriated under a fraud scheme, a mail or wire fraud theory would cover the misappropriation of "property," which may include trade secrets and other proprietary information and materials.

Illustratively, one case involving related charges concerned an employee at a manufacturer of veterinary diagnostics products in Maine who provided trade secret information including cost information, a confidential business plan, a customer list, and other information, to a chief scientific

officer at a company in Wyoming. The prosecution involved a host of legal theories that were affirmed on appeal. *See Martin*, 228 F.3d at 13-18 (affirming conspiracy to commit trade secret theft, conspiracy to transport stolen goods interstate, and mail fraud and wire fraud counts under both property and honest services theories).

In considering possible alternative charges, it helps to focus on each phase of the misappropriation, including any planning and preparation, the manner in which the trade secrets were misappropriated and transferred, any intended or actual use of the trade secret, and the defendant's role and responses in the misappropriation scheme.

Planning phase: In the planning phase, these factors may be useful to consider for alternative charges:

- Was the misappropriation planned or opportunistic? Was the defendant simply at the right place at the right time to steal something of value, such as a contractor, or did an insider execute a scheme to take the trade secret and related materials?
- What requests for the trade secret and related information were made before the defendant's departure or resignation?
- How many others participated in the plan for misappropriation? Did an insider coordinate with outsiders?
- What offers of money or employment were made before the defendant's departure or resignation?
- Did the defendant become disgruntled with his or her employer?
- Are there any other motivating factors?

Manner of misappropriation phase: Another related area concerns how the trade secret information and any related materials were misappropriated. In some cases, it may not be possible to determine specifically how the trade secret was misappropriated. For example, the investigation may show the defendant employee was found to possess trade secrets he was not entitled to access, but it may not be clear how he came to possess them. Issues to consider concerning the manner of the misappropriation may include

- What barriers were overcome?
- How was information/material stolen?
- What access did the defendant have to the area where the trade secrets were maintained?
- Was a computer used to access the trade secrets?

Manner of transfer phase: Another key phase to consider involves the manner in which the trade secret was transferred. For example, after the trade secret was misappropriated, how was it transferred either outside the company or to co-conspirators? The defendant may have used a company computer to e-mail the trade secret to an account he or she controls or to another outsider. For this phase, some areas to consider include

- Were the trade secrets transported across state lines or in foreign commerce, which would support a Foreign/Interstate Transportation of Stolen Property theory?
- Do import or export violations apply?
- Was a computer used to download, upload, or transmit the trade secret?

Manner of use phase: The investigation may highlight a use phase in the case. After the misappropriation, how did the defendant intend or actually use the trade secret?

- What is the evidence of actual use or disclosure of the trade secret to others?
- Was there a plan of competition with the owner of the trade secret?
- Was the trade secret provided directly to a competitor?
- What steps, if any, were taken to establish a competing company? Did the defendant form a new corporation with others to produce the trade secret and compete with the owner of the trade secret?
- Have business plans been identified?
- Did the defendant seek funding proposals from others to develop the product?
- What was the planned use or purpose for misappropriating the trade secret?
- Was the trade secret misappropriated to fulfill another contract?
- Was the trade secret misappropriated with the intent to benefit a foreign government, foreign agent, or foreign instrumentality (which would support a Section 1831 violation)?
- Was the trade secret misappropriated for profit (the economic benefit of anyone other than the trade secret owner)?

Defendant's role/responses: In considering appropriate charges, it also helps to focus on the defendant's role in the misappropriation scheme. Many trade secret cases involve a division of labor with distinct roles fulfilled by the co-conspirators. An insider may have exclusive access to the trade secret, but may depend on others to develop or produce it. Or one defendant may have the technical expertise concerning the trade secret but lack the ability to fund, develop, and market the product. A conspiracy theory may highlight the contributions and role of each co-defendant in the misappropriation scheme.

Summary of possible alternative charges: Based on the distinct phases involved in the misappropriation, the following table summarizes possible alternative legal theories, in addition to others depending on the facts of the case, that may be appropriate to consider:

Offense	**Statute/Notes**
Economic Espionage	18 U.S.C. § 1831 (1996) • In a Section 1831 case, it may be appropriate to charge the misappropriation of trade secrets under Section 1832, since proof of the trade secret is required for both Sections 1831 and 1832
Theft Of Trade Secret	18 U.S.C. § 1832 (1996) • How many trade secrets were misappropriated and how do they relate to one another?

Unauthorized Disclosure of Government Information, Including Trade Secrets, by a Government Employee	18 U.S.C. § 1905 (2008) • Misdemeanor offense applies to federal officer or employee (or other designated official under the statute)
Arms Export Control Act, and the International Traffic in Arms Regulations (ITAR)	22 U.S.C. § 2778 (2004), 22 C.F.R. § 120 (2006) • Do the trade secrets also constitute U.S. Munitions List items that may not leave or enter the United States without prior permission of the Secretary of State? • *See, e.g., United States v. Reyes*, 270 F.3d 1158, 1169 (7th Cir. 2001) ("Conviction on this count required that the government prove beyond a reasonable doubt that Reyes willfully exported or attempted to export an item on the United States Munitions List without having first obtained a license.")
Computer Fraud and Abuse Act Fraud Scheme	18 U.S.C. 1030(a)(4) (2008) • Was a computer used to further a fraud scheme, such as obtaining trade secrets and related materials by misrepresentations?
Unauthorized Obtaining of Information	18 U.S.C. § 1030(a)(2)(C) (2008) Was a computer used to obtain unauthorized access to the trade secrets and related materials?
Intrusion	18 U.S.C. § 1030(a)(5) (2008) • Were the trade secrets obtained by hacking into a network?
Mail/Wire Fraud	18 U.S.C. §§ 1341, 1343, 1346 (2008) • Were the trade secrets obtained as part of a fraud scheme through the use of the mails or an interstate wire communication? • *See, e.g., United States v. Martin,* 228 F.3d 1, 16-18 (1st Cir. 2000) (affirming conspiracy to commit trade secret theft and mail fraud and wire fraud counts under both a property and honest services theories) • *See also* 18 U.S.C. § 1346 ("For the purposes of this chapter, the term 'scheme or artifice to defraud' includes a scheme or artifice to deprive another of the intangible right of honest services.")

Foreign/Interstate Transportation of Stolen Property	18 U.S.C. § 2314 (1994) • Was the stolen trade secret transported across state lines or exported from the country? • *See, e.g., United States v. Martin,* 228 F.3d 1, 13-15 (1st Cir. 2000) (affirming conspiracy to commit trade secret theft and conspiracy to transport stolen goods interstate)
Money Laundering	18 U.S.C. §§ 1956, 1957 (2009) • Depending on the charges (such as wire or mail fraud), if the act or activity constitutes "specified unlawful activity" under Sections 1956(c)(7) and 1961(1), then money laundering theories may apply
False Statement	18 U.S.C. § 1001 (2006) • Did the defendant make false statements to the agents during the course of the investigation?
Obstruction Of Justice	18 U.S.C. §§ 1505 (2004), 1512 (2008), 1519 (2002) • Was evidence destroyed or concealed or did witness tampering occur with the intent to impede a pending or future investigation? • Note: Section 1519 applies to both pending and future investigations ("in relation to or contemplation of any such matter or case")
Forfeiture	18 U.S.C. § 1834 (2008) (forfeiture provision in trade secret and economic espionage cases) 18 U.S.C. § 982(a) (2007) (common criminal forfeiture provision)

VIII. Conclusion

Economic espionage and trade secret cases can be among the more challenging and rewarding cases handled by a federal prosecutor. Some of the challenges may involve identifying key evidence and witnesses abroad. Prompt decisions in the case may be required before the defendant boards an international flight or before the investigation may be fully completed. Border search decisions may be necessary. Because the misappropriation may have been discovered after the defendant left the company or country, much of the evidence involved in the offense may be limited or no longer readily available.

Notwithstanding these and other challenges, economic espionage and trade secret cases are important for promoting the objectives of the statute: protecting and promoting national and economic security. In appropriate cases, criminal trade secret prosecution can punish the wrongdoer in the particular case and send a message of deterrence to others contemplating similar conduct.

This article has surveyed some of the common issues that may arise in these cases. The Computer Crime and Intellectual Property Section has experience handling trade secret cases and has developed a library of materials to assist other prosecutors, including sample indictments, protective orders, opposition briefs, and trial and appeal briefs. CCIPS can be reached at (202) 514-1026.❖

ABOUT THE AUTHOR

❑ **Mark L. Krotoski** presently serves as the National Computer Hacking and Intellectual Property (CHIP) Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. He previously served as Deputy Chief and Chief of the Criminal Division in the U.S. Attorney's Office for the Northern District of California and as a CHIP Prosecutor in the U.S. Attorney's Offices for the Northern and Eastern Districts of California.✠

Economic Espionage Charges Under Title 18 U.S.C. § 1831: Getting Charges Approved and The "Foreign Instrumentality" Element

Thomas Reilly
Senior Trial Attorney
Counterespionage Section
National Security Division

Title 18 of the United States Code, § 1831, provides that any person who steals or without authorization misappropriates, possesses, copies, or obtains a trade secret, with the knowledge or intent that such theft or misappropriation would benefit a foreign government, foreign instrumentality, or foreign agent, is subject to imprisonment and a fine. Such an act is commonly referred to as economic espionage, and this provision is part of the Economic Espionage Act, 18 U.S.C. § 1831 (1996).

Before any person can be charged with economic espionage by complaint, information, or indictment, or if § 1831 charges are the predicate offense for any other charges such as money laundering or fraud, the Assistant Attorney General (AAG) for the National Security Division (NSD) must approve the action. Once charges are brought, the AAG must be consulted prior to any plea resolution or dismissal of any § 1831 charges. USAM 9-59.100. To obtain this approval, the prosecutor should contact the Counterespionage Section (CES) of the NSD. The best practice is to contact CES early on in an investigation and to consult with CES at all significant stages of investigation of a § 1831 offense, including grand jury subpoenas, search warrants, or electronic surveillance. If a foreign nexus to a trade secret theft is suspected, CES should be contacted immediately. CES attorneys work closely with United States Attorneys' offices and law enforcement agencies across the country to investigate and prosecute these offenses.

In a typical case, the first step in obtaining approval of § 1831 charges begins with a prosecution memo from the Unite States Attorney's office to CES. CES reviews this memo and the totality of the case with the United States Attorney's office and the applicable law enforcement agency. After that review, a formal recommendation setting forth the evidence establishing each element of the offense is sent to the AAG along with the prosecution memo and any other materials necessary for the AAG to review. CES reviews the charges and the evidence with the AAG and issues follow up questions addressing any potential issues or problems with the case. Once the AAG approves the charges, CES advises the United States Attorney's office.

The primary purposes of the requirement of NSD approval are to ensure that any United States Intelligence Community equities are properly examined, that any other investigations or intelligence operations will not be adversely impacted, and to identify any classified information discovery issues that may present themselves if charges are brought. Additionally, CES will also work closely with the United States Attorney's office to determine whether other charges, such as export control violations, are applicable, and whether charges can be brought against foreign companies or persons overseas. AAG approval is required in economic espionage cases to make certain that these issues, as well as any

potential broader national impact from the charges, are weighed and addressed prior to bringing charges. As discussed below, an economic espionage charge not only is a charge against a particular defendant but also may implicate a foreign nation in the theft of the trade secrets, the seriousness of which cannot be overstated.

Due to the nature of the charges, the primary focus of the CES review is the foreign nexus in the case, specifically any evidence that the defendant knew or intended that his actions would benefit a foreign government, instrumentality, or agent. It is important to note that the focus of the CES inquiry, and the required proof at trial, is on who will benefit from the offense, not who stole the trade secret. Consequently, it is not necessary that the defendant be associated with the intended beneficiary. All that is necessary is that the intent or knowledge to benefit a foreign government, instrumentality, or agent is provable.

The most straightforward cases in this regard will be those cases where the defendant knew or intended to benefit a foreign government or foreign agent. While the statute does not define "foreign government," the term is defined elsewhere in the United States Code as any foreign country, whether recognized by the United States or not. *See, e.g.,* 18 U.S.C. § 1116 (1996). A foreign agent is defined in the statute as "any officer, employee, proxy, servant, delegate, or representative of a foreign government." 18 U.S.C. § 1839 (2) (1996). It is important to remember that the foreign agent is an agent of the government, not an agent of a foreign instrumentality.

The more difficult cases arise when the intended benefit is to accrue to a foreign instrumentality. As cases move away from a benefit to a foreign government or agent, the class of entities that will be covered by the statute enlarges and can include a business, a research institute, or a non-governmental organization. Consequently, greater scrutiny will apply when a benefit to a "foreign instrumentality" is charged rather than benefit to a foreign government or agent. What is a "foreign instrumentality" for purposes of securing charges and a conviction under 18 U.S.C. § 1831? There is no case law interpreting this term; however, foreign instrumentality is defined as "any agency, bureau, . . . component, institution, association, or any legal, commercial, or business organization, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. §1839 (1) (1996). The legislative history states that "substantially" does not mean complete control, but rather "material or significant," not "technical or tenuous" control. The test is not meant to be "mechanistic or mathematical." 18 U.S.C. §1839 (1996). By example, the simple fact that a foreign government owns a majority of stock in a corporation will not suffic—nor will the fact that a government owns only 10 percent of a corporation make it exempt from scrutiny. The "pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government *directed*." 142 Cong. Rec. S12212 (daily ed. Oct. 2, 1996) (emphasis added).

The purpose behind the expansion of the intended beneficiaries beyond foreign governments and foreign agents is to preclude evasion of the statute by foreign governments hiding behind corporate or other shell entities. An analysis of proof regarding a foreign instrumentality requires a lot of investigation into the structure, function, operation, personnel, and conduct of the instrumentality and its business and relationship with the foreign government. Proving that the benefit was intended for a foreign instrumentality is more complicated than proving that the benefit was intended for a foreign government. Generally, the same facts and inferences will support a theory of the case that the theft was conducted with the intent to benefit a foreign government as well as the foreign entity. This evidence comes in many forms, primarily from a defendant's own statements and documents, a money trail, public records, a mutual legal assistance treaty, letters rogatory, evidentiary requests, and expert witnesses who

can explain the relationship among foreign entities and how the foreign government can benefit from the offense.

Once the intended beneficiary has been identified, be it a foreign government, instrumentality, or agent, what type of benefit must you prove to bring charges and secure a conviction? As with the definition of foreign instrumentality, there is no case law to guide this determination. Fortunately, the legislative history is particularly clear on this point. The benefit is to be interpreted broadly and can include economic, strategic, reputational, or tactical benefits. H. Rep. No. 788, 104th Cong., 2nd Sess. (1996). The cases that have been charged to date have focused primarily on an economic benefit, which is the easiest to prove and explain at trial. However, given the importance of the statute and the importance of protecting national security and economic well being, all manner of benefits will be examined to support charges in a particular case.

Protecting the nation's trade secrets is of critical importance to national security and overall economic well-being, and prosecuting § 1831 offenses is an important tool to protect these secrets. CES will continue to work to ensure that charges are appropriately and aggressively pursued.❖

ABOUT THE AUTHOR

❑ **Thomas Reilly** is a Senior Trial Attorney in the Counterespionage Section of the National Security Division. He has been with the Counterespionage Section since 2002 and has investigated and prosecuted espionage, economic espionage, and export control violations, as well as cases involving the unauthorized possession or disclosure of classified information. He also lectures at the National Advocacy Center on the use of classified information in criminal cases. He was previously a Trial Attorney in the Civil Division and in private practice in New York.✠

Common Defenses in Theft of Trade Secret Cases

Thomas Dougherty
Trial Attorney
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

This article identifies and responds to some of the most common defenses raised in trade secret theft and economic espionage cases. As with any case, but especially with Economic Espionage Act (EEA) cases, prosecutors must understand and evaluate the potential defenses early. This review is important because trade secret thefts may oftentimes be more appropriately tried in civil court and an evaluation of potential defenses will assist in determining the appropriate forum. This article reviews and highlights some useful lessons from recent trade secret cases. In particular, six common defenses are considered.

II. Common defenses

A. The "tool kit" defense

The EEA does not restrict competition or lawful innovation. According to the First Circuit, the EEA "was not designed to punish competition, even when such competition relies on the know-how of former employees of a direct competitor. It was, however, designed to prevent those employees (and their future employers) from taking advantage of confidential information gained, discovered, copied, or taken while employed elsewhere." *United States v. Martin*, 228 F.3d 1, 11 (1st Cir. 2000).

