IV.

Theft of Commercial Trade Secrets— 18 U.S.C. §§ 1831-1839

IV.A. Introduction

"A trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort." *ConFold Pac. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.) (citations omitted). Or, as Judge Posner could have pointed out, it can be unmasked by a criminal act.

Until 1996, no federal statute explicitly criminalized the theft of commercial trade secrets. Some statutes could punish trade secret theft in limited situations: 18 U.S.C. § 1905 for the unauthorized disclosure of government information, including trade secrets, by a government employee; 18 U.S.C. § 2314 for the interstate transportation of stolen property, including trade secrets; and 18 U.S.C. §§ 1341, 1343, and 1346 for the use of mail or wire communications in a scheme to use information in violation of a confidential or fiduciary relationship. See Section IV.F. of this Chapter.

In 1996, Congress acted to correct the occasional mismatch between then-existing statutes and commercial trade secret theft by enacting the Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996) (codified at 18 U.S.C. §§ 1831-1839).

This Chapter considers a number of issues arising under the Economic Espionage Act in depth. A sample indictment and jury instructions appear at Appendix D. In addition to this Chapter, prosecutors may wish to consult the following treatises or law review articles: Uniform Trade Secrets Act §§ 1 *et seq.* (1985); Roger M. Milgrim, *Milgrim on Trade Secrets* (1994); J. Michael Chamblee, *Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 et seq.)*, 177 A.L.R.

Fed. 609 (2002); James M. Fischer, Note, *An Analysis of the Economic Espionage Act of 1996*, 25 Seton Hall Legis. J. 239 (2001); Louis A. Karasik, *Under the Economic Espionage Act: Combating Economic Espionage is No Longer Limited to Civil Actions to Protect Trade Secrets*, 48-OCT Fed. Law. 34 (2001); Marc J. Zwillinger & Christian S. Genetski, *Calculating Loss Under the Economic Espionage Act of 1996*, 9 Geo. Mason L. Rev. 323 (2000); Michael Coblenz, *Intellectual Property Crimes*, 9 Alb. L.J. Sci. & Tech. 235 (1999); Sylvia N. Albert et al., *Intellectual Property Crimes*, 42 Am. Crim. L. Rev. 631 (2005); James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177 (1997).

IV.B. The Economic Espionage Act of 1996, 18 U.S.C. §§ 1831-1839

IV.B.1. Overview

The Economic Espionage Act of 1996 ("EEA") criminalizes two types of trade secret misappropriation in Title 18. Section 1831punishes the theft of a trade secret to benefit a foreign government, instrumentality, or agent:

> (a) In general.—Whoever, *intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent,* knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret;
>
> (3) receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in any of paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in any of paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,

shall, except as provided in subsection (b), be fined not more than $500,000 or imprisoned not more than 15 years, or both.

18 U.S.C. § 1831(a) (emphasis added).

Section 1832, in contrast, punishes the commercial theft of trade secrets carried out for economic advantage, whether or not it benefits a foreign government, instrumentality, or agent:

> (a) Whoever, *with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will injure any owner of that trade secret,* knowingly—
>
> (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;
>
> (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;
>
> (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
>
> (4) attempts to commit any offense described in paragraphs (1) through (3); or
>
> (5) conspires with one or more other persons to commit any offense described in paragraphs (1) through (3), and one or more of such persons do any act to effect the object of the conspiracy,
>
> shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 1832(a) (emphasis added).

Although § 1831 (foreign economic espionage) and § 1832 (commercial economic espionage) define separate offenses, they are nevertheless related. Both require the government to prove beyond a reasonable doubt that: (1) the defendant misappropriated information (or conspired or attempted to do so); (2) the defendant knew or believed that this information was a trade secret; and (3) the information was in fact a trade secret (unless, as is discussed below, the crime charged is a conspiracy or an attempt). *See* 18 U.S.C. §§ 1831(a), 1832(a). Both sections criminalize not only the misappropriation of a trade secret, but also the knowing receipt, purchase,

destruction, or possession of a stolen trade secret. *See* 18 U.S.C. §§ 1831(a)(3), 1832(a)(3).

To establish foreign economic espionage under 18 U.S.C. § 1831, the government must also prove that the defendant knew the offense would benefit or was intended to benefit a foreign government or a foreign-government instrumentality or agent.

If a foreign connection does not exist or cannot be proved, the government may still establish a violation of 18 U.S.C. § 1832 by proving, in addition to the first three elements described above, that: (4) the defendant intended to convert the trade secret to the economic benefit of anyone other than the owner; (5) the defendant knew or intended that the owner of the trade secret would be injured; and (6) the trade secret was related to or was included in a product that was produced or placed in interstate or foreign commerce.

The EEA can be applied to a wide variety of criminal conduct. It criminalizes attempts and conspiracies to violate the EEA and certain extraterritorial conduct. See Sections IV.B.6. and IV.D.3. of this Chapter.

The EEA also provides several remedies that are unusual in a criminal statute: civil injunctive relief against violations, to be obtained by the Attorney General, 18 U.S.C. § 1836, and confidentiality orders to maintain the trade secret's secrecy throughout the prosecution. See Section IV.D. of this Chapter.

For a discussion of the Department of Justice's oversight of EEA prosecutions, see Section IV.D.4.

IV.B.2. Relevance of Civil Cases

The EEA's definition of a trade secret, 18 U.S.C. § 1839(3), is based on the trade secret definition in the Uniform Trade Secrets Act. *See* H.R. Rep. 104-788, at 12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4031. Cases that address trade secrets outside the EEA should, in most cases, be relevant in EEA prosecutions.

IV.B.3. Elements Common to 18 U.S.C. §§ 1831, 1832

The elements for completed offenses are discussed in the ensuing Sections. Attempts and conspiracies are discussed in Section IV.B.6. of this Chapter.

IV.B.3.a. The Information Was a Trade Secret

IV.B.3.a.i. Generally

As mentioned in the introduction, "[a] trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that the holder tries to keep secret ..., so that the only way the secret can be unmasked is by [unlawful activity]." *ConFold Pac. v. Polaris Indus.*, 433 F.3d 952, 959 (7th Cir. 2006) (Posner, J.) (citations omitted). Whether particular information is a trade secret is a question of fact. 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[1][a][i].