Will the defense seek to claim some "plausible" reason why the trade secrets were possessed and removed from the company? This issue arose in *United States v. Shiah*, No. SA CR 06-92 (C.D. Cal. Feb. 19, 2008) (unpublished), *available at* http://www.cacd.uscourts.gov/CACD/RecentPubOp.nsf/ecc65f191f28f59b8825728f005ddf4e/37d207fcb9587a30882573f400620823/$FILE/SACR06-92DOC.pdf. The District Court for the Central District of California found the defendant not guilty of theft of trade secrets in an unpublished Findings of Fact and Conclusions of Law. The court concluded that the government had established all the elements in the case beyond a reasonable doubt with one exception. The opinion noted, "While the Court finds that the evidence makes it more likely than not that Shiah intended to convert trade secrets in these files, satisfying a preponderance standard, Shiah's explanation for his actions are sufficient to create a reasonable doubt."

Consequently, the court held that the government failed to prove beyond a reasonable doubt that the defendant intended to convert the trade secrets to the economic benefit of someone other than the owner. Although an unpublished decision, the case is instructive because the fact pattern is similar to the situation presented by many other theft of trade secret and economic espionage cases, where an employee steals trade secret information just prior to leaving to take a new job.

The defendant in *Shiah* copied 4,700 computer files belonging to his employer, Broadcom, to an external hard drive shortly before leaving to start a new job with a competitor. At trial, the defendant

testified that, as was his custom when leaving one job for another, he downloaded all files relating to his work so that he would have a "tool kit," or a reference library, of his work files to draw upon in his future work.

The Broadcom files the defendant downloaded contained both trade secret information and non-confidential information. The defendant testified that he intended to use only the information in the files that was not confidential to Broadcom.

The government presented evidence that Shiah accessed some Broadcom files while at his new job, but could not show which information within the files—trade secret or not—that Shiah accessed. The court found that the government failed to prove the element of Shiah's intent to convert the trade secrets to the economic benefit of someone other than Broadcom. The court noted that the documents were obtained in the normal course of Shiah's employment at Broadcom and related to Shiah's work at his old job, and the court concluded that there was nothing suspicious about the way the defendant initially obtained the documents. The government argued that Shiah's actions in copying files prior to leaving Broadcom indicated that he was trying to gather as many trade secrets as possible and intended to convert trade secrets to his own benefit. The court found that the defendant's actions were consistent with his explanation that he compiled a "tool kit" of information in downloading the body of his work at Broadcom so that he could use the nonconfidential information in the future. The court also focused on the fact that there was no evidence that the defendant attempted to delete any of the files from his Broadcom laptop and that he accessed thousands of files on a particular day. The court also found that there was no evidence that Shiah had provided any trade secret information to his new employer once he started his new job. The court cited all of these factors as support for Shiah's argument that he took all of these files as part of his "tool kit" and not with the intent to economically benefit someone other than the owner of the trade secrets.

While the *Shiah* case was a bench trial, it is interesting to query whether a jury would have reached the same result. After all, the court held that all the elements in the case were met, save one which was not met by a narrow margin.

This case highlights the need to ask several questions in these cases: When did the employee access the trade secret information? Did the employee take information that they did not work on during their employment at the former company? Did they access information that they did not have authority to obtain while working at the company? Was any of the stolen trade secret information provided to another person at a new company or to a representative of a possible new employer? While use of a misappropriated trade secret is not required, what evidence supports the defendant's intent to convert the trade secret and intent to injure the owner of the trade secret? Answering all of these questions should provide a good indication whether the "tool kit" defense may possibly be successful.

B. Knowledge of trade secret

Another very common tactic of defendants in trade secret theft cases is to claim that they did not know that the information that they misappropriated was in fact a trade secret and that the government must prove this under the statute. However, the government is not required to prove the defendant specifically knew that the misappropriated information was a trade secret. Knowledge of illegality of one's conduct, in essence a willfulness standard, is not an element of proof for trade secret theft under the EEA and is not supported by the plain language of the statute, legislative history, or case law. The government need not prove that a defendant himself had concluded that the information taken fit the legal definition of a "trade secret" set forth in 18 U.S.C. § 1839(3).

First, the plain language of the statute sets forth three mens rea requirements: the government must show the defendant, "[1] with intent to convert a trade secret . . . to the economic benefit of anyone other than the owner thereof, and [2] intending or knowing that the offense will injure any owner of that trade secret, [3] knowingly" engaged in misappropriation. 18 U.S.C. § 1832(a). Nothing in the language of the statute suggests that the government must allege and prove that the defendant acted with knowledge that his conduct was unlawful or with the intent to violate the law. This is the heightened willfulness standard, as required in criminal tax fraud, criminal copyright infringement, and certain money laundering charges. *See, e.g., Cheek v. United States*, 498 U.S. 192, 201 (1991) (criminal tax evasion). Instead, the Supreme Court has held that, "unless the text of the statute dictates a different result, the term 'knowingly' merely requires proof of knowledge of the facts that constitute the offense." *Bryan v. United States*, 524 U.S. 184, 193 (1998).

Moreover, the legislative history does not support a heightened knowledge standard. In enacting the statute, Congress explained that:

> *It is not necessary that the government prove that the defendant knew his or her actions were illegal*, rather the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and that the defendant *knew or should have known* that fact.

H. Rep. No. 788, 104th Cong., 2d Sess. 12 (1996) (emphasis added), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031; 142 Cong. Rec. 27,117 (1996).

The legislative history also specifically discusses that a person should not be prosecuted under the EEA if "he [took] a trade secret because of ignorance, mistake, or accident" or if "he actually believed that the information was not proprietary after [he took] reasonable steps to warrant such belief." 142 Cong. Rec. 27, 117 (1996). Thus, if a defendant can show that he took reasonable steps, such as requesting permission from his employer to take certain information, he would be immune from prosecution.

Finally, case law also does not support a heightened knowledge requirement. The Sixth Circuit has held that the "defendant need not have been aware of the particular security measures taken by [the trade secret owner]. Regardless of his knowledge of those specific measures, defendant knew the information was proprietary." *United States v. Krumrei*, 258 F.3d 535, 539 (6th Cir. 2001) (affirming denial of motion to dismiss indictment as void for vagueness). In other words, the government must only show that a defendant knowingly misappropriated property (or proprietary information) belonging to someone else without permission, not that they knowingly misappropriated information that they knew met the legal definition of a trade secret under § 1839(3).

C. Void for vagueness

The EEA has been challenged in several instances as being unconstitutionally vague. Significantly, every court that has considered vagueness challenges to the EEA has rejected the attack as applied to the defendants in those cases. *See United States v. Krumrei*, 258 F.3d at 537-39 (the term "reasonable measures," as used in EEA's definition of trade secret, held not unconstitutionally vague as applied against former contractor of trade secret owner who was caught in a sting operation trying to sell trade secrets to the owner's competitor); *United States v. Yang*, 281 F.3d 534, 544 n.2 (6th Cir. 2002) (rejecting defendants' claim that the EEA would be unconstitutionally vague if attempt and conspiracy charges need not be based on actual trade secrets, because "[w]e have every confidence that ordinary people seeking to steal information that they believe is a trade secret would understand that their conduct is proscribed by the statute"); *United States v. Genovese*, 409 F. Supp. 2d. 253, 257-58 (S.D.N.Y. 2005)

(rejecting as applied and facial vagueness challenges to the EEA); *United States v. Hsu*, 40 F. Supp. 2d 623, 628 (E.D. Pa. 1999) (the term "reasonable measures," as used in EEA's definition of trade secret, held not unconstitutionally vague as applied against officers of foreign corporation who were caught in a sting operation trying to purchase trade secrets relating to anti-cancer drug Taxol, owned by Bristol-Myers Squibb); *United States v. Nosal*, No. CR 08-00237 MHP, 2009 WL 981336, *3 (N.D. Cal. Apr. 13, 2009) (rejecting void for vagueness challenge to nearly identical indictment language, and rejecting argument that knowledge of illegality must be alleged); *United States v. Chung,* No. SACR 08-00024-CJC, 2009 WL 997341 (C.D. Cal. Apr. 13, 2009) (rejecting vagueness challenge to economic espionage indictment alleging intent to benefit foreign instrumentality).

The void-for-vagueness doctrine has its constitutional foundation in the Due Process Clauses of the Fifth and Fourteenth Amendments to the Constitution. *See Belle Maer Harbor v. Charter Twp. of Harrison*, 170 F.3d 553, 556 (6th Cir. 1999); *United States v. Haun*, 90 F.3d 1096, 1101 (6th Cir. 1996); *Columbia Natural Resources, Inc. v. Tatum*, 58 F.3d 1101, 1104 (6th Cir. 1995). A criminal statute is unconstitutionally vague and violates the Due Process Clause if it fails (1) to define the offense with sufficient definiteness that ordinary people can understand the prohibited conduct; or (2) to establish standards to permit law enforcement to enforce the law in a non-arbitrary, non-discriminatory manner. *See Kolender v. Lawson*, 461 U.S. 352, 357 (1983); *see also United States v. Krumrei*, 258 F.3d 535, 537 (6th Cir. 2001) (rejecting void for vagueness as applied challenge to Economic Espionage Act).

Claims of vagueness that do not involve First Amendment freedoms must be examined in light of the facts of the particular case at hand and should not be examined on the basis of the statute's facial validity. *See Krumrei*, 258 F.3d at 537; *Columbia Natural Resources, Inc. v. Tatum*, 58 F.3d at 1109 n.6 (limiting vagueness challenge to an "as applied" analysis because the case did not implicate First Amendment rights); *United States v. Avant*, 907 F.2d 623, 625 (6th Cir. 1990) (reviewing vagueness challenge to a statute not involving First Amendment rights on the facts of that specific case). Furthermore, defendants must show that the statute as applied to the particular facts of their case is so indefinite that it does not present them with an ascertainable standard of guilt. *Parker v. Levy*, 417 U.S. 733, 756 (1974).

In *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999), the defendant was charged with attempted theft of trade secrets in violation of 18 U.S.C. § 1832(a)(4) and conspiracy to steal trade secrets in violation of 18 U.S.C. § 1832(a)(5). The defendant moved to dismiss the indictment on the basis that the EEA was unconstitutionally vague on several grounds.

One of Hsu's arguments was that the EEA's definition of "trade secret" under § 1839(3) was unconstitutionally vague as applied to Hsu. The court rejected this argument and found that the use of the words "reasonable" or "unreasonable" in the language requiring a trade secret owner to take "reasonable measures" to keep trade secret information secret does not render the statute vague. *Id*. at 628. The court also rejected Hsu's arguments on the basis that the trade secret definition was taken "with only minor modifications" from the Uniform Trade Secrets Act, which had been adopted in 40 states and the District of Columbia and had also withstood a void-for-vagueness attack. *Id.*

Hsu's void-for-vagueness challenge was also undercut by his own knowledge of the facts at the time of the offense. Hsu knew that the trade secret owner had taken many steps to keep its technology secret. He had been told on several occasions that the technology was proprietary to the victim company, that it could not be acquired through a license or joint venture, and that the information could be obtained only through an allegedly corrupt employee. Thus, the court found that since the facts clearly demonstrated that Hsu was aware that the information was proprietary and aware of the victim company's measures to protect the information, Hsu could not argue that the term "reasonable measures" was vague as it applied to him. *Id.*

Finally, the *Hsu* court concluded that the trade secret definition in the EEA was not void for vagueness when it stated that trade secret information not be "generally known to" or "readily ascertainable by" the public. The court found that the use of those terms in the statute was problematic because "what is 'generally known' and 'readily ascertainable' about ideas, concepts, and technology is constantly evolving in the modern age." *Id.* at 630. Based on a review of the defendant's e-mails, telephone calls, and conversations, the court found that Hsu was aware that the information could not be obtained through authorized means. Thus, the court found that the trade secret definition in § 1839(3) was not unconstitutionally vague as applied to Hsu. Therefore, as demonstrated in *Hsu*, proof of the defendant's conduct will usually allow the government to prevail in a vagueness challenge to the EEA as applied to a specific defendant.

While defendants continue to challenge trade secret indictments as void for vagueness, as noted above, the courts have consistently rejected these efforts.

D. Public disclosure

A person cannot be convicted for theft of a trade secret unless the trade secret owner took "reasonable measures to keep the information secret" and the "information derives independent economic value . . . from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839(3)(A), (B) (1996). Thus, the defense may argue that the trade secret information was in the public domain or the defendant rightfully believed it lawfully belonged to the defendant.

The first situation requires the government to work closely with a victim company to ensure that the information at issue has not been disclosed in some public forum such as in articles, in public presentations, in a patent application, or on the Internet. In a related vein, it is important to ensure that the company used reasonable measures to protect the trade secret. As noted in the House Report:

> The definition of trade secret requires that the owner of the information must have taken objectively reasonable and active measures to protect the information from becoming known to unauthorized persons. If the owner fails to attempt to safeguard his or her proprietary information, no one can be rightfully accused of misappropriating it.

H. Rep. No. 788, 104th Cong., 2d Sess. 7 (1996). The measure is an objective one and not evaluated from the view or understanding of the defendant.

The second situation can occur when two parties have a legitimate dispute over who owns the trade secret. This type of dispute is most likely to occur after the parties developed the information at issue together but their ownership interests are unclear. These types of cases are rarely appropriate for criminal prosecution and are often best resolved through private litigation.

E. Reverse engineering

Defendants may also claim that they obtained trade secret information through reverse engineering. A person may legally obtain information underlying a trade secret by "reverse engineering," or the act of analyzing something to determine how it works or how it was made or manufactured. *Kewanee Oil Co. v. Bicron Corp*., 416 U.S. 470, 476 (1974) (holding that the law does not protect the owner of a trade secret from "discovery by fair and honest means, such as by independent invention, accidental disclosure, or by so-called reverse engineering"); *ConFold Pac., Inc. v. Polaris Indus.*, 433

F.3d 952, 959 (7th Cir. 2006) ("[I]t is perfectly lawful to 'steal' a firm's trade secret by reverse engineering.")

Congress stated that the owner of a trade secret, unlike the holder of a patent, does not have "an absolute monopoly on the information or data that comprises a trade secret." 142 Cong. Rec. 27, 116 (1996). Other companies and individuals have the right to discover the information underlying a trade secret through their own research and hard work; if they do, there is no misappropriation under the EEA. *Id.* Even though the EEA does not specifically state when reverse engineering is a valid defense, the legislative history provides that:

> [T]he important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has "reverse engineered." If someone has lawfully gained access to a trade secret and can replicate it without violating copyright, patent, or this law, then that form of "reverse engineering" should be fine.

142 Cong. Rec. 27, 116 (1996). The fact that a particular secret might have been reverse engineered after a time consuming and expensive laboratory process does not provide a defense for someone who intended to avoid that time and effort by stealing the secret, unless the information was so apparent as to be deemed "readily ascertainable" and thus not a trade secret at all. *See* 4 Roger M. Milgrim, Milgrim on Trade Secrets, § 15.01[d][iv]; *Alcatel USA, Inc. v. DGI Techs., Inc.*, 166 F.3d 772, 784-85 (5th Cir. 1999) (holding that a competitor could not assert reverse engineering defense after it had first unlawfully obtained a copy of the software and then used the copy to reverse engineer); *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.,* 35 F.3d 1226, 1237 (8th Cir. 1994) (stating the fact "that one 'could' have obtained a trade secret lawfully is not a defense if one does not actually use proper means to acquire the information"); *Telerate Sys., Inc. v. Caro*, 689 F. Supp. 221, 233 (S.D.N.Y. 1988) ("[T]he proper focus of inquiry is not whether an alleged trade secret can be deduced by reverse engineering, but rather, whether improper means are required to access it.") In cases where there is a legitimate issue of a trade secret being "readily ascertainable," prosecutors should give strong consideration to allowing the parties to resolve the matter in civil court.

In most cases, prosecutors will be successful in rebutting a claim of reverse engineering by showing the defendant obtained the trade secret information without the authorization of the trade secret owner.

F. Advice of counsel

A defendant who "honestly and in good faith" relies on the advice of counsel may "not be convicted of a crime which involves willful and unlawful intent." *Williamson v. United States,* 207 U.S. 425, 453 (1908).

As the Seventh Circuit has noted:

> if a criminal statute requires proof that the defendant knew he was violating the statute in order to be criminally liable for the violation, and it is unclear whether the statute forbade his conduct, the fact that he was acting on the advice of counsel is relevant because it bears on whether he knew that he was violating the statute.