The EEA's definition of a trade secret is very broad. As defined at 18 U.S.C. § 1839, a trade secret includes generally all types of information, regardless of the method of storage or maintenance, that the owner has taken reasonable measures to keep secret and that itself has independent economic value:

> (3) the term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if —
>
> > (A) the owner thereof has taken reasonable measures to keep such information secret; and
> >
> > (B) 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). As mentioned above, the EEA's definition of a trade secret, 18 U.S.C. § 1839(3), comes from civil law, so cases that address trade secrets outside the EEA should, in most cases, be relevant in EEA prosecutions. See Section IV.B.2. of this Chapter.

Examples of trade secrets include:

- a computer software system used in the lumber industry. *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994).
- measurements, metallurgical specifications, and engineering drawings to produce an aircraft brake assembly. *United States v. Lange*, 312 F.3d 263 (7th Cir. 2002).

- information involving zinc recovery furnaces and the tungsten reclamation process. *Metallurgical Indus. Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1202 (5th Cir. 1986).
- information concerning pollution control chemicals and related materials. *Apollo Techs. Corp. v. Centrosphere Indus. Corp.*, 805 F. Supp. 1157, 1197 (D.N.J. 1992).
- information regarding contact lens production. *Syntex Ophthalmics, Inc. v. Tsuetaki*, 701 F.2d 677, 684 (7th Cir. 1983).
- pizza recipes. *Magistro v. J. Lou, Inc.*, 703 N.W.2d 887, 890-91 (Neb. 2005).

For an extensive collection of cases analyzing whether specific types of information constitute a trade secret, see 1 *Milgrim on Trade Secrets* § 1.09.

In cases alleging attempt and conspiracy, the government need not prove that the information actually was a trade secret. See Section IV.B.6. of this Chapter.

IV.B.3.a.ii. Employee's General Knowledge, Skill, or Abilities Not Covered

The EEA does not apply "to individuals who seek to capitalize on the personal knowledge, skill, or abilities they may have developed" in moving from one job to another. H.R. Rep. No. 104-788, at 7 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026. "The statute is not intended to be used to prosecute employees who change employers or start their own companies using general knowledge and skills developed while employed." *Id.* Section 1832(a) "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) (emphasis in original). "It is not enough to say that a person has accumulated experience and knowledge during the course of his or her employ. Nor can a person be prosecuted on the basis of an assertion that he or she was merely exposed to a trade secret while employed. A prosecution that attempts to tie skill and experience to a particular trade secret should not succeed unless it can show that the particular material was stolen or misappropriated." 142 Cong. Rec. 27, 117 (1996).

These principles are often cited when the purported trade secret is one the defendant remembered only casually. For example, one court held that

a terminated agent cannot be prohibited from using skills that he acquired, or casually remembered information that he acquired, while employed by the principal. *Apollo Techs. Corp. v. Centrosphere Indus. Corp.*, 805 F. Supp. 1157, 1200 (D.N.J. 1992) (quoting Restatement (Second) of Agency § 396 comments b, h). In another case, a court ruled that "[r]emembered information as to specific needs and business habits of particular customers is not confidential." *Tactica Int'l, Inc. v. Atlantic Horizon Int'l, Inc.*, 154 F. Supp. 2d 586, 606 (S.D.N.Y. 2001) (citations omitted). In *Tactica*, the court cited two reasons for finding that remembered information concerning customer preferences was not a trade secret. First, no evidence was offered that the defendants intentionally memorized information, or that they stole it in any other way. *Id.* at 606-07 (citing *Levine v. Bochner*, 517 N.Y.S.2d 270, 271 (N.Y. App. Div. 1987) ("The use of information about an employer's customers which is based on casual memory is not actionable.")). Second, the information in question could easily be recalled or obtained subsequently by the defendants. *Id.* at 607.

Moreover, an employee who changes employers or starts his own company cannot be prosecuted under the EEA merely on the ground that he was exposed to a trade secret while employed. Rather, the government must establish that he actually stole or misappropriated a particular trade secret, or at least that he conspired or attempted to do so.

IV.B.3.a.iii. Specification of Trade Secrets

The government should ascertain which specific information the victim claims as a trade secret early on. "[A] prosecution under [the EEA] must establish a particular piece of information that a person has stolen or misappropriated." 142 Cong. Rec. 27, 117 (1996). This will help avoid the defendant's defense that he was merely relying on his general knowledge, skills, and abilities along, perhaps, with legitimate reverse-engineering (see Section IV.C.2. of this Chapter).

The defense, however, has no right to take pre-trial depositions of the government's expert witnesses to determine what the government will claim is a trade secret and why. *See United States v. Ye*, 436 F.3d 1117 (9th Cir. 2006).

IV.B.3.a.iv. Novelty

Unlike patents or copyrights, which require higher degrees of novelty, trade secrets must possess only "minimal novelty." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974) (quoting Comment, *The Stiffel Doctrine and*

the Law of Trade Secrets, 62 Nw. U. L. Rev. 956, 969 (1968)); *see also Arco Indus. Corp. v. Chemcast Corp.*, 633 F.2d 435, 442 (6th Cir. 1980) (same).

In other words, a trade secret must contain some element that is not known and that sets it apart from what is generally known. "While we do not strictly impose a novelty or inventiveness requirement in order for material to be considered a trade secret, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience." 142 Cong. Rec. 27, 117 (1996). *See, e.g.*, *Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir. 1996) (holding that plaintiff's recipes were not trade secrets in part because they lacked the requisite novelty).

IV.B.3.a.v. Secrecy

The key attribute of a trade secret is that the underlying information "not be[] generally known to ... the public" and that it "not be[] readily ascertainable through proper means by [] the public." 18 U.S.C. § 1839(3)(B). The "public" may not necessarily mean the general public. "[E]ither the phrase 'readily ascertainable' or the phrase 'the public' must be understood to concentrate attention on either potential users of the information, or proxies for them (which is to say, persons who have the same ability to 'ascertain' the information)." *United States v. Lange*, 312 F.3d 263, 268 (7th Cir. 2002) (Easterbrook, J.). *But see id.* at 271-72 (Ripple, J., concurring) (suggesting that this holding is dictum). In other words, information will not necessarily be a trade secret just because it is not readily ascertainable by the general public. Under the Seventh Circuit's view, the information will not be a trade secret if it is readily ascertainable by those within the information's field of specialty.