United States v. Urfer, 287 F.3d 663, 666 (7th Cir. 2002) (charges of willfully injuring federal property). In other words, advice of counsel can only be used as a defense if it negates the mens rea needed to prove a violation. For example, a defendant cannot be convicted unless he knew that he was misappropriating information he was not authorized to have. Thus, the advice-of-counsel defense may be available if a

defendant can show that counsel advised him that he could claim an ownership interest in the information at issue.

In order to use the advice-of-counsel defense at trial, the defendant must provide "independent evidence 'showing (1) the defendant made full disclosure of all material facts to his or her attorney before receiving the advice at issue; and (2) he or she relied in good faith on the counsel's advice that his or her course of conduct was legal.' " *Covey v. United States*, 377 F.3d 903, 908 (8th Cir. 2004). Otherwise, the defense will fail. As in other previously cited examples, if you are presented with a case where advice of counsel may be a legitimate defense, prosecutors should consider allowing the parties to resolve the dispute in private litigation.

III. Conclusion

This review highlights some of the defenses that may be asserted in a trade secret case. As seen in most of these situations, proof of the basic facts concerning the misappropriation will negate a defendant's specific defense. Early assessment of these issues is critical in evaluating the merits of the case and successfully prosecuting a trade secret theft case.❖

ABOUT THE AUTHOR

❑ **Thomas Dougherty** has been a trial attorney with the Computer Crime and Intellectual Property Section for 2 years. Mr. Dougherty joined the Department of Justice as an Assistant United States Attorney in the District of Nevada U.S. Attorney's Office in 2001.✠

Parallel Proceedings in Trade Secret and Economic Espionage Cases

Tyler G. Newby
Trial Attorney
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

Like other criminal intellectual property statutes, the Economic Espionage Act (EEA) shares a number of elements with civil trade secret enforcement statutes. 18 U.S.C.A. §§ 1831-39 (2006). This overlap is by design, as Congress expressly based the EEA on the Uniform Trade Secrets Act, upon which 46 states have also based their trade secret statutes. *See* H. Rep. No. 788, 104th Cong., 2d Sess., at 12 (1996). In fact, § 1838 under the Economic Espionage Act expressly provides that it does not "preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret. . . . "

Additionally, § 1836(a) provides, "The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter." The House Report further clarifies that the statute "does not preempt non-federal remedies, whether civil or criminal, for dealing with the theft or misapplication of trade secrets." According to the House Report, the fact that "the Attorney General is authorized . . . to commence civil proceedings in order to enjoin further conduct which would violate [the statute] is not to be interpreted to mean that other persons and entities may not also seek injunctive relief that may be available in other civil actions (using state law tort or contract claims) in order to prevent the further misuse of a trade secret." H. Rep. No. 788, 104th Cong., 2d Sess. 14 (1996).

In light of this overlap, and the fact that owners of trade secrets who fail to enforce their rights risk waiving them, prosecutors pursuing EEA charges are likely to confront a parallel civil trade secret misappropriation proceeding at some point during the criminal EEA investigation. These parallel proceedings can present both challenges and opportunities for law enforcement.

Parallel proceedings are simultaneous or successive criminal, civil, or administrative investigations or litigation involving a common set of facts, conducted by different agencies, branches of the government, or private litigants. In the context of an EEA prosecution, a parallel proceeding is most likely to arise in the form of a concurrent or pre-existing civil trade secret misappropriation action pursued by the victim trade secret owner against one or more of the subjects of the criminal investigation. Private party civil proceedings typically generate evidence in the form of interrogatory responses, responses to document requests, and testimony at depositions, preliminary injunction hearings, or trials that would be of interest to the prosecution team investigating potential EEA violations. In many cases, a victim or civil plaintiff may be more than willing to turn over this evidence to law enforcement. While there is nothing inherently wrong, ethically or legally, with conducting a parallel criminal proceeding, prosecutors and investigators handling EEA cases should be attuned to the legal and strategic issues that can arise from such proceedings. It is the objective of this article to help prosecutors in EEA cases recognize these issues early in their investigations so that they do not materialize into problems later.

II. Legal issues inherent in parallel proceedings

Provided that each proceeding is conducted in good faith for a proper purpose, parallel proceedings do not offend a defendant's rights to due process or a prosecutor's professional responsibility obligations. *See, e.g., United States v. Kordel*, 397 U.S. 1 (1970) (approving government's parallel civil and criminal proceedings against defendant); *Abel v. United States*, 362 U.S. 217 (1960) (lacking bad faith, mere cooperation of different branches of the Department of Justice is neither illegitimate nor unconstitutional); *Sec.& Exch. Comm'n v. Dresser Indus., Inc.*, 628 F.2d 1368, 1374 (D.C. Cir. 1980) (en banc) (In the absence of substantial prejudice to the rights of the parties involved, parallel proceedings are unobjectionable under [United States] jurisprudence). The converse is that parallel proceedings that are deemed to have been conducted for the benefit of another proceeding may result in the suppression of evidence or even the outright dismissal of the criminal proceeding. Bad faith conduct may include misusing a civil or criminal proceeding for the purpose of benefitting the other proceeding; making affirmative misstatements of fact or law during one of the proceedings; or engaging in conduct involving dishonesty, fraud, deceit, or misrepresentation.

Although there has yet to be a published opinion addressing allegations of bad faith conduct in parallel proceedings in an EEA prosecution, several recent decisions concerning prosecutions of other white collar crimes provide some general guidance as to the types of conduct a court may consider to be in bad faith. This discussion comes with an important caveat: as is the case with all professional responsibility questions with regard to specific factual scenarios, questions should be directed to the U.S. Attorney's office's Professional Responsibility Officer and/or the Department of Justice's Professional Responsibility Advisory Office.

A. From *Kordel* to *Posada-Carilles*

Modern jurisprudence on the propriety of parallel civil and criminal proceedings stems from the Supreme Court's consideration of the issue nearly four decades ago in *United States v. Kordel.* There, the Food and Drug Administration's regulatory arm, with the assistance of civil attorneys in a U.S. Attorney's office, initiated a civil *in rem* action seeking the seizure and removal from the marketplace of two products that were alleged to violate the Food, Drug, and Cosmetic Act. During the course of civil discovery, the FDA served civil interrogatories on the corporate distributor of the products, and shortly thereafter provided statutory notice that it was initiating a criminal investigation concerning those products. *Kordel,* 397 U.S. at 3-4. Before answering the interrogatories, the corporation moved to stay the civil case pending the outcome of the criminal investigation. The district court denied the motion to stay on the grounds that it was uncertain that the criminal investigation would result in charges and that the interests of justice favored allowing the government to proceed with its civil case. The corporation answered the interrogatories, which its vice president verified under oath. *Id.* at 4-6. Several months after the civil matter settled, the U.S. Attorney's office obtained a criminal indictment charging the vice president, the CEO, and the corporation with criminal violations of the Food, Drug and Cosmetic Act based on the same general facts and circumstances at issue in the civil matter. *Id.* at 6.

Appealing their convictions following a jury trial, the defendants argued that the government improperly used the civil action to obtain evidence, including the vice president's sworn interrogatory responses, against them in the criminal proceeding in violation of their due process and fifth amendment rights. The Supreme Court rejected both arguments. *Id.* at 7-8. The Court noted that the vice president was never compelled to answer the interrogatories in the civil action, but rather the company selected him to verify the interrogatories on its behalf. Furthermore, the vice president could have asserted his fifth amendment rights during the civil action by refusing to answer the interrogatories, but he did not. *Id* at 8-9. The Court was equally dismissive of the CEO's fifth amendment argument since he never provided any

testimony in the civil action. In rejecting the defendants' due process arguments, the Court found that because the government had (1) not brought the civil action "solely to obtain evidence for its criminal prosecution"; had (2) not failed to advise the defendants that the government was contemplating criminal proceedings; and (3) because the defendant had counsel in the civil claim and was not prejudiced by pre-trial publicity, there was no due process violation. *Id.* at 11-12.

Nearly 40 years later, a trio of opinions from the Fifth, Ninth, and Eleventh Circuit Courts of Appeals filled in the analytical framework erected in *Kordel*. *See United States v. Posada Carilles,* 541 F.3d 344 (5th Cir. 2008); *United States v. Stringer*, 535 F.3d 929 (9th Cir. 2008); *United States v. Moses*, 219 Fed. Appx. 847 (11th Cir. 2007). On somewhat similar factual records, those courts found that parallel criminal and civil proceedings conducted by different divisions of the U.S. government did not violate due process rights, even though there was some coordination between the government's civil attorneys and the prosecution team concerning the evidence to be developed in the civil case.

In the first of these opinions, *United States v. Moses*, a criminal securities fraud prosecution, the Eleventh Circuit considered the argument by a defendant in that the government engaged in prosecutorial misconduct when the Securities and Exchange Commission (SEC) deposed the defendant shortly before the U.S. Attorney's office initiated its criminal case. The SEC had already referred the case to the U.S. Attorney's office and had been providing evidence it obtained in the civil enforcement proceeding to the prosecution team. In rejecting the defendant's argument, the Eleventh Circuit found that the SEC had a legitimate purpose in pursuing its civil case. In addition, the SEC notified the defendant that it may provide evidence to Department of Justice prosecutors, and the defendant was advised of his fifth amendment rights prior to his civil deposition. Nonetheless, the defendant made incriminating statements during his testimony that were used against him in the subsequent criminal proceeding. *Id.* at 849-50. In reaching its ruling, the court noted that "[i]t is well established that the federal government may pursue civil and criminal actions either 'simultaneously or successively.' " *Id*. at 849.

In *United States v. Stringer*, the Ninth Circuit reached the same finding on similar facts. There, the court considered the conduct of a parallel civil investigation led by the SEC that led to a criminal referral and prosecution by the U.S. Attorney's Office in Oregon. At the outset of the SEC's investigation, the agency provided a standard letter to the defendants informing them that the agency may turn over evidence to criminal investigators. Prior to depositions, the SEC provided witnesses with the agency's standard Form 1662 that advises all SEC testifying witnesses of their fifth amendment rights. The agency referred the case for criminal prosecution to the U.S. Attorney's office early in the civil case and provided evidence to the criminal prosecution team during the course of its case. At the request of the investigating Assistant U.S. Attorney, the SEC scheduled depositions of subjects of the criminal investigation to be held in the jurisdiction of the investigating U.S. Attorney's office. However, the agency did not otherwise inform the witnesses for the defendants in the civil action of the pending criminal investigation. When defense counsel asked the SEC attorney whether the agency was working with other government agencies like the Department of Justice, the attorney referred defense counsel to the SEC Form 1662 and otherwise declined to answer.

In moving to dismiss the indictment, the defendant claimed that the government used deceit and trickery to obtain incriminating evidence and statements in the civil proceeding, in violation of his due process rights. The district court agreed, dismissing the indictment, and the Ninth Circuit reversed. Central to the Ninth Circuit's ruling analysis was the fact that the SEC made no affirmative misrepresentations and advised defendants of possible criminal referrals at the outset of the civil proceeding. The court further recognized:

> [i]t is significant to our analysis that the SEC began its civil investigation first and brought in the U.S. Attorney later. This tends to negate any likelihood that the government began the civil investigation in bad faith, as, for example, in order to obtain evidence for a criminal prosecution.

Stringer, 535 F.3d at 939.

Similarly, in *United States v. Posada-Carilles*, the Fifth Circuit reversed the district court's dismissal of a false statement indictment arising out of statements made by the defendant to a federal immigration officer during a naturalization interview. The defendant, a high-profile Cuban dissident who had been linked to a terrorist attack decades earlier, had illegally entered the United States and applied for citizenship after he was detained. Prior to conducting the naturalization interview, the immigration officer met with federal prosecutors to prepare for the interview. At the beginning of the interview, the immigration officer advised the defendant of his fifth amendment rights, which the defendant invoked at various times during the interview. As in *Stringer*, the district court dismissed the indictment, finding improper coordination between the prosecution team and the administrative INS lawyers.

Reversing the district court's dismissal of the indictment, the Fifth Circuit held that the immigration officer did not have an affirmative duty to warn the defendant of the possibility of criminal prosecution, provided that she did not make any material misrepresentations. The court concluded: "the mere failure of a government official to warn that an investigation may result in criminal charges does not constitute fraud, deceit, or trickery." *Posada-Carilles,* 541 F.3d at 355. Also key to the court's ruling were the facts that the defendant, and not the government, initiated the civil proceeding in which he made the false statements by applying for citizenship; the defendant was advised of his fifth amendment rights; and the U.S. Citizenship and Immigration Services, like the SEC, is required by law to coordinate with federal law enforcement.

The case law is not uniform, however. In *United States v. Scrushy*, 366 F. Supp. 2d 1134 (N.D. Ala. 2005), an Alabama district court judge reached a different conclusion based on facts that are largely indistinguishable from *Stringer* and *Moses*. As in those cases, the *Scrushy* case involved a parallel civil SEC investigation and a criminal securities fraud investigation by the Northern District of Alabama U.S. Attorney's Office. *Id.* at 1136. As in *Stringer*, the SEC rescheduled the defendant's deposition to be held in the investigating U.S. Attorney's office's district at the request of the prosecution team. The SEC lawyers received input from the prosecution team regarding which deposition topics to cover and which topics not to cover, and shared evidence with the prosecution team. In addition, an SEC accountant who had been working on the civil action attended the interviews of two cooperating witnesses in the criminal action. The criminal investigation did not surface until after the defendant was deposed in the SEC case. *Id.* at 1136-37. In granting the motion to suppress the defendant's testimony in that deposition, which resulted in the dismissal of three perjury charges, the district court found that the collaboration between the prosecution team and the SEC before the defendant's deposition and at the witness interviews improperly merged the parallel proceedings. *Id.* at 1139. In light of the jury's acquittal on the remaining charges, that decision was not appealed.

Viewed together, the *Moses*, *Stringer*, *Posada-Carilles*, and *Scrushy* cases share the following common elements: there were legitimate factual and legal bases for the civil actions that were initiated before the criminal investigations; the defendants were advised of their fifth amendment rights prior to making statements in response to government questions in the civil actions; and no affirmative misleading statements were made to the defendants during the civil proceedings regarding the pendency of any criminal proceedings. The *Moses*, *Stringer*, and *Posada-Carilles* courts found these facts to be determinative in ruling that the sharing of evidence and limited coordination of evidence gathering between the government's civil and criminal legal teams did not violate due process. For the district court in *Scrushy*, however, any coordination of evidence gathering between the government's civil and criminal legal teams was impermissible. In that court's view, "to be parallel, by definition, the separate investigations should be like the side-by-side train tracks that never intersect." *Scrushy*, 366 F. Supp. 2d at 1139. *Scrushy*, in short, is irreconcilable with *Moses*, *Stringer,* and *Posada-Carilles*. While a strong argument can be made that the *Scrushy* opinion is an aberration, particularly in light of its failure to

reference the principles set forth in *United States v. Kordel* and the 11th Circuit's subsequent opinion in *Moses*, prosecutors should be mindful that increased collaboration with the civil investigation comes with an increased risk of an adverse finding from a district court.

B. Avoiding the due process challenge

It remains to be seen how a court would address similar types of interaction between prosecutors and private parties who were pursuing a civil trade secret action against the subjects of a criminal investigation. Certainly, where private parties initiate and pursue a civil action, there is less of an appearance of the government misusing its civil and administrative enforcement arm to obtain evidence its criminal arm could not. On the other hand, the defendants in *Kordel*, *Moses*, *Stringer*, and *Posada-Carilles* were all provided notice in their civil and administrative actions that the civil agencies may share information with law enforcement and that they had a fifth amendment right not to testify against themselves. Even though those notices were contained in boilerplate letters in the SEC cases, they were still of importance to the Ninth and Eleventh Circuits. While skilled defense counsel in a civil trade secret misappropriation action may spot potential criminal exposure for their clients and advise them of the risks and benefits of invoking their fifth amendment rights in the civil action, it would be unusual for the plaintiff's attorney to inform the witness of his rights or to otherwise provide notice that the plaintiffs may share evidence with law enforcement.

Whether a district court deems parallel trade secret proceedings to be in good faith or bad faith will likely depend on the level of coordination between the plaintiffs' attorneys and the prosecution team. Where the relationship is entirely at arms length and the prosecution team receives evidence from the civil case following the issuance of a formal request like a grand jury subpoena, there appears to be little risk that a court would find that the defendants' due process rights were violated. The question becomes more vague where there is greater coordination. For example, would it be permissible for the prosecution team to provide the plaintiff's attorneys with a list of documents that would be useful to its investigation, which the plaintiff later includes in a list of document requests? Or would a district court find a defendant's due process rights had been violated if the prosecution team were to provide the plaintiffs with a list of topics it would like covered in depositions of the targets of the criminal investigation? The *Scrushy* opinion suggests that at least one district court would be troubled by such a scenario, while the *Stringer*, *Posada-Carilles,* and *Moses* cases, on the other hand, suggest that it would not implicate a target's due process rights, provided that the civil trade secret suit was for a legitimate, independent purpose and no material, misleading statements were made regarding the possibility of criminal prosecution.

In sum, when confronted with a parallel civil trade secret misappropriation proceeding, prosecutors should tread carefully in seeking to use the fruits of the civil action. While specific advice is impossible in a vacuum, prosecutors should consider at least the following factors when shaping their interactions with the private litigants:

- Is the existence of the criminal investigation known to the defendants in the civil action?
- Are the defendants in the civil actions represented by counsel?
- Has the plaintiff made any misrepresentations to the defendants regarding its knowledge of a criminal investigation?
- Is the plaintiff offering to provide the government with the fruits of its investigation, or is it seeking affirmative input from the government on what would be useful for a criminal prosecution?

III. Strategic considerations and stays of civil litigation

Apart from the legal issues outlined above, the potential for parallel proceedings in EEA investigations may also require important strategic decisions considering whether to intervene in the civil case. While evidence gathered by the trade secret owner plaintiff in a civil action is likely to be of assistance in putting together a criminal case, the potential also exists for the civil proceeding to interfere with the criminal investigation. Defendants in civil proceedings are entitled to broad, liberal discovery, which they typically use in trade secret cases to poke holes in both the secrecy of the alleged trade secret information and in the security measures employed by the victim. Plaintiffs and defendants alike have the opportunity to depose all of the witnesses the prosecutor may eventually call in the criminal case and lock in their testimony before the prosecution has fully developed its theory of the case. Furthermore, using subpoenas issued under Rule 45 of the Federal Rules of Civil Procedure, defendants may pursue extensive third-party discovery designed to cloud the issue of whether the allegedly secret information is in fact known to a variety of entities. Similarly, depositions of employees of the owner of the alleged trade secret information could result in conflicting testimony on what they understand to be secret and not secret. A particularly aggressive defendant may initiate a civil declaratory relief action against the trade secret owner in an effort to gain access to these civil discovery tools when confronted with a criminal investigation for the very purposes outlined above.

In circumstances where the civil action may jeopardize the effectiveness of the criminal investigation, the government may consider intervening in the civil action for the limited purpose of moving to stay the parallel civil proceeding. This is a two-step process: first, the government must convince the court in the civil action that it is entitled, as a third party, to intervene for the limited purpose of moving for a stay; and second, the government must convince the court that the interests of justice in the enforcement of federal criminal laws require a stay of discovery in the civil proceeding.

Federal Rule of Civil Procedure 24 governs third-party motions to intervene. Rule 24(a) allows intervention as "of right" by a party that is given an unconditional right by statute to intervene and to a party with:

> an interest relating to the property or transaction which is the subject of the action and the applicant is so situated that the disposition of the action may as a practical matter impair or impede the applicant's ability to protect that interest, unless the applicant's interest is adequately represented by existing parties.

Fed. R. Civ. P. 24(a). Rule 24(b) allows permissive intervention within the trial court's discretion "when an applicant's claim or defense and the main action have a question of law or fact in common." Fed. R. Civ. P. 24(b). Typically, courts that have permitted intervention by the United States for the limited purpose of filing a motion to stay a parallel civil action have done so under Rule 24(b). *See, e.g.*, *Ashworth v. Albers Med. Inc.*, 229 F.R.D. 527, 529-30 (S.D. W.Va. 2005); *Bureerong v. Uvawas,* 167 F.R.D. 83, 85-86 (C.D. Cal.1996); *Twenty First Century Corp. v. LaBianca,* 801 F. Supp. 1007, 1009 (S.D.N.Y.1992); *Bridgeport Harbour Place I, LLC v. Ganim,* 269 F. Supp. 2d 6, 8 (D. Conn. 2002). To succeed on a motion to intervene for a limited purpose of filing a motion to stay the civil proceedings, the government must show that its motion was filed in a timely manner and that there is a nexus between the factual or legal issues in the civil trade secret action and the criminal investigation. *See* Fed. R. Civ. P. 24(b); *Ashworth*, 229 F.R.D. at 529-30. To make such a showing, the government may be required to submit an affidavit by the prosecutor setting forth the status of the criminal proceeding. *See, e.g., Ashworth*, 229 F.R.D. at 528-29.

If the United States is permitted to intervene in the civil action, the court has complete discretion in deciding whether to stay the civil proceedings or otherwise limit the scope of civil discovery. *See, e.g., Landis v. North Am. Co.*, 299 U.S. 248, 254 (1936) ("[T]he power to stay proceedings is incidental to the

power inherent in every court to control the disposition of the causes on its docket with economy of time and effort for itself, for counsel, and for litigants.") Neither the government nor a litigant in a parallel civil proceeding has a statutory or constitutional right to a stay of the civil proceeding. *See, e.g., Keating v. OTS,* 45 F.3d 322, 324 (9th Cir.1995).

In deciding whether to exercise its discretion to enter a stay of the civil action, most courts apply a five factor analysis set forth by the Ninth Circuit in *Keating*, which weighs*:*

> (1) the interest of the plaintiffs in proceeding expeditiously with [the] litigation or any particular aspect of it, and the potential prejudice to plaintiffs of a delay; (2) the burden which any particular aspect of the proceedings may impose on defendants; (3) the convenience of the court in the management of its cases and the efficient use of judicial resources; (4) the interests of persons not parties to the civil litigation; and (5) the interest of the public in the pending civil and criminal litigation.

Keating, 45 F.3d at 325. In addition, courts may look to the extent of the overlapping factual issues in the civil and parallel criminal actions and to whether a target of the criminal investigation appears to be using the civil action as a means of obtaining discovery to which it would not be entitled in the criminal proceeding. *See, e.g.*, *Ashworth*, 229 F.R.D. at 531-32 (court must review relatedness of civil and criminal action).

A *Westlaw* search on November 2, 2009 yielded no published opinions addressing motions by the United States to intervene and stay civil trade secret misappropriation action pending the completion of a parallel criminal EEA investigation. However, a Southern District of West Virginia court's opinion in a 2005 civil consumer class action concerning the distribution of counterfeit pharmaceuticals considered the same arguments that are likely to arise in an EEA case. *See Ashworth*, 229 F.R.D. 527. There, the district court granted motions by the United States both to intervene in the civil case where the facts at issue and two of the three defendants were also the subject of a federal criminal investigation into the distribution of counterfeit drugs.

Applying the first of the *Keating* factors, the court noted that the first factor will always favor the plaintiff but that the plaintiff's interest in proceeding expeditiously may be trumped by a pending criminal investigation. *Id.* at 531. The *Ashworth* court noted that the parallel investigation was complex and had already resulted in four guilty pleas, three active criminal cases, and two forthcoming indictments. *Id.*

The court also found that the interests of the defendants in the civil case favored a stay of discovery. Three of the defendants had received target letters in the criminal investigation and would potentially be forced into choosing between the adverse inference that may be drawn in a civil action from invoking one's fifth amendment rights or the risks associated with waiving those rights. *Id.* The court noted that while stays of civil litigation involving targets of parallel criminal proceedings typically are not granted pre-indictment, the fact that the government had represented that indictments were forthcoming mitigated that factor. *Id.* at 532 n.3.

The *Ashworth* court further found that judicial economy, the interests of the United States, and the public interest favored a stay. With respect to judicial economy, the court found that allowing the criminal proceeding to proceed first could streamline issues in the civil matter. *Id.* The court further found that the United States had a significant interest in not allowing the subjects of its criminal investigation to use liberal civil discovery to circumvent the restrictions of criminal discovery. *Id.*; *see also Campbell v. Eastland*, 307 F.2d 478, 487 (5th Cir. 1962) (taxpayer who filed civil suit for tax refund after learning of pending criminal investigation for tax fraud should not have been permitted to use civil discovery to investigate the government's evidence in the criminal investigation); *Sec. & Exch. Comm'n v. Dresser Indus.*, 628 F.2d 1368 (D.C. Cir. 1980) (en banc) (government may seek stay of civil proceeding "to prevent the criminal defendant from broadening his rights of criminal discovery against the

government."). Finally, the court found that the public's interest in the enforcement of criminal laws trumped the interests of private litigants. *Ashworth*, 229 F.R.D. at 532. Weighing all of the *Keating* factors, the *Ashworth* court imposed a stay of all civil discovery until the indictments were issued, at which point the court would revisit the issue. *Id.* at 532-33.

Although motions to stay are highly fact dependent, the *Ashworth* case suggests that a few key factors will have the greatest influence on whether the government will be successful when moving to stay a civil trade secret misappropriation action. First, the court will likely be heavily influenced by whether an indictment has been issued against one or more defendants in the civil action, or whether such an indictment is forthcoming. The court will likely balance this factor with the status of the civil litigation. Where a civil action is substantially underway but the criminal investigation is in its infancy, *Ashworth* suggests that a court may be less likely to enter a stay. Also, the court is likely to give significant consideration to whether one of the targets of the criminal investigation appears to be using the civil discovery rules to short-circuit the more limited criminal discovery available under Rules 16 and 17 of the Federal Rules of Criminal Procedure. For example, if a subject of a criminal investigation were to file a civil declaratory relief action against the trade secret owner and seek extensive discovery aimed clearly at the focus of the criminal investigation, that fact would likely weigh in favor of a stay.

IV. Conclusion

While prosecutors are likely aware of the potential benefits of parallel proceedings to a criminal EEA investigation–namely, access to evidence gathered by the trade secret owner–they also need to be aware of the risks outlined in this article. Careful planning at the early stages of the investigation with respect to the prosecution team's interactions with the plaintiff's counsel will help avoid a later due process challenge once criminal charges are brought. An early assessment of whether civil discovery is more likely to help or hinder the criminal investigation will make a motion to intervene to stay the civil action more likely to succeed than one that is brought after several months of civil discovery.❖

ABOUT THE AUTHOR

❑ **Tyler G. Newby** is a Trial Attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice's Criminal Division and previously served as Special Assistant United States Attorney in the Cyber Unit of the Eastern District of Virginia. Prior to joining the Justice Department, Mr. Newby practiced civil intellectual property litigation in Silicon Valley and San Francisco, where he handled a number of trade secret misappropriation cases.✠

Identifying and Using Electronic Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases

Mark L. Krotoski
National Computer Hacking and Intellectual Property (CHIP) Coordinator
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

Electronic evidence can take many forms. Broadly, it includes e-mail, text messages, chat and other electronic communications, information stored on a computer or other storage media or platform, and Internet records such as browsing activity and logs. Even efforts to delete electronic evidence, indicating consciousness of guilt or obstruction of justice, may be futile as remnants of the evidence may still be found in unallocated space on a hard drive or on other servers where the information was transmitted.

In civil actions, electronic evidence is usually referred to as "electronically stored information," and has become common in many cases. Electronically stored information, which is undefined under the civil rules, must usually be preserved and produced as part of a discovery plan and considered during a meet and confer conference. *See, e.g.,* FED. R. CIV. P. 16, 26, 34.

While electronic evidence is increasingly important in many criminal and civil cases, it has proven to be particularly significant and often essential in trade secret and economic espionage cases. For example, the electronic evidence may show how the trade secrets were downloaded from the company network, stored on a thumb drive, or transmitted to others. E-mail evidence may reveal planning among co-conspirators about how they intend to use or sell the trade secret.

This article reviews the importance of identifying and developing a strategy to obtain electronic evidence early in a trade secret or economic espionage case. Some recent case examples involving electronic evidence are highlighted. Specific steps are suggested to develop an Electronic Evidence Case Plan, which is particularly important in trade secret and economic espionage cases, but may be effectively used in other criminal cases.

II. Importance of electronic evidence in general

For at least four reasons, electronic evidence may be among the best evidence possibly obtained during a criminal investigation. First, electronic evidence can capture details of the moment that may be unavailable through other forms of the same or similar evidence. As an example, compare a document or photograph in hard copy or physical form with an electronic copy of the document or photograph. A witness can authenticate or explain the contents or circumstances of a particular document. In digital

form, this same evidence may have other useful metadata information, such who the author was, the date of creation, and date they were last saved, and by whom. Changes and the evolution or history of the document can be tracked. For photographs, the metadata may reveal camera type, settings, and the date and time the photograph was taken.

Second, electronic evidence can advance an investigation concerning key events in the case. The evidence may identify a transaction or event on which the investigation can concentrate. For example, an e-mail about a particular meeting confirms that it took place, where, and who was present. With this information, the investigation can focus on the events surrounding the meeting. If co-defendants later elect to provide truthful cooperation, they cannot deny that the meeting transpired. Instead, they may be able to add further facts about the meeting. In a related manner, the electronic and non-electronic evidence may fill in gaps in the time line of the case as it is presented to the jury.

Third, electronic communications often include candid and informal statements, which may shed light on the defendant's intent or provide evidence of planning. E-mail and chat usually are unguarded and frank. For this reason, e-mail or other communication records between the targets can be effective to show their role in the scheme and future plans.

Fourth, one strength of electronic evidence is that it can corroborate other evidence in the case. The electronic evidence may confirm evidence obtained through witness interviews, the execution of a search warrant, undercover activities, or surveillance, for example. The case is strengthened by the corroboration of the electronic and non-electronic evidence.

III. Recent examples of electronic evidence in trade secret and economic espionage cases

A review of some recent trade secret and economic espionage cases shows the importance of electronic evidence in investigating and prosecuting these cases.

A. The Coca-Cola trade secret conspiracy investigation and trial

During the Coca-Cola trade secret conspiracy trial, investigators and prosecutors developed a case plan that allowed them to gather electronic evidence while events were developing, in addition to other traditional forms of evidence. The electronic evidence included e-mail and text communications and Title III court-authorized intercepts. The electronic evidence furthered key phases of the investigation and was also introduced at trial against the primary defendant.

The case started when a Pepsi senior vice president received a letter offering Coca-Cola information to the "highest bidder." After Pepsi contacted Coca-Cola, the matter was referred to the Federal Bureau of Investigation, which commenced an undercover investigation. Initially, it was unclear who was behind the effort to sell Coca-Cola trade secrets and proprietary information. The investigation established that a Coca-Cola insider, an executive assistant to a high ranking Coca-Cola official, was responsible for misappropriating the trade secrets and other proprietary information. In her position, she had access to confidential documents and product samples. She provided trade secrets and other proprietary information to an outsider who contacted Pepsi. *See generally United States v. Williams*, 526 F.3d 1312 (11th Cir. 2008) (per curiam).

At trial, text and e-mail communications were introduced, including e-mail communications between the undercover agent and a co-conspirator. As one example from the trial, in an e-mail to the undercover agent, co-defendant Dimson expressed concern about the delay in receiving a "good faith

payment" from the agent. He asked that $9,000 be wired to his account as "an indication of your seriousness." He claimed to have access to sensitive information: "Besides the Red Book, I have information that's all Classified and extremely confidential, that only a handful of the top execs at my company have seen. I can even provide actual products and packaging of certain products, that no eye has seen, outside of maybe 5 top execs."

One of the confidential documents in the case included an e-mail concerning a special project. Investigators determined that defendant Williams "printed - out three copies of an e-mail dated June 19, 2006 that was sent to the high ranking officer for whom she worked." The subject line of the e-mail referenced a "Project N*******." Shortly afterwards, co-conspirator Dimson faxed an e-mail with the same subject line to the undercover agent. *See United States v. Dimson, Duhaney, and Williams*, Criminal Indictment No. 1:06-CR-313, ¶¶ 11E, 11F (N.D. Ga. July 11, 2006) (listing overt acts in furtherance of the conspiracy), *available at* http://news.findlaw.com/wsj/docs/ip/usdimson 71106ind.html.

Three defendants were convicted: two by plea, and the insider executive assistant after a jury trial. The electronic evidence in the case was useful to confirm the roles of the conspirators and show their involvement in the scheme. The e-mail or other communication records among the co-conspirators revealed their plans and included negotiations for the sale of the trade secrets to the undercover agent.