If a scientist could ascertain a purported trade secret formula only by gleaning information from publications and then engaging in many hours of laboratory testing and analysis, the existence of such publications would not necessarily disqualify the formula as a trade secret under the EEA, since the scientist's work would probably not qualify as "readily ascertainable by the public." *See* 18 U.S.C. § 1839(3)(B). But the formula would not be a trade secret if it could be ascertained or reverse-engineered within a relatively short time. *See Lange*, 312 F.3d at 269 (EEA case) ("Such measurements could not be called trade secrets if ... the assemblies in question were easy to take apart and measure."); *Marshall v. Gipson Steel*, 806 So.2d 266, 271-72 (Miss. 2002) (holding that company's bid estimating system was readily ascertainable by using simple math applied to data on past bids, and thus was not a trade secret); *Weins v. Sporleder*, 569 N.W.2d 16, 20-21 (S.D. 1997) (holding formula of cattle feed product not a trade

secret because the ingredients could be determined through chemical or microscopic analysis in four or five days, at most, and for about $27); *Buffets, Inc. v. Klinke*, 73 F.3d 965, 968 (9th Cir. 1996) (holding restaurant chain's recipes not to be trade secrets because, although innovative, the recipes were readily ascertainable by others).

A trade secret can include elements that are in the public domain if the trade secret itself constitutes a unique, "effective, successful and valuable integration of the public domain elements." *Rivendell Forest Prods., Ltd. v. Georgia-Pacific Corp.*, 28 F.3d 1042, 1046 (10th Cir. 1994); *accord Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1202 (5th Cir. 1986); *Apollo Techs. Corp. v. Centrosphere Indus.*, 805 F. Supp. 1157, 1197 (D.N.J. 1992). In fact, "[a] trade secret can exist in a combination of characteristics and components, each of which, by itself, is in the public domain, but the unified process, design and operation of which, in unique combination, affords a competitive advantage and is a protectable secret." *Metallurgical Indus.*, 790 F.2d at 1202 (quoting *Imperial Chem., Ltd. v. National Distillers & Chem. Corp.*, 342 F.2d 737, 742 (2d Cir. 1965)); *accord Syntex Ophthalmics, Inc. v. Tsuetaki*, 701 F.2d 677, 684 (7th Cir. 1983); *Rivendell Forest Prods.*, 28 F.3d at 1046. For example, in *Metallurgical Industries*, when the company modified a generally-known zinc recovery process, the modified process could be considered a trade secret even though the original process and the technologies involved were publicly known, because the details of the modifications were not. 790 F.2d at 1201-03.

IV.B.3.a.vi. Disclosure's Effects

A trade secret can lose its protected status through disclosure. To prove secrecy, the government often has the difficult burden of proving a negative, i.e., that the information was not generally available to the public. For this reason, the prosecutor should ascertain early on whether the purported trade secret was ever disclosed and to what extent those disclosures affect the information's status as a trade secret. These issues are covered thoroughly in Donald M. Zupanec, Annotation, *Disclosure of Trade Secret as Abandonment of Secrecy*, 92 A.L.R.3d 138 (2005) and 1 Roger M. Milgrim, *Milgrim on Trade Secrets* §§ 1.05-1.06 (2005). The following is an overview.

- **Disclosure Through the Patent and Copyright Processes**

Information that has been disclosed in a patent application can nevertheless qualify as a trade secret between the times of the application's submission and the patent's issuance, as long as the patent application itself is not published by the patent office. *Scharmer v. Carrollton Mfg. Co.*, 525 F.2d

95, 99 (6th Cir. 1975) (citing *Grant v. Raymond*, 31 U.S. 218, 242 (1832)). The patented process or device is no longer a trade secret once the application is published or the patent is issued, because publication of the application or patent makes the process publicly available for all to see. *Id.* (citing *A.O. Smith Corp. v. Petroleum Iron Works Co.*, 73 F.2d 531, 537 (6th Cir. 1934)); 37 C.F.R. § 1.14, 35 U.S.C.A. App. I, at 653); *see also On-Line Techs. v. Perkin-Elmer Corp.*, 253 F. Supp. 2d 313, 323-27 (D. Conn. 2003). In return for the disclosure, the owner enjoys patent protection against other companies' use of the technology. See Chapter VII of this Manual. A subsequent refinement or enhancement to the patented technology may be a trade secret if it is not reasonably ascertainable from the published patent itself. *See United States v. Hsu*, 185 F.R.D. 192, 200 (E.D. Pa. 1999).

Substantially the same analysis applies to information that has been submitted to the United States Copyright Office for registration. Submitting material to the Copyright Office can render it open to public examination and viewing, thus destroying the information's value as a trade secret, unless the material is submitted under special procedures to limit trade secret disclosure. *See Tedder Boat Ramp Sys. v. Hillsborough County, Fla.*, 54 F. Supp. 2d 1300, 1303-04 (M.D. Fla. 1999); *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 923 F. Supp. 1231, 1255 n.28 (N.D. Cal. 1995); 1 *Milgrim on Trade Secrets* § 1.06[6]-[9]. *But see Compuware Corp. v. Serena Software Int'l*, 77 F. Supp. 2d 816 (E.D. Mich. 1999) (holding that material could continue to be a trade secret even after its owner submitted it to the Copyright Office without redaction, because the owner had taken other steps to keep it secret and there was no evidence that it had become known outside the owner's business).

- **Disclosure Through Industry Publications or Conferences**

Information can also lose protection as a trade secret through accidental or intentional disclosure by an employee at a conference or trade show, or in technical journals or other publications. *See, e.g.*, *Mixing Equip. Co. v. Philadelphia Gear, Inc.*, 436 F.2d 1308, 1311 n.2 (3d Cir. 1971) (holding that industrial mixing equipment charts and graphs lost trade secret status through publication in trade journals).

- **Disclosure to Licensees, Vendors, and Third Parties**

Information that has been disclosed to licensees, vendors, or third parties for limited purposes can remain a trade secret under certain circumstances. *See, e.g.*, *United States v. Lange,* 312 F.3d 263, 266 (7th Cir. 2002) (EEA case); *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 177 (7th Cir. 1991). For the security measures the trade secret owner

must take to maintain secrecy during those disclosures, see Section IV.B.3.a.vii. of this Chapter.

- **Disclosure Through Internet Postings**

A trade secret can lose its protected status after it is posted anonymously on the Internet, even if the trade secret was originally gathered through improper means. *See Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 923 F. Supp. 1231 (N.D. Cal. 1995). If the Internet posting causes the information to fall into the public domain, a person who republishes the information is not guilty of misappropriating a trade secret, even if he knew that the information was originally acquired by improper means. *DVD Copy Control Ass'n Inc. v. Bunner*, 10 Cal. Rptr. 3d 185, 194 (Cal. Ct. App. 2004). "[T]hat which is in the public domain cannot be removed by action of the states under the guise of trade secret protection." *Id.* at 195.