B. Encouraging active use of the trade secret

Electronic communications have helped reveal the defendant's intended use of the misappropriated trade secret, as demonstrated in *United States v. Malhotra*, Case No. CR 08-00423 JF (N.D. Cal. July 11, 2008). The case involved the misappropriation of cost information trade secrets by an IBM Director of Sales and Business Development, Output Management Services. About 5 weeks before leaving International Business Machines Corporation (IBM), he requested and received the "latest" trade secret information concerning IBM Global Services, CC Calibration Metrics, which included sensitive pricing and strategy information for IBM products. The IBM official who provided the requested information specifically noted: "given the sensitive nature of the material please do not distribute." Each page of the information was marked "IBM Confidential."

A few weeks later, the defendant started a new position at the Hewlett Packard Company (HP) as Vice President of Imaging and Printing Services. E-mail evidence established that the defendant willingly shared the trade secret and other confidential information with senior officials at his new company with the intent to injure his former company. In one e-mail to an HP Senior Vice President, with the subject, "For Your Eyes Only," the defendant attached the IBM Global Services, CC Calibration Metrics. Two days later, the defendant sent an e-mail to another HP Senior Vice President with the subject, "For Your Eyes Only confidential." In this e-mail, he stated that he had shared the IBM Global Services, CC Calibration Metrics attachment with the first HP Senior Vice President, and noted:

> This is the latest version and is more recent than what I gave you earlier. I would like the Pursuit Teams to have knowledge of this info as well so they know what their competition shoots for as they price their deals. This is good stuff!

See generally United States v. Malhotra, Case No. CR 08-00423 JF, ¶¶ 6-7 (N.D. Cal. July 11, 2008) (plea agreement factual basis and sentencing memorandum and exhibits). This e-mail helped establish the defendant's intent to convert the IBM trade secret to the economic benefit of someone other than IBM, the trade secret owner, and the intent to injure IBM, as required under § 1832(a). The message shows how the defendant was interested in benefitting his new employer at the expense of his former employer, the owner of the trade secret information.

The defendant also e-mailed additional IBM proprietary information to other HP officials. In one

e-mail, he stated: “Team–this is some good info on Lexmark capabilities, tools and services. . . .” On the next day, the defendant willingly disclosed an IBM "competitor" template and asked the HP recipient to “keep to your self and do not distribute to anybody. . . . Let’s try and emulate these terms as closely as possible . . . where it makes sense. thx." *See generally Malhotra*, Case No. CR 08-00423 JF (sentencing memorandum and exhibits C & D). Based on this and other evidence, defendant Malhotra pled guilty to stealing an IBM trade secret under 18 U.S.C. § 1832(a)(2).

The e-mail in the case was important to show various phases of the case. First, the IBM e-mails demonstrated the confidentiality obligations when the defendant first requested and received the trade secret information. Second, the HP e-mails confirmed the defendant’s intent that the misappropriated trade secret be actively used.

C. Providing evidence of intent

Electronic evidence has often been important to show the defendant’s intent. The case in *United States v. Meng,* Case No. CR 04 20216-JF (N.D. Cal. Aug. 29, 2007), began after law enforcement received a report that the defendant was using trade secrets from a Silicon Valley company at a demonstration project for the People’s Republic of China Navy Research Center in Beijing. The defendant had previously served as an engineer at Quantum3D, which produced high-end visual simulation systems for military and commercial aircraft training. After severing his ties as an employee and contractor, he began working for a direct competitor in the People’s Republic of China.

The electronic evidence in the case was obtained largely through e-mail accounts and the defendant’s laptop, which was seized after he entered the United States to attend a 3-day conference. A preliminary examination of his laptop confirmed the presence of files that were consistent with Quantum3D’s trade secret files. An arrest warrant was obtained and executed about 6 hours before the defendant was scheduled to depart the United States. After an extensive investigation, defendant Sheldon Meng was charged with economic espionage, trade secret misappropriation, and violating the Arms Export Control Act, along with other counts.

The U.S. Munitions List materials that he misappropriated also constituted trade secrets. Under the Arms Export Control Act, the government was required to show that the defendant willfully exported an item on the United States Munitions List without having first obtained permission from the Secretary of State. *See* 22 U.S.C. § 2778; 22 C.F.R. § 120. Company e-mails were important to demonstrate this higher intent. For example, in one e-mail sent to the defendant, he was warned about the export controls:

> Sheldon:
>
> Since [Quantum3D products] nvsensor and vixsen are under export control and on the munitions list, we would most likely need an export license to do this. I would make this a low priority as I may have to order you to remove the software and hardware from the system.

Defendant Meng responded via e-mail: “I understand.” *Meng,* Case No. CR 04 (plea agreement factual basis). This and other e-mails showed the defendant was aware of the export restrictions on the products he later was found to possess outside the United States.

Since much of the activity in the case occurred in the Far East, without the e-mail evidence it would have been more challenging to develop the case and demonstrate this willful level of intent. Defendant Meng was ultimately convicted of committing economic espionage for misappropriating a trade secret from his former employer with the intent to benefit a foreign government, specifically the People’s Republic of China (PRC) Navy Research Center, and for willfully exporting a defense article without authorization from the United States to the PRC in violation of the Arms Control Export Act. As

noted below, additional electronic evidence in the case was also used to demonstrate other aspects of the misappropriation scheme.

D. Using computers to misappropriate trade secrets

In a number of trade secret and economic espionage cases, computer evidence is important to show that trade secret and other proprietary information were accessed and misappropriated. The Economic Espionage Act specifically applies to the misappropriation of a trade secret by "downloads, uploads," or replication, transmission, sending, communicating, or conveying. 18 U.S.C. §§ 1831(a)(2), 1832(a)(2) (1996).

The following recent cases illustrate the use of a computer to misappropriate a trade secret by downloading, copying, or transmitting information:

- *United States v. Jin*, Case No. CR 04 20216-JF, ¶¶ 1(h),(k) (N.D. Ill. Dec. 9, 2008) (economic espionage superseding indictment alleging: "Between approximately 9:00 a.m. and 2:00 p.m. on February 26, 2007, defendant JIN downloaded over 200 technical documents belonging to Company A on Company A's secure internal computer network"; "At approximately 9:00 p.m. on February 26, 2007, defendant JIN returned to her Company A office building and downloaded technical documents belonging to Company A on Company A's secure internal computer network, and removed numerous documents and other materials from the offices of Company A.") (case pending).
- *United States v. Pani*, Case No 4:08-CR-40034-FDS, ¶¶ 11-12 (D. Mass. Nov. 5, 2008) (trade secret indictment alleging: "From June 8 through June 11, 2008, while on both Intel's and AMD's payrolls, PANI used his Intel-issued laptop computer to access Intel's computer network from outside the company and thereby download 13 'top secret' (according to Intel's classification system) Intel documents."; "PANI copied the downloaded files to an external hard drive, so he would have a copy after returning his Intel-issued laptop.") (case pending).
- *United States v. Cotton,* Case No. CR S-08-0042-EJG (E.D. Cal. Feb. 29, 2008) (trade secret plea agreement factual basis noting that the defendant downloaded from the computers of his employer, Genesis Microwave, Inc., designs "for the manufacture and testing of detector logarithmic video amplifiers (DLVAs) and successive detection logarithmic video amplifiers (SDLVAs) which are components used in microwave technologies"; "The military applications of these technologies include enhancing navigation and guidance capabilities, radar jamming, electronic countermeasures, and the ability to locate and pin-point enemy signals during warfare.").
- *United States v. Roberts and Howley*, Case No. No. 3:08-CR-175, ¶¶ 14(h), (i), 24(e) (E.D. Tenn Mar. 3, 2009) (trade secret indictment alleging that the defendant used a "cellular phone to take seven (7) photographs of Goodyear's roll over-ply down device," "downloaded the seven (7) photographs from his cellular telephone to his personal email account … and emailed the photographs to his work email account," and "transmit[ted] the unauthorized photographs of Goodyear's roll over-ply down device to other Wyko employees to be used to assist Wyko in constructing a roll over-ply down device for" completing a contract with a Chinese tire manufacturing company) (case pending).
- *United States v. Zeng*, Case No. H-08-075 (S.D. Tex. May 16, 2008) (trade secret plea agreement factual summary noting that the defendant, a chemist for International Paint with access to "an epoxy-based intumescent fireproofing material" known as Chartek,

"downloaded Chartek's formula, printed it out, and kept it in his private residence" and "sent several emails to contacts in the People's Republic of China (PRC) … in which he sought to form a 'joint [business] venture' regarding various chemical compounds that he hoped to produce and/or sell within China," including Chartek).

- *United States v. Lee*, Case No. 09 CR 290-1, ¶¶ 1(f), (i), (k) (N.D. Ill. June 23, 2009) (trade secret indictment alleging that technical director "downloaded technical documents and materials, including trade secrets, belonging to Valspar from Valspar's secure internal computer network" and the defendant "transferred Valspar and Huarun documents and materials, including product data," and also trade secrets, "to an external thumb drive") (case pending).

IV. Key issues in obtaining electronic evidence

Each of the prior examples highlights the role of electronic evidence in recent trade secret and economic espionage prosecutions. Notwithstanding the increasing importance of electronic evidence in trade secret cases, there are special challenges to obtain this kind of evidence. Fortunately, by identifying the electronic evidence early in the case and preserving it, many of the challenges can be overcome.

A. Retention issues

One key challenge involves whether the records will be available when requested. Electronic evidence, while important, may not be available for long. The custodian of the electronic evidence normally decides how long to maintain it. Internet Service Providers retain records for a limited period, depending on what records are involved. For example, text messages may only be retained for a couple of days. After that period, the records are no longer available.

The following table provides a recent example of the retention records maintained by a large wireless telephone and internet provider:

Record Type	Retention
Subscriber Account Records	3 years
Text Message Content	3-5 days
IP Destination Information	30 days
IP Session Information	1 year
Call Detail Records / Cell Sites	1 year
Credit Card Numbers	6 months
Bill Copies	Last 12 months
Payment History	3-5 years

Many providers have Law Enforcement Guides which provide guidance on the records they keep, the periods of retention, and the suggested manner to request specific records. For example, some of the guides recommend search warrant or subpoena language to obtain particular records maintained by the provider. The Computer Crime and Intellectual Property Section (CCIPS) has collected a number of these law enforcement guides for prosecutors and they are available at CCIPS Online, the Department of Justice Intranet, or on request by telephoning CCIPS.

One lesson from the *Meng* case, noted above, is the importance of using an Electronic Evidence Case Plan early in an economic espionage and trade secret case. Based on a preliminary examination of his laptop, which was obtained at the airport when he entered the United States, files consistent with the

source code for the company were located. An arrest warrant was obtained and the defendant was arrested about 6 hours before he was to leave the country. As a matter of course, an Electronic Evidence Case Plan was considered early. At the time of the arrest, preservation requests were made to all known e-mail providers under 18 U.S.C. § 2703(f). This law enforcement request preserved the evidence in its current state for 90 days pending legal process. After an initial indictment was obtained, legal process was obtained about 30 days after the arrest and preservation requests were made.

The e-mail provider advised that someone tried to delete about 966 e-mails from the defendant's e-mail account. When the preservation request was made, there were about 980 e-mails in the account. The logs showed that the deletions were made by someone utilizing an IP address in the PRC. *See also Meng*, No. CR 04-20216-JF at ¶ 37 (Superseding Indictment alleging: "It was further part of the conspiracy that defendant XIAODONG SHELDON NIENG, directed, and caused to be directed, another person unknown to the Grand Jury, to delete approximately nine-hundred sixty-six (966) emails from defendant XIAODONG SHELDON MENG's account at smeng~cn@yahoo.com.cn.") The defendant remained in custody during this time in Florida, pending his transportation to the Northern District of California. The defendant was unable to access his e-mail account while in custody. Since the deletion activity occurred after the defendant's federal arrest, questions were raised whether the person(s) responsible may have violated obstruction of justice statutes.

Since the e-mail account was preserved, the e-mail provider gave law enforcement all of the 980 e-mails from the account after service of the search warrant. Many of these e-mails were important to further the investigation and were ultimately used in the superseding indictment or other court documents. The case presented many challenges, particularly since much of the activity occurred in the Far East and there was little ability to interview witness or pursue other common investigation avenues. Ultimately, defendant Meng pled guilty to the two most serious counts for violating § 1831 of the Economic Espionage Act and also the Arms Export Control Act. 18 U.S.C. § 1831 (2008); 22 U.S.C. § 2778 (2004).

B. Records are often in more than one place

Another important attribute of electronic evidence is that records may often be in more than one place. For example, if an e-mail is transmitted from co-conspirator A to co-conspirator B, records of the e-mail may be found in at least four places, including (1) co-conspirator A's computer, (2) co-conspirator B's computer or device used to receive the communication, (3) the internet service provider used by co-conspirator A to transmit the message, and (4) the internet service provider used by co-conspirator B to receive the e-mail. Additionally, if the sender tries to delete the e-mail from his computer, it may be located in unallocated space on his computer. It may also be on the recipient's computer or in other internet service provider records.

With this information, it may be possible to search multiple locations to piece together the central communications or events in the case. Investigators should develop a plan to coordinate legal process (such as executing simultaneous search warrants for the computers used by co-conspirators A and B).

C. Obtaining electronic evidence abroad: 24/7 High Tech Crime Network

Many trade secret and economic espionage cases have international dimensions. The defendant may be planning to form a company in another country to develop and produce the trade secret. There may be co-conspirators abroad. The defendant may have designs on selling the trade secrets outside the United States. Efforts to obtain electronic evidence abroad can introduce separate challenges, including delay in obtaining the records.

In addressing this problem, the 24/7 High Tech Crime Network was established to provide a law enforcement point of contact, 24 hours a day, 7 days a week. Presently, there are about 55 member countries. The network supplements but does not replace traditional methods of obtaining evidence and does not compete with the Legal Attaché (or Legat) Network. It is an important tool that can be used promptly to augment these traditional resources, which is vital in the era of electronic evidence. Typically, 24/7 High Tech Crime Network will be used to preserve evidence in the foreign country and the request is followed up with a Mutual Legal Assistance Treaty request. The 24/7 High Tech Crime Network ensures that immediate attention is given to the law enforcement request.

Each member country has a legal point of contact designated to respond to law enforcement requests to collect evidence either in electronic form or involving investigations or proceedings concerning criminal offenses related to computer systems and data. In the United States, CCIPS in the Criminal Division of the U.S. Department of Justice, serves as the point of contact.

Prosecutors or agents in the United States may contact CCIPS to obtain electronic evidence abroad. Alternatively, law enforcement officials in other countries may contact CCIPS to obtain electronic evidence in the United States.

There are many examples where law enforcement officials successfully used the 24/7 High Tech Crime Network to preserve and request evidence on services in the United States to aid pending cases involving an imminent threat of harm or other offenses. Similarly, if your case involves evidence in electronic form, or investigations or proceedings concerning criminal offenses related to computer systems and data in a member country, the 24/7 High Tech Crime Network can assist in requesting this evidence.

V. Developing an electronic evidence case plan at the inception of the case

A. Two key questions

Since electronic evidence may be retained for only a brief period or may be located in more than one place, it is important to consider electronic evidence early in the investigation, preferably upon the opening of the case. As part of an Electronic Evidence Case Plan, investigators and prosecutors may want to focus on two central questions. This will help concentrate the investigation on issues such as the timing of executing any search warrants or obtaining other legal process. The two questions are:

Q1: Do you have electronic evidence in the case, such as on or in computers, laptops, e-mails, chat communications, other Internet records, or financial transactions?

Q2: Can the evidence be found in more than one place?

On the *first* question, consider the following factors:

- How is the defendant communicating with others (i.e., chat, e-mail, cell phone)?
- What access does the defendant have to networks containing the trade secrets?
- What media is being used to access or transfer the trade secret information?
- What kinds of electronic records reflect the transactions under investigation?
- What computers/devices are being used by the defendant?
- Is the computer an instrument of the crime or a storage platform?
- What is the retention period for the different forms of electronic evidence?

On the *second* question, consider:

- Tracing the communications or transmission from the source to the destination
- What legal processes are required to obtain the evidence?
- A search warrant for the contents of communications and any other records under 18 U.S.C. § 2703;
    - A Section 2703(d) order for non-contents, including user connection logs and transactional records;
    - A grand jury subpoena for non-content information such as account holder name and history, session times and durations, length of service and types of service utilized, and means and source of payment for such service, under 18 U.S.C. § 2703(c)(2); or
    - A traditional search warrant under FED. R. CRIM. P. 41 for computers, electronic equipment, and other related evidence.
- If the defendants possess their own computers, what computers and networks are likely to be found if search warrants are executed at their residence or place of business?
- Is there electronic evidence abroad that the 24/7 High Tech Crime Network may assist in preserving and requesting?