Disclosure over the Internet does not, however, strip away a trade secret's protection automatically. For example, in *United States v. Genovese*, the court held that a trade secret could retain its secrecy despite a brief disclosure over the Internet: "[A] trade secret does not lose its protection under the EEA if it is temporarily, accidentally or illicitly released to the public, provided it does not become 'generally known' or 'readily ascertainable through proper means.'" 409 F. Supp. 2d 253, 257 (S.D.N.Y. 2005) (citing 18 U.S.C. § 1839(3)(B)). Publication on the Internet does not destroy the trade secret's status "if the publication is sufficiently obscure or transient or otherwise limited so that it does not become generally known to the relevant people, i.e., potential competitors or other persons to whom the information would have some economic value." *DVD Copy Control Ass'n*, 10 Cal. Rptr. 3d at 192-93.

- **Disclosure During Law Enforcement Investigations**

Disclosures to the government to assist an investigation or prosecution of an EEA case should not waive trade secret protections. *See United States v. Yang*, 1999 U.S. Dist. LEXIS 7130 (N.D. Ohio Mar. 18, 1999) (holding that victim's disclosure of trade secret to government for use in a sting operation under oral assurances that the information would not be used or disclosed for any purpose unrelated to the case did not vitiate trade secret status). Disclosure to the government is essential for the investigation and prosecution of illegal activity and is expressly contemplated by the EEA. First, 18 U.S.C. § 1833(2) specifically encourages disclosures to the government, stating: "[the EEA] does not prohibit ... the reporting of a suspected violation of law to any governmental entity of the United States ... if such entity has lawful authority with respect to that violation." Second,

18 U.S.C. § 1835 authorizes the court to "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 ... and all other applicable laws." *See also infra* Section IV.D.2. Section 1835 gives "a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1988). Together, these sections demonstrate Congress's intent to encourage the reporting of an EEA violation.

Laws other than the EEA similarly limit the Department of Justice's disclosure of trade secrets without the consent of the trade secret owner or the express written authorization of senior officials at the Department. *See, e.g.*, 28 C.F.R. § 16.21 (2005).

Information does not lose its status as a trade secret if the government discloses it to the defendant as "bait" during a sting operation. *See United States v. Hsu*, 185 F.R.D. 192, 199 (E.D. Pa. 1999). "[T]o hold that dangling such bait waives trade secret protection would effectively undermine the Economic Espionage Act at least to the extent that the Government tries ... to prevent an irrevocable loss of American technology before it happens." *Id.*

- **Disclosure by the Original Misappropriator or His Co-Conspirators**

The person who originally misappropriates a trade secret cannot immunize himself from prosecution by disclosing it into the public domain. Although disclosure of a trade secret may cause it to lose trade-secret status *after* the disclosure, disclosure does not destroy trade-secret status retroactively. Consequently, one who initiates the disclosure may be prosecuted, whereas one who distributes the information post-disclosure may not, unless he was working in concert with the original misappropriator. *Cf. Underwater Storage, Inc. v. United States Rubber Co.*, 371 F.2d 950, 955 (D.C. Cir. 1966) ("We do not believe that a misappropriator or his privies can 'baptize' their wrongful actions by general publication of the secret."); *Religious Tech. Ctr. v. Netcom On-Line Communication Servs.*, 923 F. Supp. at 1256.

IV.B.3.a.vii. Reasonable Measures to Maintain Secrecy

Trade secrets are fundamentally different from other forms of property in that a trade secret's owner must take reasonable measures under the circumstances to keep the information confidential. *See* 18 U.S.C. § 1839(3)(A); *United States v. Lange*, 312 F.3d 263, 266 (7th Cir.

2002). This requirement is generally not imposed upon those who own other types of property. For example, a thief can be convicted for stealing a bicycle the victim left unlocked in a public park, whereas a thief cannot be convicted (at least under the EEA) for stealing the bicycle's design plans if the victim left the plans in a public park.

For these reasons, prosecutors should determine what measures the victim used to protect the trade secret. These protections will be a critical component of the case or the decision not to prosecute.

Typical security measures include:

- keeping the secret physically secure in locked drawers, cabinets, or rooms
- restricting access to those with a need to know
- restricting visitors to secret areas
- requiring recipients to sign confidentiality, nondisclosure, or noncompetition agreements
- marking documents as confidential or secret
- encrypting documents
- protecting computer files and directories with passwords
- splitting tasks among people or entities to avoid concentrating too much information in any one place

See 1 Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.04 (2005); *Lange*, 312 F.3d at 266 (EEA case concerning aircraft brake assemblies); *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) (discussing steps to safeguard computer system manufacturer's trade secrets from computer servicing company); *Reingold v. Swiftships, Inc.*, 126 F.3d 645, 650 (5th Cir. 1997) (discussing steps to protect ship-builder's mold for fiberglass boat hulls).

The owner's security measures need not be absolutely airtight. Rather, they must be reasonable under the facts of the specific case. *See* H.R. Rep. No. 104-788, *reprinted in* 1996 U.S.C.C.A.N. 4021, 4026, 4031; *Lange*, 312 F.3d at 266. *See also* 1 *Milgrim on Trade Secrets* § 1.04; *Pioneer Hi-Bred Int'l v. Holden Found. Seeds, Inc.*, 35 F.3d 1226, 1235-36 (8th Cir. 1994) (discussing steps to safeguard genetic messages of genetically engineered corn); *Gates Rubber Co. v. Bando Chem. Indus.*, 9 F.3d 823, 848-49 (10th Cir. 1993) (discussing steps to protect industrial belt replacement software); *K-2 Ski Co. v. Head Ski Co.*, 506 F.2d 471, 473-74 (9th Cir. 1974) (discussing steps

to protect design and manufacture specifications of high performance skis); *Elm City Cheese Co. v. Federico*, 752 A.2d 1037, 1049-53 (Conn. 1999) (holding that victim's failure to require defendant employee to sign a confidentiality, nondisclosure, or noncompetition agreement was reasonable "in light of the close personal relationship enjoyed over the years" by the parties).

Information might not qualify as a trade secret if any low-level employee in a large company could access it. The theft of relatively unprotected information might, however, be prosecuted under a different statute. See Section IV.F. of this Chapter.

If the trade secret was disclosed to licensees, vendors, or third parties for limited purposes, those disclosures do not waive trade secret protections so long as the trade secret owner took reasonable security measures before and during disclosure, such as requiring non-disclosure agreements from all recipients. *See, e.g.*, *Quality Measurement Co. v. IPSOS S.A.,* 56 Fed. Appx. 639, 647 (6th Cir. 2003); *MAI Sys. Corp.*, 991 F.2d at 521; *Religious Tech. Ctr.*, 923 F. Supp. at 1254. However, where the trade secret owner "rel[ies] on *deeds* (the splitting of tasks) rather than *promises* to maintain confidentiality," it is "irrelevant that [the victim] does not require vendors to sign confidentiality agreements." *Lange,* 312 F.3d at 266 (emphasis in original).

As is discussed above, information does not lose its status as a trade secret if it is disclosed to the government for purposes of investigation or prosecution. For this reason, federal prosecutors and law enforcement agents need not sign protective orders with victims before accepting trade secret information.

A defendant who was unaware of the victims' security measures can be convicted under the EEA if he was aware that the misappropriated information was proprietary. *United States v. Krumrei*, 258 F.3d 535, 538-39 (6th Cir. 2001) (rejecting void-for-vagueness argument against EEA); *accord United States v. Genovese*, 409 F. Supp. 2d 258 (S.D.N.Y 2005) (rejecting void-for-vagueness challenge to EEA indictment). *But see id.* (noting that the defendant could argue that he was unaware of the victim's security measures at trial).

IV.B.3.a.viii. Independent Economic Value

The trade secret must derive "independent economic value, actual or potential, from not being generally known to and not being readily ascertainable by the public." 18 U.S.C. § 1839(3)(B). Although the EEA does not require the government to prove a specific jurisdictional level of

value, the government must prove that the secret had some value. Economic value "speaks to the value of the information to either the owner or a competitor; any information which protects the owner's competitive edge or advantage." *US West Communications v. Office of Consumer Advocate*, 498 N.W.2d 711, 714 (Iowa 1993) (citations omitted). "[I]nformation kept secret that would be useful to a competitor and require cost, time and effort to duplicate is of economic value." *Id.* (citation omitted).

The secret's economic value can be demonstrated by the circumstances of the offense, such as the defendant's acknowledgment that the secret is valuable; the defendant's asking price, or an amount of time or money the defendant's buyers would have required to replicate the information. *See Lange*, 312 F.3d at 269; *Genovese*, 409 F. Supp. 2d at 257. For more on methods of proving a trade secret's specific value, see Section VIII.C.2. of this Manual.

Not all of a business's confidential information is valuable in a competitor's hands. For example, in *Microstrategy v. Business Objects*, 331 F. Supp. 2d 396, 421 (E.D. Va. 2004), the court found that a company-wide e-mail concerning the firm's financial problems and plans for survival was not a trade secret because it was unclear what economic value it would have had to anyone outside the company. *See also US West Communications*, 498 N.W.2d at 714 (finding no evidence of economic value without evidence that disclosure would have harmed the victim).

IV.B.3.a.ix. Example: Customer Lists

Some information that a company deems proprietary will not qualify as a trade secret. For example, under the Uniform Trade Secrets Act—which defines trade secrets in a manner similar to the EEA—a customer list is generally a trade secret only if the customers are not known to others in the industry, and could be discovered only by extraordinary efforts, and the list was developed through a substantial expenditure of time and money. *See ATC Distribution Group v. Whatever It Takes Transmissions & Parts*, 402 F.3d 700, 714-15 (6th Cir. 2005); *Conseco Fin. Servicing Corp. v. North Am. Mortgage Co.*, 381 F.3d 811, 819 & n.6 (8th Cir. 2004) (holding customer files of thousands of customers nationwide who were identified through a complex computer system to be trade secrets); *Electro Optical Indus., Inc. v. White*, 90 Cal. Rptr. 2d 680, 684 (Cal. Ct. App. 1999); *Leo Silfen, Inc. v. Cream*, 278 N.E.2d 636, 639-41 (N.Y. 1972). Conversely, a customer list is less likely to be considered a trade secret if customers' identities are readily ascertainable to those outside the list-owner's business and the list was compiled merely through general marketing efforts. *See ATC*

Distribution Group, 402 F.3d at 714-15 (affirming that customer list of transmission parts customers was not a trade secret because names of purchasers could "be ascertained simply by calling each shop and asking"); *Standard Register Co. v. Cleaver*, 30 F. Supp. 2d 1084, 1095 (N.D. Ind. 1998) (holding that customer list was not a trade secret where owner's competitors knew customer base, knew other competitors quoting the work, and were generally familiar with the customers' needs); *Nalco Chem. Co. v. Hydro Techs., Inc.*, 984 F.2d 801, 804 (7th Cir. 1993) (holding that customer lists were not a trade secret when base of potential customers was neither fixed nor small).

IV.B.3.b. Misappropriation

IV.B.3.b.i. Types of Misappropriation

Under either § 1831 or § 1832, the defendant must have misappropriated the trade secret through one of the acts prohibited in § 1831(a)(1)-(5) or § 1832(a)(1)-(5). Misappropriation covers a broad range of acts. It includes not only traditional methods of theft in which a trade secret is physically removed from the owner's possession, but also less traditional methods of misappropriation and destruction such as copying, duplicating, sketching, drawing, photographing, downloading, uploading, altering, destroying, photocopying, replicating, transmitting, delivering, sending, mailing, communicating, or conveying the information. *See* 18 U.S.C. §§ 1831(a)(1) (2), 1832(a)(1)-(2). Although many of these means of misappropriation leave the original property in the hands of its owner, they reduce or destroy the trade secret's value nonetheless. Congress prohibited all types of misappropriation "to ensure that the theft of intangible information is prohibited in the same way that the theft of physical items is punished." H.R. Rep. No. 104-788, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

Misappropriation also includes the knowing receipt, purchase, or possession misappropriated trade secrets. *See* 18 U.S.C. §§ 1831(3), 1832(3).