If the answer to either of the two questions is yes and the information is stored by providers, then promptly issue § 2703(f) preservation requests. The Electronic Communications and Privacy Act contains a preservation request provision. Section 2703(f)(1) provides: "A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."

This provision allows an agent or prosecutor to make a request to preserve electronic records within the scope of the investigation, pending appropriate legal process. Under § 2703(f)(2), the provider must retain the records, pending legal process, "for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity."

For electronic evidence that is not maintained by a provider, which does not require a § 2701(f) preservation request, consider the legal processes that may be used to obtain the evidence. This may include a search warrant on one or more locations, depending on where the evidence is stored.

B. Other recommended steps

As part of the Electronic Evidence Case Plan, there are other steps that can be effective. If electronic evidence is identified early in the case, another recommended step is for early consultation between the prosecutor, agent, and forensic examiner. This three-way discussion may highlight particular places to look for evidence or focus on legal issues concerning the best ways to obtain it.

Timing is certainly important in any criminal case. Consider coordinated legal strategy and timing to obtain the electronic evidence. The existence of the investigation will not be revealed if a search warrant is issued to an internet service provider for e-mail accounts. However, if a search warrant is executed at a business or residence for evidence on a computer or server, then others will learn about the

existence of the evidence. These factors will weigh in the balance on the timing of any necessary and coordinated legal process.

These suggestions for identifying and obtaining electronic evidence early in the case will enhance the prospects that this evidence can be effectively used in the trade secret investigation. By identifying electronic evidence early in the case, the proper and best steps can be pursued to obtain it. As already noted, electronic evidence has provided some of the best evidence in trade secret and economic espionage cases.

VI. Conclusion

In recent trade secret and economic espionage cases, the electronic evidence that was obtained early was significant to advance the investigation or to present as evidence at trial. It is therefore important to identify electronic evidence early in the case. One way to further this objective is to consider an Electronic Evidence Case Plan. The plan can be tailored to the facts of the case by asking whether there is electronic evidence in the case and how many places that evidence may be found. The answers to these questions will guide preservation requests for the electronic evidence and the timing of any legal process. Electronic evidence can help fill in gaps in the investigation or open a window on the activities of the defendant or co-conspirators in misappropriating trade secrets.❖

ABOUT THE AUTHOR

❑ **Mark L. Krotoski** presently serves as the National Computer Hacking and Intellectual Property (CHIP) Coordinator at the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. He previously served as Deputy Chief and Chief of the Criminal Division in the U.S. Attorney's Office for the Northern District of California and as a CHIP Prosecutor in the U.S. Attorney's Offices for the Northern and Eastern Districts of California.✠

Border Searches In Trade Secret and Other Cases

Evan Williams
Trial Attorney
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

United States law enforcement authorities have broad power to conduct warrantless searches of persons, baggage, objects, vehicles, and vessels at this country's borders. Coincident with this authority, border officials track the entry and exit of all persons crossing the nation's borders. In the case of air travelers, officials have authority to access to the airlines' flight reservation system, allowing them to determine in advance when an individual will be crossing the border.

Border search authority, which finds ample support in case law and statute, is based in broad part upon the sovereignty of the United States, the need to insure the security of its citizens, and the power to enforce customs duties. Even before passage of the Constitution, customs authorities were given "full power and authority" to conduct a warrantless search of any ship or vessel which might be carrying goods subject to duty. Act of July 31, 1789, ch. 5, 1 St. 29. Since then, the Supreme Court and lower courts have repeatedly affirmed the government's power to conduct border searches. *See United States v. Villamonte-Marquez*, 462 U.S. 579, 585 (1983) (border searches have long "historical pedigree").

Border search authority has proved especially useful for investigating violations of the Economic Espionage Act. 18 U.S.C. §§ 1831-32. The targets of these investigations often attempt, on short notice, to leave the United States with misappropriated trade secrets or associated information. In fact, the target's sudden travel plans may be precisely what alerts the trade secret owner to the theft. As a result, the owner's first opportunity to apprise law enforcement of the suspected theft is when the target is literally on the way to the airport, leaving little or no time to obtain a search warrant. Similarly, the targets may return to the United States after an indefinite stay abroad. It can be extremely helpful for law enforcement to be able to both track the target's arrival and to search her belongings. *See, e.g., United States v. Fei Ye*, 436 F.3d 1117, 1119 (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 . . . from defendants' personal luggage, homes, and offices"); *United States v. Jin*, Case No. 08 CR 192 (N.D. Ill. Dec. 9, 2008) (indictment alleging that the defendant "traveled to O'Hare International Airport in Chicago, Illinois, for the purpose of departing to China" and "had in her possession over 1,000 electronic and paper documents belonging to Company A containing technical information, certain of which were marked as containing confidential and proprietary information belonging to Company A") *Id.* at 3; *United States v. Meng*, Case No. CR 04-20216-JF (N.D. Cal. Aug. 29, 2007) (plea agreement factual basis stating that after the defendant arrived in the United States "at the Minneapolis St. Paul International Airport on a flight originating from Beijing, the People's Republic of China," with his laptop computer, "My computer was initially viewed by U.S. Customs & Border Protection (CBP) Officers at the airport who noticed that Quantum3D properties were on my laptop. A subsequent examination of my computer revealed the Mantis 1 S.5, and the source code of viXsen embedded in the source code of Mantis, as well as other Quantum3D programs and materials that I had misappropriated from Quantum3D.")

This article is designed to help any prosecutor who is contemplating a border search or assessing whether evidence obtained from one is admissible. First, it will lay out the basic legal principles of border searches. Second, it will summarize the border search policies of Immigration and Customs Enforcement (ICE) and Customs and Border Protection (CBP), the main agencies tasked with protecting the borders, for electronic devices. Finally, it will describe practical tools, such as flight reservation databases, which law enforcement can use to track an individual's passage over the borders. Border search issues have been important in a number of trade secret cases as individuals attempt to leave or enter the United States with misappropriated trade secret materials.

II. Basic legal principles

This section of the article is based largely on a monograph entitled "Border Searches and Seizures," revised in May 2009, issued by the Counterterrorism Section of the National Security Division of the Department of Justice.

Border search authority allows authorized law enforcement agents to conduct warrantless searches of persons, baggage, objects, vehicles, and vessels crossing the nation's borders. In general, no heightened level of suspicion is required. The Supreme Court has recognized that this is reasonable and necessary to protect the sovereignty of the United States. *See United States v. Ramsey*, 431 U.S. 606, 616 (1977).

This authority, while broad, is circumscribed primarily by three factors. First, the search must occur at the border, with certain narrowly-defined exceptions. Second, only certain classes of law enforcement agents are authorized to conduct border searches. Third, the extent of border search authority depends on what is being searched.

A. Defining the border

Border searches must occur at the border, with certain narrowly-defined exceptions. The border is made up of three components. First, there is the geographical border. Second, there are "functional equivalents" of the border. Third, courts have recognized "extended borders."

As an initial matter, border search authority and its limitations extend equally to those entering and exiting the United States. *See United States v. Abbouchi*, 502 F.3d 850 (9th Cir. 2007); *United States v. Boulelhem*, 339 F.3d 414 (6th Cir. 2003); *United States v. Ezeiruaku*, 936 F.2d 136, 143 (3d Cir. 1991); *United States v. Berisha*, 925 F.2d 791, 795 & n.8 (5th Cir. 1991); *United States v. Hernandez-Salazar*, 813 F.2d 1126, 1138 (11th Cir. 1987); *United States v. Udofot*, 711 F.2d 831, 839-40 (8th Cir. 1983); *United States v. Ajlouny*, 629 F.2d 830, 834 (2d Cir. 1980).

The geographical border is made up of land, sea, and air borders. The land borders lie between the United States and Canada and the United States and Mexico. *See United States v. McPherson*, 664 F.2d 69, 72 (5th Cir. 1981). The sea borders generally comprise the territorial waters of the United States, which extend up to three miles off the nation's coasts. *Id.* For CBP enforcement purposes, however, "customs waters" extend up to 12 miles off the coasts. 19 U.S.C. §§ 1401, 1581 (2008). The air borders extend upward directly from the land and sea borders.

The "functional equivalents" of the border include locations where persons or things are effectively entering or exiting the United States even though they do not lie on one of the geographical land, sea, or air borders. No particularized suspicion is required for searches at functional equivalents of the border. *See United States v. Cardenas*, 9 F.3d 1139, 1148 (5th Cir. 1993). For example, the nation's

international airports, even those such as St. Louis or Chicago which are located in the heartland, are functional equivalents of the border for persons and things originating directly from or heading directly to foreign destinations. *See United States v. Almeida-Sanchez*, 413 U.S. 266, 272-73 (1973) (Lambert-St. Louis International Airport functional equivalent of the border for air travelers arriving directly from Mexico City). This extends to structures connected to the airports. *See United States v. Ramos*, 645 F.2d 318 (5th Cir. 1981) (proper to conduct border search of customer who returned to Customs area from lobby of hotel attached to airport terminal). Similarly, private planes that fly some distance into the United States before they can be practically or safely stopped by law enforcement are subject to border searches on the theory that their landing spot is the functional equivalent of the border. *See United States v. Garcia*, 672 F.3d 1349, 1363-64 (11th Cir. 1982) (private plane monitored by law enforcement from time it crossed air border); *United States v. Stone*, 659 F.2d 569 (5th Cir. 1981) (same).

The same principles apply on water and land. Inland waters with direct access to the oceans are functional equivalents of the border. *See Villamonte-Marquez*, 462 U.S. at 579. A railroad yard where trains arrive directly from or depart directly to foreign locations is the functional equivalent of the border. *See United States v. Boumelhem*, 339 F.3d at 414 (6th Cir. 2003). Private consignment hubs for international shipping, such as those for Federal Express or United Parcel Service, are considered functional equivalents of the border. *See United States v. Seljan*, 547 F.3d 993 (9th Cir. 2008) (Federal Express); *United States v. Abbouchi*, 502 F.3d at 850 (9th Cir. 2007) (United Parcel Service).

In sum, there are three factors to be considered in determining whether a search occurred at the "functional equivalent of the border":

- Whether there is reasonable certainty that an international border was crossed
- Whether there was opportunity for the object of the search to have changed materially since crossing the border
- Whether the search occurred at the earliest practical point after the border crossing.

United States v. Hill, 939 F.2d 934, 936 (11th Cir. 1991). The "extended border" doctrine also permits border searches at locations remote from actual geographical borders but requires "reasonable suspicion" of criminal activity. *See Cardenas*, 9 F.3d at 1148. A search at the "extended border," unlike one at the functional equivalent of the border, need not occur at the earliest practical point after the border crossing, and thus permits searches further away from the border. *See Hill*, 939 F.2d at 934. Because this makes the extended border search more intrusive, however, courts demand a heightened level of suspicion, along with other factors:

- Reasonable certainty the border was crossed
- Reasonable certainty that the person or thing searched had not changed condition since crossing the border
- Reasonable suspicion of criminal activity.

See Cardenas, 9 F.3d at 1148. The *Cardenas* court defined "reasonable certainty" as more than probable cause, but less than proof beyond a reasonable doubt.

B. Who may conduct border searches

Border searches must be conducted only by authorized border law enforcement agents. In most cases, this means either ICE or CBP, which have concurrent jurisdiction to enforce the customs and immigration laws of the United States. *See* 8 U.S.C. §§ 1225 and 1357 (2009); 19 U.S.C. §§ 482, 1499,

1581, and 1582 (2008). The United States Coast Guard also has officers authorized to enforce customs laws and therefore to conduct border searches. *See* 14 U.S.C. § 143 (2008); 19 U.S.C. § 1401(I) (2008). In rare instances, the Secretary of the Treasury may delegate border search authority to outside law enforcement personnel who "may perform any duties of an officer of the Customs Service." *Id.*

So long as authorized agents conduct the border search, the presence of other law enforcement agents does not invalidate it. First, ICE and CBP agents have statutory authority to seek assistance when necessary from other law enforcement agencies. *See* 19 U.S.C. § 507. Second, the presence of other law enforcement agencies does not detract from the authority of authorized border agents to conduct warrantless searches pursuant to their role as guardians of the border. *See Boumelhem*, 339 F.3d at 414; *United States v. Gurr*, 471 F.3d 144 (D.C. Cir. 2006); *United States v. Schoor*, 597 F.2d 1303 (9th Cir. 1979). *Compare United States v. Soto-Soto*, 598 F.2d 545 (9th Cir. 1979) (ordering suppression where FBI agent conducted border search of vehicle without assistance of border personnel or delegation of authority from Secretary of Treasury).

C. What is being searched

The extent of border search authority depends on what is being searched. The main distinction is between persons and things. There are also special rules for documents and mail. Ultimately, differences are based on the level of intrusion of the search.

Persons: All persons crossing United States borders are subject to search. *See United States v. Montoya de Hernandez*, 473 U.S. 531 (1985); 19 U.S.C. § 1582 (2008). No particularized suspicion is necessary for "routine" searches. *Montoya de Hernandez*, 473 U.S. at 538.

"Non-routine," or more intrusive border searches of persons, however, may require "reasonable suspicion." *Id*. at 541 (holding that reasonable suspicion is required to detain a traveler in order to monitor her bowel movements for contraband in her alimentary canal but expressly declining to rule on other "non-routine border searches such as strip, body-cavity, or involuntary x-ray searches"). In so holding, the Supreme Court cited its conclusion some 20 years prior that "[t]he interests in human dignity and privacy which the Fourth Amendment protects forbid any such intrusion [beyond the body's surface] on the mere chance that the desired evidence might be obtained." *Id.* at 540, n. 3 (quoting *Schmerber v. California*, 384 U.S. 757, 769-70 (1966)).

The Supreme Court has not yet revisited the issue of non-routine border searches of persons. The Circuit Courts which have considered the issue, however, have generally required border agents to have reasonable suspicion for non-routine searches involving any significant intrusion on privacy, such as involuntary x-rays. *See United States v. Vega-Barvo*, 729 F.2d 1341 (11th Cir. 1984) (requiring "reasonable suspicion" even for a *consensual* x-ray). It seems likely that the results of any such search initiated upon less would be suppressed. *See United States v. Braks*, 842 F.2d 509 (1st Cir. 1988) (denying suppression of drugs which smuggler pulled voluntarily from her girdle following a pat-down by Customs officials but noting that had agents conducted a strip search, "reasonable suspicion" would have been required). The First Circuit set out a six-prong test for determining whether a non-routine border search required "reasonable suspicion":

- Whether the search resulted in exposure of intimate body parts or required disrobing
- The degree of physical contact between the Customs official and the individual being searched
- Whether force was used

- Whether the search exposed the individual to pain or danger
- Whether the individual's reasonable expectation of privacy (if any) was abrogated
- The overall manner in which the search was conducted.

Id. at 512. **Things:** All baggage, vehicles, and vessels crossing the nation's borders are subject to search. 19 U.S.C. §§ 1496, 1581 and 1582 (2008). Moreover, border officials may use force, if necessary, to stop vehicles and vessels. 19 U.S.C. § 1581 (2008). This is primarily so that CBP and ICE officials can enforce the nation's customs laws.

Thus far, the courts have not required particularized suspicion for any searches of baggage, vehicles, or vessels. The analysis which applies to persons, especially regarding intrusion on privacy, simply does not carry over to things. *See United States v. Flores-Montano*, 541 U.S. 149 (2004) (declining to suppress contents of gas tank which was removed from vehicle and dismantled even though border officials did not have reasonable suspicion that a crime had been committed). The Supreme Court however, declined to rule out the possibility that a search conducted in a "particularly offensive manner" might violate the Fourth Amendment. *Id.* at 154, n.2 (quoting *United States v. Ramsey*, 431 U.S. 606 (1977).

Documents: The seizure of documents during border searches has been somewhat more controversial. While the courts have generally recognized that the documents, just like other objects, may be inspected, there is some dispute about whether and under what circumstances they may be copied. This appears to turn on whether the materials copied are evidence of customs violations or other crimes. Moreover, the proliferation of laptop computers and handheld devices, like Blackberries, which can contain thousands of documents, has raised new questions.