IV.B.3.b.ii. Memorization Included

The above types of misappropriation include not only manipulating a physical object, but also conveying or using intangible information that has been memorized. The EEA defines a trade secret as "*all forms and types* of financial, business, scientific, technical, economic, or engineering *information*, ... *whether tangible or intangible*, and whether or how stored." 18 U.S.C. § 1839(3) (emphasis added). The statute also prohibits not only

actions taken against a trade secret's physical form, such as "steal[ing], ...tak[ing], [and] carr[ying] away", 18 U.S.C. §§ 1831(a)(1), 1832(a)(1), but also actions that can be taken against a trade secret in a memorized, intangible form, such as "sketch[ing], draw[ing], ... download[ing], upload[ing], ..., transmit[ting], ... communicat[ing], [and] convey[ing]," 18 U.S.C. §§ 1831(a)(2), 1832(a)(2). *See* James H.A. Pooley et al., *Understanding the Economic Espionage Act of 1996*, 5 Tex. Intell. Prop. L.J. 177 (1997). In this respect, as in others, the EEA echoes civil law and some pre-EEA caselaw. *See, e.g.*, 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.01[e]; *Stampede Tool Warehouse v. May*, 651 N.E.2d 209, 217 (Ill. App. Ct. 1995) ("A trade secret can be misappropriated by physical copying or by memorization.") (citations omitted). Trade secret cases to the contrary that do not involve the EEA are thus not persuasive authority on this point.

This is not to say, however, that any piece of business information that can be memorized is a trade secret. As noted, the EEA does not apply to individuals who seek to capitalize on their lawfully developed knowledge, skill, or abilities. When the actions of a former employee are unclear and evidence of theft has not been discovered, it may be advisable for a company to pursue its civil remedies and make another criminal referral if additional evidence of theft is developed.

Where available, tangible evidence of theft or copying is helpful in all cases to overcome the potential problem of prosecuting the defendant's "mental recollections" and a defense that "great minds think alike."

IV.B.3.b.iii. Lack of Authorization

The crux of misappropriation is that the defendant acted "without authorization" from the trade secret's owner. The necessary "authorization is the permission, approval, consent or sanction of the owner" to obtain, destroy, or convey the trade secret. 142 Cong. Rec. 27,116 (1996). Thus, although an employee may be authorized to possess a trade secret during his employment, he would violate the EEA if he conveyed it to a competitor without his employer's permission.

IV.B.3.b.iv. Misappropriation of Only Part of a Trade Secret

The defendant can be prosecuted even if he misappropriated only part of the trade secret. Using only part of the secret, so long as it too is secret, qualifies as misappropriation. *Mangren Research and Dev. Corp. v. National Chem. Co.*, 87 F.3d 937, 943-44 (7th Cir. 1996); *cf. United States v. Pemberton*, 904 F.2d 515, 517 (9th Cir. 1990) (rejecting argument of defendant convicted for receiving 30 stolen technical landscape and irrigation

drawings for a commercial development "that the incomplete nature of the drawings rendered them worthless," because evidence established that "some of the drawings would have been useful to the developer, even though not entirely finished," and the developer might have been willing to adjust the price for the drawings' incomplete nature); *United States v. Inigo*, 925 F.2d 641, 653-54 (3d Cir. 1991) (Hobbs Act conviction) (rejecting defendant's argument that the victim should not have feared economic loss because, *inter alia*, he possessed less than five percent of the confidential documents on a subject, and that "what matters is how important the documents [the defendant] had were to [the defendant], not their number").

IV.B.3.b.v. Mere Risk of Misappropriation Not Prosecutable, But Attempts and Conspiracies Are

However, a former employee cannot be prosecuted just because she was exposed to a trade secret at her former job and has now moved to a competitor. The government must establish that she actually stole or misappropriated a particular trade secret or that she attempted or conspired to do so.

IV.B.3.c. Knowledge

The first mens rea element in an EEA case is that the defendant misappropriated the trade secret "knowingly." Section 1831(a) applies to anyone who misappropriates a trade secret "knowingly." Section 1832(a), by contrast, applies to "[w]hoever, with intent to convert a trade secret," engages in misappropriation. This is a distinction without a difference, because knowing misappropriation is equivalent to the intent to convert.

"A knowing state of mind with respect to an element of the offense is (1) an awareness of the nature of one's conduct, and (2) an awareness of or a firm belief in or knowledge to a substantial certainty of the existence of a relevant circumstance, such as whether the information is proprietary economic information as defined by this statute." S. Rep. No. 104-359, at 16 (1996). Because criminal statutes covering the theft of tangible property generally require the government to prove that the defendant "[knew] that the object he [stole was] indeed a piece of property that he [had] no lawful right to convert for his personal use," the government generally must show that the defendant knew or had a firm belief that the information he or she was taking was a trade secret in an EEA case as well. 142 Cong. Rec. 27,117 (1996) (EEA legislative history). *See United States v. Genovese*, 409 F. Supp. 2d 253, 258 (S.D.N.Y. 2005) (discussing alleged circumstances that

would indicate that EEA defendant knew the information was a trade secret).

Ignorance of the law is no defense. The government need not prove that the defendant himself had concluded that the information he took fit the legal definition of a "trade secret" set forth in 18 U.S.C. § 1839(3). If the government had to prove this, EEA violations would be nearly impossible to prosecute and Congress's intent would be contravened:

> This [knowledge] requirement should not prove to be a great barrier to legitimate and warranted prosecutions. Most companies go to considerable pains to protect their trade secrets. Documents are marked proprietary; security measures put in place; and employees often sign confidentiality agreements.

142 Cong. Rec. 27,117 (1996). Based on this legislative history, the government should be able to establish that the defendant knew that the information was a trade secret by proving that he was aware that the information was protected by proprietary markings, security measures, and confidentiality agreements. *Id.* More generally, the government could simply prove that the defendant knew or had a firm belief that the information was valuable to its owner because it was not generally known to the public, and that its owner had taken measures to protect it, that is, the information had the attributes of a trade secret described in 18 U.S.C. § 1839(3). *Cf. Genovese*, 409 F. Supp. 2d at 258 (discussing alleged circumstances that would indicate that EEA defendant knew the information was a trade secret). On the other hand, a person cannot be prosecuted under the EEA if "he [took] a trade secret because of ignorance, mistake, or accident." 142 Cong. Rec. 27,117 (1996). Nor could he be prosecuted if "he actually believed that the information was not proprietary after [he took] reasonable steps to warrant such belief." *Id.*

IV.B.4. Additional 18 U.S.C. § 1831 Element: Intent to Benefit a Foreign Government, Foreign Instrumentality, or Foreign Agent

Under 18 U.S.C. § 1831, the second mens rea requirement is that the defendant intended or knew that the offense would "benefit" a "foreign government, foreign instrumentality, or foreign agent." A "foreign instrumentality" is "any agency, bureau, ministry, component, institution, association, or any legal, commercial, or business organization, corporation, firm, or entity that is substantially owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1). A "foreign agent" is "any officer, employee, proxy,

servant, delegate, or representative of a foreign government." 18 U.S.C. § 1839(2). Thus, the government must show that the defendant knew or had a firm belief that misappropriation would benefit an entity tied to a foreign government. See Section IV.B.3.c. of this Chapter. If this "entity" is not a government entity per se, such as a business, there must be "evidence of foreign government sponsored or coordinated intelligence activity." 142 Cong. Rec. 27,116 (1996).

The "benefit" to the foreign entity should be interpreted broadly. It is not limited to an economic benefit, but rather also includes a "reputational, strategic, or tactical benefit." H.R. Rep. No. 104-788, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

The requirement that the benefit accrue to a foreign government, instrumentality, or agent should be analyzed very carefully. To establish that the defendant intended to benefit a "foreign instrumentality," the government must show that the entity was "*substantially* owned, controlled, sponsored, commanded, managed, or dominated by a foreign government." 18 U.S.C. § 1839(1) (emphasis added). The EEA does not define "substantially," but its use suggests that the prosecution need not prove complete ownership, control, sponsorship, command, management, or domination:

> Substantial in this context, means material or significant, not technical or tenuous. We do not mean for the test of substantial control to be mechanistic or mathematical. The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.

142 Cong. Rec. 27,116 (1996).

Thus, § 1831 does not apply to a foreign corporation that acted without the sponsorship of, or "coordinated intelligence activity" by, a foreign government. *Id.* In such an instance, however, the foreign corporation could still be properly charged under 18 U.S.C. § 1832.

For questions concerning charges under § 1831, contact the Department's Counterespionage Section at (202) 514-1187 or CCIPS at (202) 514-1026.

IV.B.5. Additional 18 U.S.C. § 1832 Elements

IV.B.5.a. Economic Benefit to a Third Party

Under 18 U.S.C. § 1832, the government must prove that the defendant's misappropriation was intended for the "economic benefit of anyone other than the owner thereof." 18 U.S.C. § 1832(a). The recipient of the intended benefit can be the defendant, a competitor of the victim, or some other person or entity.

One who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under 18 U.S.C. § 1832. This requirement differs from foreign-government economic espionage under 18 U.S.C. § 1831, for which the economic or non-economic nature of the misappropriation is immaterial. *Compare* 18 U.S.C. § 1831(a) *with* § 1832(a).

IV.B.5.b. Intent to Injure the Owner of the Trade Secret

Beyond demonstrating in a § 1832 case that the defendant both knew that the information he took was proprietary and that he intended the misappropriation to economically benefit someone other than the rightful owner, the government must also prove that the defendant intended to "injure" the owner of the trade secret. *See* 18 U.S.C. § 1832(a). This provision "does not require the government to prove malice or evil intent, but merely that the actor knew or was aware to a practical certainty that his conduct would cause some disadvantage to the rightful owner." H.R. Rep. No. 104-788, at 11-12 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030.

By definition, for a trade secret to have value, it must confer a commercial advantage to its owner. *See* 18 U.S.C. § 1839(3)(B); H.R. Rep. No. 104-788, at 4 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4023. The trade secret loses its value once it is disclosed to another person for the recipient's benefit. *See* H.R. Rep. No. 104-788, at 11 (1996), *reprinted in* 1996 U.S.C.C.A.N. 4021, 4030 ("[M]isappropriation effectively destroys the value of what is left with the rightful owner."). Most employees understand that their misappropriation will injure the victim once he loses the exclusive use of his trade secret.

IV.B.5.c. Product Produced for or Placed in Interstate or Foreign Commerce

On a charge of domestic economic espionage under 18 U.S.C. § 1832, the government must prove that the trade secret was "related to or included in a product that is produced for or placed in interstate or foreign

commerce." 18 U.S.C. § 1832; *compare* 18 U.S.C. § 1831 (containing no explicit language about being included in or related to a product).

The defendant need not have known that the trade secret was related to or included in a product that was produced for or placed in interstate or foreign commerce. The nexus to interstate or foreign commerce appears to have been intended merely to allow federal jurisdiction. The statute's plain text confirms this. The jurisdictional language quoted above is set off in the statute by commas to qualify which types of trade secrets fall under the statute. It precedes the word "knowingly," thus putting it outside the elements the government must prove the defendant knew.

The phrase "a product produced for or placed in interstate or foreign commerce" includes trade secrets developed for existing products and for future products. In the case of an existing product, this nexus can usually be satisfied by evidence of the trade secret's connection to the current product and the product's current or potential interstate or foreign sales.

By contrast, if the product is still being developed, § 1832 would merely require proof that the trade secret was "related to ... a product that is produced for ... interstate or foreign commerce." 18 U.S.C. § 1832(a). A defendant might argue that a product still in the research and development stage is not yet being "produced for ... interstate commerce," 18 U.S.C. § 1832, because the prototype itself is not being "produced" for sale. But this argument would withhold the EEA's protection when it was most needed. The research and development phase is often when a trade secret is most valuable. Once the final product embodying the trade secret is released to the public, the trade secret's value can be lost because of its availability to competitors who can examine the product legitimately and obtain or deduce the trade secret for themselves.

To prove that the product was produced for interstate or foreign commerce, the government need only show the victim's intent to distribute the product or utilize the process under development for a product. This can be demonstrated through evidence of the project's goals.

At this writing, the only published case concerning these issues is *United States v. Yang*, 281 F.3d 534, 551 & n.4 (6th Cir. 2002), which held that a patent application had a sufficient nexus to interstate commerce because it involved a product that generated $75-100 million in sales the previous year and it was related to products produced and sold in the United States and Canada; and also because the victim also had sought patents for the product in Europe.

This element implicitly distinguishes between the misappropriation of trade secrets related to products—which is punishable under § 1832—and trade secrets related to services—which is not. For criminal charges to consider when the trade secret is related to services, see Section IV.F. of this Chapter.

Distinguishing when a trade secret relates to a product and when it relates to a service is sometimes easier said than done. Although the "product" requirement is not discussed in the legislative history, the term's plain meaning appears to exclude pure services such as technical skills and know-how that are not embodied in or related to a saleable, transportable good. Consider a chiropractor's secret technique to treat back pain by manipulating a patient's spine. If the chiropractor is not developing and has not developed a medical product that uses or embodies the secret, but instead merely uses the technique in private practice, the technique's theft by a coworker or common thief would not violate § 1832. By contrast, cellular telephone companies sell services that are accompanied by a "free" cellular phone or require the purchase of a compatible phone. If a cellular company develops a trade secret relating to the technical operation of its cellular network, the fact that the essence of what the company provides is a service should not necessarily preclude a prosecution under the EEA, given that the secret could be categorized as being "related to ... a product [the phone] that is produced for or placed in interstate or foreign commerce." §1832(a).