The courts have clearly recognized that border search authority gives law enforcement the right to read documents. *See United States v. Seljan*, 547 F.3d 993 (9th Cir. 2008) (upholding border search of Federal Express package and reading of correspondence inside). In fact, the enforcement of certain statutes, such Title 19, United States Code, § 1305, which prohibits the importation of obscene materials, practically requires it. *See United States v. 12 200-Ft. Reels of Super 8mm Film*, 413 U.S. 123 (1973) (upholding Constitutionality of 19 U.S.C. § 1305).

Copying the documents pursuant to border search authority is not so clear. For instance, as discussed more fully below, CBP and ICE policies allow copying of information contained in electronic devices for the purpose of inspection, but require destruction of those copies if no evidence of customs violations or other crimes is found. Courts have differed on whether border search authority permits agents to copy documents. *See United States v. Rodriguez*, 995 F.2d 776, 778 (7th Cir. 1993) (upholding copying of documents as border search because this simply preserved the border officer's eyewitness observations); *United States v. Fortna*, 796 F.2d 725 (5th Cir. 1986) (same); *but see United States v. Cardona*, 769 F.2d 625, 629 (9th Cir. 1985) (border search authority did not allow copying of cashier's checks which were not evidence of currency violation enforced by border officials).

So far, circuit courts have upheld warrantless border searches of laptop computers, Blackberries, and other handheld electronic devices. *See United States v. Arnold,* 523 F.3d 941 (9th Cir. 2008) (no particularized suspicion required for border search of laptop because it is analogous to a container); *see also United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005). In a recent district court case, the magistrate, later affirmed by a federal court, suppressed the contents of a laptop computer primarily because it was taken 170 miles from the border for inspection and held for 2 days. The judge determined that the search occurred at the "extended border," and thus required reasonable suspicion of criminality. *See United States v. Cotterman*, No. CR 07-1207-TUC-RCC, 2009 WL 465028 (D. Ariz. Feb. 24, 2009). Even this decision, however, which the government has appealed, does not seem to contravene generally the

findings of the *Arnold* and *Ickes* courts that reasonable suspicion is not required for ordinary border searches of computers.

Mail: Mail handled by the United States Postal Service (as opposed, for instance, to packages handled by private companies such as Federal Express or United Parcel Service) is subject to border search with certain exceptions. Generally, border officials may not open sealed correspondence (or what appears to be solely correspondence) or letter class mail weighing less than 16 ounces. *See* 19 U.S.C. § 1583 (2008); 19 C.F.R. § 145 (2009).

III. ICE and CBP policies for border searches of electronic devices

ICE and CBP have both promulgated policies to give agents more specific guidance in conducting border searches. While these policies are based in part on statute and case law, both agencies have implemented more restrictive policies than the controlling law allows. This appears to be because courts, as discussed above, have generally been reluctant to place limits on all but the most intrusive and/or offensive border searches. In addition, as a practical matter, the agencies do not want to generate litigation that might result in more stringent limits on border searches.

Two recent documents, one from ICE and one from CBP, lay out procedures for border searches of information in electronic devices. As discussed above, this is the category of border search most likely to generate litigation, because the law is more settled for persons, things, and mail. The ICE directive entitled "Border Searches of Electronic Devices," issued August 18, 2009 (ICE Information Policy), sets forth:

> legal guidance and . . . policy and procedures within U.S. Immigration and Customs Enforcement (ICE) with regard to border search authority to search, detain, seize, retain, and share information contained in electronic devices possessed by individuals at the border, the functional equivalent of the border, and the extended border to ensure compliance with customs, immigration, and other laws enforced by ICE.

ICE Information Policy, ¶ 1.1. The CBP directive entitled "Border Search of Electronic Devices Containing Information," dated August 20, 2009 (CBP Information Policy), similarly sets forth

> guidance and standard operating procedures for searching, reviewing, retaining, and sharing information contained in computers, disks, drives, tapes, mobile phones and other communications devices, cameras, music and other media players, and any other electronic or digital devices, encountered by U.S. Customs and Border Protection (CBP) at the border, both inbound and outbound, to ensure compliance with customs, immigration, and other laws that CBP is authorized to enforce.

CBP Information Policy, ¶ 1.

A. The policy

> The basic policies of ICE and CBP, especially in light of the recent *Arnold* decision, both take the position that agents may conduct border searches of electronic devices without individualized suspicion. ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion, consistent with the guidelines and applicable laws set forth [in the ICE Information Policy]. Assistance to complete a border search may be sought from other Federal agencies and non-Federal entities, on a case by case basis, as appropriate. When U.S. Customs and

> Border Protection (CBP) detains, seizes, or retains electronic devices, or copies of information therefrom, and turns such over to ICE for analysis and investigation (with appropriate documentation), ICE policy will apply once it is received by ICE. Nothing in this policy limits the authority of Special Agents to make written notes or reports or to document impressions relating to a border encounter in ICE's paper or electronic record keeping systems.

ICE Information Policy, ¶¶ 6.1-6.3.

> In the course of a border search, with or without individualized suspicion, an Officer may examine electronic devices, and may review and analyze the information encountered at the border, subject to the requirements and limitations provided [in the CBP Information Policy] and applicable law.

CBP Information Policy, ¶ 5.1.2. Officer is defined as a "Customs and Border Protection Officer, Border Patrol Agent, Air Interdiction Agent, Marine Interdiction Agent, Internal Affairs Agent, or any other official of CBP authorized to conduct border searches." CBP Information Policy, ¶ 3.1.

B. Detention

Both ICE and CBP take the position that they may detain documents and electronic media crossing the border for a "reasonable time" to review them. ICE Information Policy, ¶ 8.3; CBP Information Policy, ¶ 5.3.1. While neither agency's policy defines "reasonable time" per se, ICE does set out the following factors for agents to consider:

- The amount of information needing review;
- Whether the traveler was deprived of his or her property and, if so, whether the traveler was given the option of continuing his or her journey with the understanding that ICE would return the property once its border search was complete or a copy could be made;
- Whether assistance was sought and the type of such assistance;
- Whether and when ICE followed up with the agency or entity providing assistance to ensure a timely review;
- Whether the traveler has taken affirmative steps to prevent the search of his or her property in a timely fashion; and
- Any unanticipated exigency that may arise.

ICE Information Policy, ¶ 8.3(3). Both agencies stipulate that this includes making copies. ICE Information Policy ¶ 8.1(4); CBP Information Policy, ¶ 5.3.1. Both add, however, that the copies must thereafter be destroyed if there is no probable cause to seize them. ICE Information Policy, ¶ 8.5(1)(e); CBP Information Policy, ¶ 5.3.1.2. Both agencies require documentation of all steps taken by the detaining officers. ICE Information Policy, ¶ 8.2; CBP Information Policy, ¶ 5.5.

C. Assistance from other federal agencies and entities

Both agencies allow agents to seek assistance from other federal agencies or non-federal entities for translation, decryption, and other technical assistance. ICE Information Policy, ¶ 8.4(1); CBP Information Policy, ¶ 5.3.2.2. No individualized suspicion is required; the reasoning is that without this assistance, the

agents cannot even read the documents or electronic media. *Id.* Both agencies also allow agents to seek assistance from other federal agencies or non-federal entities for "subject matter" assistance, but require that an agent have "reasonable suspicion of activities in violation of the laws enforced by [his agency]." ICE Information Policy, ¶ 8.4(2); CBP Information Policy, ¶ 5.3.2.3. Both agencies also set time limits for the assistance to be rendered—30 days for ICE and 15 days for CBP—with extensions requiring supervisory approval. ICE Information Policy, ¶ 8.4(5); CBP Information Policy, ¶ 5.3.3.2.

D. Retention and sharing

Generally, ICE and CBP may retain and/or seize information from a border search only if they have "probable cause of unlawful activity." ICE Information Policy, ¶ 8.5(1)(a); CBP Information Policy, ¶ 5.4.1.1. Probable cause is not required to retain immigration documents but they must be handled under the "privacy and data protection standards of the system in which such information is retained." ICE Information Policy, ¶ 8.5(1)(b); CBP Information Policy, ¶ 5.4.1.2.

Both agencies permit agents to share information from a border search with "[f]ederal, state, local, and foreign law enforcement agencies" in accordance with applicable law and policy. ICE Information Policy, ¶ 8.5.(1)(c); CBP Information Policy, ¶ 5.4.1.3. The applicable law is quite favorable to the government. *See United States v. Gargotto*, 476 F.2d 1009, 1014 (6th Cir. 1973) (evidence obtained by one police agency may be shared with another without a warrant). On the other hand, an agency from which ICE or CBP sought assistance in order to read or understand the documents may retain copies only if it has "independent legal authority to do so—for example, when the information is of national security or intelligence value," and must inform ICE or CBP of its intention to do so. ICE Information Policy, ¶ 8.5(2)(c); CBP Policy, ¶ 5.4.2.3.

E. Special categories

Both agencies set out special rules for the following categories of information, among others: (i) business or commercial information, (ii) medical records, and (iii) legal information. Both agencies require agents to treat business information as if it is confidential and to make sure that it is not subject to unauthorized disclosure. Both cite the possible ramifications of the Trade Secrets Act and the Privacy Act. ICE Information Policy, ¶ 8.6(2)(a); CBP Information Policy, ¶ 5.2.3. Both agencies warn agents that they may encounter attorney-client privileged material. In such a case, they are to seek advice from agency counsel or the local United States Attorney's office before proceeding any further. ICE Information Policy, ¶ 8.6.(2)(b), CBP Information Policy, ¶ 5.2.1.

IV. Border enforcement lookout tools

There are a number of databases which ICE and CBP use to monitor the movement of individuals crossing the nation's borders. The most complete are those with information about air passengers, which pull data primarily from the airline data bases.

A. Treasury Enforcement Communications System (TECS)

The Treasury Enforcement Communications System (TECS) is an overarching repository for law enforcement and investigative information to which all federal law enforcement agencies have access in varying degrees. TECS comprises several modules which are available to and used by appropriate federal

law enforcement agencies for screening and targeting, among other purposes. One is the Automated Targeting System, the primary database for the Department of Homeland Security, which is described in more detail below. The Advanced Passenger Information System (APIS) is another, in which an airline or sea carrier electronically transmits a passenger manifest to Customs a prescribed period of time prior to crossing the United States border.

B. Automated Targeting System (ATS)

The Automated Targeting System (ATS) is used by agents with the Department of Homeland Security, which includes both ICE and CBP. ATS, in turn, comprises six components:

- ATS-N, for screening inbound or imported cargo
- ATS-AT, for screening outbound or exported cargo
- ATS-L, for screening private passenger vehicles crossing at land border ports of entry using license plate data
- ATS-I, for cooperating with international customs partners in shared cargo screening and supply chain security
- ATS-TAP, for assisting tactical units in identifying anomalous trade activity and performing trend analysis
- ATS-P, for screening travelers and conveyances entering the United States in the air, sea and rail environments.

System of Records Notice for the Automated Targeting System, issued August 3, 2007 (SORN-ATS).

ATS-P is the most important component for law enforcement agents seeking to track individuals. It maintains Passenger Name Record (PNR) data, which is the information provided to airlines and travel agents by or on behalf of air passengers seeking to book travel. PNR data, which in turn comes from the industry's Air Carriers Reservation System, comprises some or all of the following, depending upon availability:

- PNR record locator code
- Date or reservation/issue of ticket
- Date(s) of intended travel
- Name(s)
- Available frequent flier and benefit information
- Other names on PNR
- All available contact information
- All available billing/payment information
- Travel itinerary
- Travel agency/agent
- Travel status of passenger
- Ticketing information

- Baggage information
- Seat information
- Any collected APIS information
- All historical changes to the PNR.

SORN-ATS at 14. Queries made on the ATS-P system will provide field agents with notification of a "hit" when PNR data is dumped into the system.

C. Reservation monitoring

Reservation Monitoring (ResMon) is a database available to select ICE and CBP assets, primarily the airport "Passenger Analysis Units," which contains all of the information that an airline views upon pulling up a reservation. It is analogous to having "read only" access to an airline agent's terminal, except that it contains itinerary data only for travel crossing the United States border, not purely domestic or foreign travel. Most of the information in ResMon is also available in the ATS-P database, with the exception of credit card numbers, frequent flier information, and the like. ResMon queries give agents notice when an individual makes a reservation for cross-border travel.

V. Conclusion

Border searches are an extremely useful tool for law enforcement. They are particularly relevant in trade secrets investigations because of the frequency with which targets enter or exit the country shortly after misappropriating the secret. Like any warrantless search, however, they are not a substitute for a search warrant, and, if time permits, a warrant is preferable. Even if there is not time for a warrant, however, a border search will be most effective when border agents have at least some lead time and information on the suspected crimes of the individuals to be searched—especially for complex crimes such as theft of trade secrets.❖

ABOUT THE AUTHOR

❑ **Evan Williams** has served as a Trial Attorney in the Computer Crime and Intellectual Property Section of the United States Department of Justice since 2008. He previously served as Assistant U.S. Attorney in the Eastern District of New York, serving first in the General Crimes Division and later in the Long Island Division. Prior to that he was an Assistant District Attorney in the New York County District Attorney's Office, serving first in the Trial Division and later in the Investigations Division.✠

Addressing Sentencing Issues in Trade Secret and Economic Espionage Cases

Christopher S. Merriam
Assistant Deputy Chief
Intellectual Property, International and Policy Matters
Computer Crime and Intellectual Property Section
Criminal Division

I. Introduction

Sentencing in trade secret theft and economic espionage cases presents several potential hurdles not found with other types of offenses. Consequently, the prosecution team should prepare a strategy early in the case to anticipate sentencing issues and potential defense arguments, ensure a proper guideline calculation, and obtain a meaningful deterrent sentence upon conviction of a defendant. Among the issues of particular importance is the proper valuation of a trade secret and guideline factors that reflect the role of the defendant in the scheme to steal the trade secret.

As discussed below, valuation of the trade secret may be a thorny issue in several regards. Damage to the victim can vary greatly depending on when the offense is discovered. For example, consider the difference in pecuniary harm to a victim corporation that has its proprietary design stolen by an employee who is leaving to work for a competitor. The actual harm to the company may be small if the defendant is caught downloading confidential files at the time he announces his resignation, while the damage will be much greater if the defendant has already sent the downloaded files to a competitor overseas who then produces a less expensive knock-off of the victim company's product.

Not only may pecuniary harm vary, but the value of the trade secret itself can also be measured in different ways, with dramatically different results. For example, where a trade secret product has not yet been introduced, one common measure of value – the research and development cost – may be substantial, while another measure –the product's current market value – may be speculative or nonexistent at the time of the misappropriation. Conversely, trade secret information used to produce an existing product may be valued at the cost that the corporation would reasonably charge to license the formula, or, alternatively, by an estimate of the profits that a competitor could earn by producing a copy, whereas the cost of the original development of the trade secret might have been quite small.

Within the wide range of trade secret thefts that have been the subject of criminal investigation since the passage of the Economic Espionage Act in 1996, a majority of cases involve an insider in the victim company who has an understanding of, and access to, the trade secret. The role of the insider in these trade secret cases can raise guideline enhancement issues as a result of the use of a special skill and the violation of a position of trust. Even where specific guideline provisions may not apply, the prosecution team should look to develop a compelling story about the actions of the defendant for consideration by the court at sentencing. Many of the factors that trial courts are directed to consider under 18 U.S.C. §3553(a) (2003) can be presented to explain the damage caused by a particular defendant's conduct and the seriousness of the trade secret theft.

II. Sentencing overview

The maximum penalty for theft of trade secrets, in violation of 18 U.S.C. § 1832(a) (2008), is a prison sentence of 10 years, a fine of up to $250,000, a term of supervised release of 3 years, and a mandatory special assessment of $100. The longest prison sentence imposed in a trade secret case to date was 96-months. *See generally United States v. Williams,* 526 F.3d 1312 (11th Cir. 2008) (*per curiam*). The maximum penalty for economic espionage, in violation of 18 U.S.C. § 1831(a) (2008), is a prison sentence of 15 years, a fine of up to $500,000, a term of supervised release of 3 years, and a mandatory special assessment $100.

Restitution for the loss suffered by the victim and the return of stolen property is required at sentencing in trade secret and economic espionage cases. 18 U.S.C. § 3663(A) (2008). Although the loss amount for restitution purposes may match the guideline calculation for loss under section 2B1.1, some cases will require a separate calculation depending on the method used to determine loss under the Sentencing Guidelines.

Another important issue during the sentencing phase concerns the return of the trade secret materials. Prosecutors should seek to have the sentencing court include a provision for the return of any trade secret material in the order of restitution. By including a return of property term, the court will provide an additional assurance to the trade secret owner and will retain the power to punish any future misuse of the victim's trade secret material by the defendant with a contempt citation.

As a second avenue, the request for the return of the stolen property may also be required under the terms of a protective order. Normally, the protective order may specify that the trade secret materials shall be returned upon the conclusion of the case or after sentencing.

III. Guideline sentencing factors

A. Valuation (U.S. Sentencing Guidelines Manual §2B1.1(b) (2008))

Because the loss table in section 2B1.1(b) will have a significant impact on the guideline calculation in a case of trade secret theft, developing an accurate and defensible measure of the actual or reasonably foreseeable pecuniary loss to the trade secret owner from the defendant's conduct is a critical step in the development of a sentencing strategy. For definitions of "actual loss" and "intended loss," refer to U.S. Sentencing Guidelines Manual § 2B1.1(2008), Application Notes 3(A)(i),(ii).

Identifying a pecuniary loss figure for sentencing purposes may be complicated. In some instances a victim company will put a very high - and possibly unrealistic - value on its trade secrets. This may be based in part on a misunderstanding of how valuation operates under the Sentencing Guidelines. Conversely, a defendant may argue that, due to the circumstances of the particular case, the actual loss was small or nonexistent.

The goal of the prosecutor is often to find the balance point between the two extremes and to provide the sentencing judge with a meaningful basis to make findings as to the value. To do so, the prosecution team needs to develop a theory, or theories, of valuation and determine a method of proof to support the theory.

Since the Sentencing Guidelines section 2B1.1(b) loss table applies valuations ranges, precise determination of the valuation of the misappropriated trade secret is not necessary. In fact, the guidelines recognize that "[t]he court need only make a reasonable estimate of the loss." U.S. Sentencing Guidelines Manual § 2B1.1 (2008), Application Note 3(C).

The process of establishing a reasonable loss figure has resulted in hotly contested hearings requiring testimony at the sentencing phase of several trade secret cases. One case, involving the theft of

proprietary software used in making drivers' licenses, provides a good overview of the issues that the prosecution and court face at sentencing. *United States v. Ameri*, 412 F.3d 893 (8th Cir. 2005). The district court heard evidence of loss, including estimates of the value of the software, at the trial. Following the initial sentencing hearing, the district court was not comfortable with its understanding of the amount of loss. The district court then held second and third sentencing hearings to fully explore the issue. Following the hearings, the district court made detailed findings on loss which provide an overview of the issues that can arise at sentencing. The court eventually determined that:

- The development cost for the software was about $700,000.
- The software was not generally available for sale without an installation contract, so there was not a verifiable "fair market value."
- The stolen software was at the heart of the victim contractor's $10 million contract.
- The contractor's software, rather than the contractor's other services, comprised the bulk of the value for its clients.
- The defendant offered another person $200,000 to participate in fraudulent use of the software.
- An employee of the contractor estimated the fair market value for a copy of the software to be about $1 million.
- The defendant possessed two discs containing stolen copies of the software.
- The contractor spent between 300 and 500 man hours over the course of 2 years dealing with the fallout from the software theft.
- The software remained in service in many states and the contractor did not have to "repair" the software.

It is rare that this range of evidence relating to valuation will be available at sentencing, but the findings of the court suggest some of the possible means of assigning a value to the trade secret (and, perhaps, to avoid three sentencing hearings). Some possible methods for assessing the value of a trade secret are outlined below.

B. Valuation methods

Research and development costs of the trade secret. Using an estimate of the research and development costs associated with a trade secret can be a useful valuation method and an appropriate measure of pecuniary loss where the theft is intended as a shortcut allowing a competitor to avoid the time and expense involved in developing a competing product or procedure. Research and development costs may also be a straightforward method, as most businesses will track the costs associated with a particular project and should be able to provide testimony showing the investment in employee work hours, equipment costs, and other expenses related to the trade secret. Valuing a trade secret in this way has the additional advantage of being a widely-used measure for the valuation of assets, both in business accounting and transactions, and in court during civil litigation, so the court and parties may be on familiar ground.

Research and development costs may understate the loss in cases where the trade secret, while central to a profitable product or service, was developed without much expense or many years before. In May 2009, the U.S. Sentencing Guideline Commission submitted an amendment which expressly recognizes this factor as one that may be considered. Under the amendment, "the court *may* estimate loss

using the *cost of developing that information* or the reduction in the value of that information that resulted from the offense. The new provision responds to concerns that the guidelines did not adequately explain how to estimate loss in a case involving proprietary information such as trade secrets." Amendments to the Sentencing Guidelines, U.S. Sentencing Guideline Commission, (May 1, 2009) (emphasis added), *available at* http://www.ussc.gov/2009guid/20090501_Reader_Friendly_Amendments.pdf.

The advantages to using research and development costs to value a trade secret are that they provide an accurate estimate of the trade secret value and the proof comes in economic terms that are regularly used in a civil context. The disadvantages are that it may require expensive expert testimony and increased complexity of proof at sentencing, and that it may not accurately reflect the harm to the victim in a particular case, especially where the theft would not substantially reduce the victim's competitive advantage derived from the trade secret.

The amount for which the defendant sold or tried to sell the trade secret. Although not a traditional economic measure of the value of a trade secret, the cost set by a defendant in the "thieves' market" may be a useful measure of pecuniary harm in several scenarios. In cases where attempt or conspiracy are charged, either because the case is a government sting operation where no trade secret material is actually misappropriated, or where valuation of the trade secret in court would compromise the secrecy of the information, the price set by the defendant will often be the most accurate value. *See United States v. Hsu*, 155 F.3d 189 (3d Cir. 1998). Some types of trade secret information, including marketing plans, proprietary customer lists, or sales data, are otherwise hard to value.

In a case where government investigators are alerted to a trade secret theft early in the process and are able to arrange an undercover purchase of the stolen material, there may be compelling reasons to value the trade secret at the sale price offered by the defendant. Similarly, in a government sting operation where a defendant believes that he is purchasing stolen trade secrets, the price that the defendant is willing to pay can provide a measure of the intended pecuniary harm.

This method may be particularly useful in cases where the trade secret material is not a model, plan, or formula for a particular product, but rather relates to marketing or bid information which would be of value to a competitor, if known. For example, corporations regularly prepare cost estimates to be used in developing a competitive bid proposal for a contract. The value in maintaining the secrecy of this information prior to the submission of the bid is high, as the success of the proposal may turn on underbidding competitors. However, the value of the information will not match the cost of the underlying product, and the cost of developing the bid estimates may be substantially less than the value of maintaining the secrecy of the bid terms. In this case, the price negotiated by a defendant for the sale of the information may be the most straightforward method of valuing the trade secret. A similar argument can be made where the trade secret information consists of marketing plans or sales plans based upon customer data.

One clear advantage to this method of valuation is that the defendant has already endorsed the price and will have an uphill battle explaining to the court why the trade secret has a value less than the price set by the defendant. Another advantage is that the prosecutor may avoid testimony on the actual trade secret at trial.

The disadvantages to this method of valuation include the potential to underestimate "reasonably foreseeable pecuniary harm" and the fact that this method nominally validates a market for stolen trade secrets which may be substantially lower than the value assigned by the victim.

The amount for which similar trade secret information has been sold in the open market (such as the merger/acquisition price for the trade secret). In some cases, a trade secret may be similar to other information that the victim company has sold in the past, even if the particular trade secret itself was not available for sale or licensing. Some examples include the development of pharmaceutical or

chemical compounds that are intended for licensing and production by other corporations and where a consistent approach was taken by the developer of the trade secret in earlier negotiated agreements with legitimate businesses.

In other cases, trade secret information may be valued by the company internally as part of a merger or acquisition of the company or for regulatory filings requiring a valuation of company assets. Whatever method of loss calculation is used, to ensure consistency or to explain any discrepancy with the value asserted in court, prosecutors should seek to identify any Securities and Exchange Commission filings or publicly available accounting documents where the victim valued its trade secret information. While internal valuations may contain less detail than is ideal for sentencing purposes, these estimates can provide a good starting point for the prosecution team.

A reasonable licensing or royalty fee for the proprietary information, based on what a willing buyer would pay a willing seller in an arms-length transaction. Although trade secret material is not typically made available for use by others, in some cases an estimate of the reasonable fee that the trade secret owner would charge in a legitimate, arms-length transaction for use of the trade secret information can be used to determine the fee. In cases where the trade secret owner would not typically release the information outside the company, developing a reasonable royalty or licensing fee will often require the assistance of an independent expert.

While this method may provide an accurate measure of pecuniary harm to the victim under the circumstances, the victim may feel that the trade secret is undervalued in relation to the cost of development and the reasons for maintaining secrecy, and this method may also require the testimony of an outside expert to determine the value.

The fair market value of the business or product line that could be infringed upon by a competitor with access to the trade secret. In one scenario that has been repeated over the history of the Economic Espionage Act, the design specifications for a product are taken and the product is copied by a lower-priced manufacturer overseas. These cases are often discovered when the existing customers of the trade secret owner receive offers for a strikingly similar item at a reduced price.

In these cases, which may come to light long after the actual theft took place, it is reasonable to argue that the intended pecuniary harm is the entire market where the copycat product was intended to compete. This is particularly true where the trade secret material relates to a highly specialized item or industrial process that is only produced by one company. Some examples of this type of item include the trade secrets underlying a metallurgical process to manufacture truck chassis parts, machinery and chemical solutions used to increase the speed of placing lids on canned goods, and a computer-based system for refinishing automobiles using die-cut stickers matched to numerous makes and models of cars. Production records, sales trends, the expected life of the product, and market share data that may already be in the possession of the victim company will provide a valuation based on the existing market. In some instances, records and business plans from the defendant or the company manufacturing the copied products may also be available to show the intended loss.

The advantages to using this method include the fact that the value may be proved using existing data from the victim company and that it is an accurate measure of the intended pecuniary loss for small-market or highly specialized items. The disadvantage is that estimates of the future market share and product life may be difficult to acquire or overly speculative in industries where technology changes rapidly.

Any other methodology that calculates the reasonably foreseeable pecuniary losses caused by the defendant's conduct. Other methods for evaluating the loss suffered by the victim include an assessment of the costs to the victim in recovering from the theft and the costs of protecting confidential material from future misappropriation. Another method may include information showing the amount of

money spent on improving the security of computer networks, physical storage, and employees to prevent future theft. Where susceptible to determination, in appropriate cases, another factor may include "the reduction in the value of that information that resulted from the offense." *See* Amendments to the Sentencing Guidelines, U.S. Sentencing Guideline Commission, *available at* http://www.ussc.gov/2009guid/20090501_Reader_Friendly_Amendments.pdf. At the time of publication, it was undetermined whether this amendment would become effective by November 1, 2009, under the Sentencing Guideline rulemaking process.

C. Foreign instrumentality enhancement

In cases where economic espionage is charged, the Sentencing Guidelines expressly provide for a two-level enhancement where the defendant misappropriated a trade secret and "knew or intended that the offense would benefit a foreign government, foreign instrumentality, or foreign agent." U.S.S.G. § 2B1.1(b)(5). While the language of the enhancement tracks the economic espionage provision of § 1831, there may be instances where the conduct of the defendant warrants the enhancement contained in § 1832 trade secret prosecutions.

D. Other guideline factors

Chapter three of the Sentencing Guidelines includes other provisions that may be worthy of consideration, including the defendant's role in the offense.

The theft of trade secrets often involves a corporate insider who is able to access the trade secret material while at work. In some cases, the insider is able to facilitate and conceal the offense because of a managerial role in the victim corporation which results in less direct supervision and greater deference to the defendant's actions. In those cases, a two-level enhancement may be appropriate under section 3B1.1, which distinguishes, for example, the case of a bank executive's fraudulent loan scheme, where the enhancement would apply, from a theft or embezzlement by a bank teller, where it would not.

Similarly, the use of a special skill by the defendant may warrant a two-level enhancement under section 3B1.1. In trade secret cases, a special skill may include the use of a computer to access protected files in a corporate network or the use of work-related skills that are unusual and necessary for the completion of the offense. *See United States v. Lange*, 312 F.3d 263, 270 (7th Cir. 2002).

IV. Arguing § 3553(a) factors in trade secret cases

In light of the current discretion resting with the district court, application of the § 3553(a) factors has taken on greater importance in the sentencing for trade secret and economic espionage cases. *See generally Gall v. United States*, 552 U.S. 38 (2007) (expanding sentencing discretion of district courts). The theft of trade secrets is not prosecuted with the regularity of many other white collar crimes and the court may benefit from information regarding the damaging effects of trade secret theft under the § 3553 factors in fashioning an appropriate sentence.

The nature and circumstances of the offense may strongly demonstrate the need for a particular sentence, depending on the manner of misappropriation or use of the trade secret under § 3553(a)(1). The court may also wish to consider the specific steps taken by the defendant to injure the owner of the trade secret. The defendant may have sold the trade secret to a direct competitor or formed a new company to compete with the trade secret owner.

The offense may directly implicate the primary objectives of the Economic Espionage Act to promote national and economic security. *See, e.g.,* H. REP. NO. 788, 104th Cong., 2d Sess. 4 (1996). ("[T]he nation's economic interests are a part of its national security interests. Thus, threats to the nation's economic interest are threats to the nation's vital security interests.") For example, the trade secret may involve unique technological or military applications.

Given the facts of the case, a particular sentence may be necessary to reflect the seriousness of the defendant's conduct, promote respect for the law, and provide just punishment for the offense under § 3553(b)(2). *See, e.g.*, *United States v. Williams*, 526 F.3d 1312, 1323 (11th Cir. 2008) (per curiam) (Applying the § 3553 factors: "In describing why it found the offense to be so serious, the court discussed the harm that Coca–Cola could have suffered if Williams and her co-conspirators had succeeded in selling its trade secrets to a rival, and the danger to the United States economy these crimes pose.")

Under § 3553(a)(1), the personal history and characteristics of the defendant may reveal the motivations for engaging in the trade secret offense (such as for profit or to injure the owner of the trade secret), as well as disregard for conforming his conduct to the law, rules, commitments, and obligations expected of him, which further warrants imprisonment for a significant period of time. For example, it may be significant that in committing the misappropriation, an insider defendant may have breached non-disclosure and other confidentiality agreements and policies of the company.

Under § 3553(a)(2)(C), depending on the nature of the trade secret or the manner in which the offense was committed, it may be important to protect the public from individuals who commit economic espionage and trade secret theft. Similarly, despite the relatively small number of trade secret theft prosecutions annually, there is a substantial opportunity to deter others from committing similar offenses. The deterrent effect of a substantial sentence for trade secret theft tends to carry far beyond the immediate area of the case as business journals and legal scholars disseminate the information to a broad audience. The House Report noted that one of the goals of the statute was to promote deterrence, stating that "these problems [under prior law] underscore the importance of developing a systematic approach to the problem of economic espionage. The Committee believes that such a scheme will serve as a powerful deterrent to this type of crime." H. REP. NO. 788, 104th Cong., 2d Sess. 7 (1996). The Computer Crime & Intellectual Property Section (CCIPS) maintains the Web site, www.cybercrime.gov, and posts press releases containing information about charges and convictions under the Economic Espionage Act and other intellectual property and computer crimes. In addition, CCIPS also maintains a separate intranet for prosecutors which includes sentencing memoranda and other information for many trade secret and economic espionage cases.

These examples illustrate the importance of applying the § 3553 sentencing factors to the facts of the specific trade secret or economic espionage case. This application will allow the court to impose an appropriate sentence based on the facts of the case.

V. Conclusion

Sentencing in trade secret and economic espionage cases can present unique challenges to the prosecution team, particularly in the area of valuing the trade secret information. While valuation is not an element of proof at trial, it is important to address valuation issues early in the case to explore possible resolution of the case by plea agreement or to address anticipated issues at a contested sentencing hearing. By identifying the available evidence early in the case, a preferable method of valuation should become clear. Finally, as noted, the § 3553 sentencing factors, when applied to the facts of the case, are an important part of the sentencing recommendation.❖

ABOUT THE AUTHOR

❑ **Christopher S. Merriam** presently serves as the Assistant Deputy Chief, Intellectual Property, International, and Policy Matters for CCIPS. Among other cases, he worked on sentencing and related issues in the Four Pillars trade secret prosecution (*United States v. Yang*), and served as the CCIPS point of contact on trade secret cases from 2002-05.✠