IV.B.6. Attempts and Conspiracies, Including the Impossibility Defense

As noted, the EEA—both foreign and domestic—punishes attempts and conspiracies to misappropriate trade secrets. 18 U.S.C. §§ 1831(a)(4)-(5), 1832(a)(4)-(5). For an attempt, the defendant must (1) have the intent needed to commit a crime defined by the EEA, and (2) perform an act amounting to a "substantial step" toward the commission of that crime. *United States v. Hsu*, 155 F.3d 189, 202 (3d Cir. 1998). For a conspiracy, the defendant must agree with one or more people to commit a violation, and one or more of the co-conspirators must commit an overt act to effect the object of the conspiracy. 18 U.S.C. §§ 1831(a)(5), 1832(a)(5).

In *Hsu*, the Sixth Circuit ruled that to convict a defendant under the EEA of attempt or conspiracy, the government need not prove that the information the defendant sought actually constituted a trade secret. *Hsu*, 155 F.3d at 204.

The defendants were charged with attempting and conspiring to steal the techniques for manufacturing an anti-cancer drug from Bristol-Meyers Squibb. The district court compelled the government to disclose to the defendants the trade secrets at issue, on the grounds that the defendants were entitled to demonstrate that the materials were not trade secrets in fact. *United States v. Hsu*, 982 F. Supp. 1022, 1024 (E.D. Pa. 1997). The Third Circuit disagreed, holding that to prove an attempt or conspiracy under the EEA, the government need not prove the existence of an actual trade secret, but, rather, that the defendants *believed* that the information was a trade secret—regardless of whether the information was truly a trade secret or not—and that they conspired in doing so. *Hsu*, 155 F.3d at 203-04.

The government need not prove the existence of an actual trade secret, because "a defendant's culpability for a charge of attempt depends only on 'the circumstances as he believes them to be,' not as they really are." *Id.* at 203. Thus, to prove an attempt, the government need only prove "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." *Id.*

The Third Circuit also rejected the defendants' contention that the government had to disclose the trade secrets so the defendants could prepare a potential defense of legal impossibility. Although elsewhere the Third Circuit generally allowed the common-law defense of legal impossibility in cases charging attempt, it found that the EEA evidenced Congress's intent to foreclose an impossibility defense. *Hsu,* 155 F.3d at 202 ("[T]he great weight of the EEA's legislative history evinces an intent to create a comprehensive solution to economic espionage, and we find it highly unlikely that Congress would have wanted the courts to thwart that solution by permitting defendants to assert the common law defense of legal impossibility."). The court found it significant that "[t]he EEA was drafted in 1996, more than twenty-five years after the National Commission on Reform of the Federal Criminal Laws had concluded that the abolition of legal impossibility was already 'the overwhelming modern position.'" *Id.* Lastly, the court noted that if legal impossibility were "a defense to the attempted theft of trade secrets, the government would be compelled to use actual trade secrets during undercover operations." *Id.* This would "have the bizarre effect of forcing the government to disclose trade secrets to the very persons suspected of trying to steal them, thus gutting enforcement efforts under the EEA." *Id.* Therefore, the court held that "legal impossibility is not a defense to a charge of attempted

misappropriation of trade secrets in violation of 18 U.S.C. § 1832(a)(4)." *Id.*

Nor is legal impossibility a defense to a charge of conspiracy to violate the EEA. Because the basis of a conspiracy charge is the "conspiratorial agreement itself and not the underlying substantive acts," the impossibility of achieving the conspiracy's goal is irrelevant *See Hsu*, 155 F.3d at 203 (citing *United States v. Jannotti*, 673 F.2d 578, 591 (3d Cir.1982) (en banc)); *see also United States v. Wallach*, 935 F.2d 445, 470 (2d Cir. 1991)*; United States v. LaBudda*, 882 F.2d 244, 248 (7th Cir. 1989); *United States v. Petit*, 841 F.2d 1546, 1550 (11th Cir. 1988); *United States v. Everett*, 692 F.2d 596, 599 (9th Cir. 1982).

Hsu's reasoning has been adopted by the Sixth Circuit in *United States v. Yang*, 281 F.3d 534, 542-45 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003), and the Seventh Circuit in *United States v. Lange*, 312 F.3d 263, 268-69 (7th Cir. 2002).

IV.C. Defenses

IV.C.1. Parallel Development

According to the EEA's legislative history, 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.*

IV.C.2. Reverse Engineering

Similarly, a person may legally discover the information underlying a trade secret by "reverse engineering," that is, the practice of taking something apart to determine how it works or how it was made or manufactured. *See, e.g.*, *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.") (Posner, J.) (citations omitted).

Although the EEA does not expressly address when reverse engineering is a valid defense, its legislative history states 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 mere fact that a particular secret *could* 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. *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 that 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.").

To counter a defense of reverse engineering, prosecutors should establish how the defendant obtained the trade secret. Proving misappropriation should refute a claim of reverse engineering.

IV.C.3. Impossibility

The defense of impossibility has largely been rejected by courts in EEA prosecutions. See Section IV.B.6. of this Chapter.

IV.C.4. Advice of Counsel

"There is no such thing as an 'advice of counsel' defense." *United States v. Urfer*, 287 F.3d 663, 666 (7th Cir. 2002) (Posner, J.) (charges of willfully injuring federal property). Rather, "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." *Id.* In other words, advice of counsel is a defense only if it negates the mens rea needed to prove a violation.

Advice of counsel could conceivably negate an EEA defendant's mens rea in several ways. As is discussed Section IV.B.3.c. of this Chapter, the defendant cannot be convicted unless he knew that he was misappropriating a trade secret. Thus, the defendant's mens rea might be negated if counsel advised him either that the information in question was not a trade secret or that it was a trade secret to which he could claim ownership. *See* Section IV.C.5.

To rely on advice of counsel at trial, the defendant must first 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) (citations and alterations omitted); *see also United States v. Butler*, 211 F.3d 826, 833 (4th Cir. 2000) (same).

IV.C.5. Claim of Right—Public Domain and Proprietary Rights

As is discussed in Section IV.B.3.c. of this Chapter, the defendant cannot be convicted unless he knew that he was misappropriating a trade secret. Thus, the defendant's mens rea might be negated if he believed in good faith that he had a right to use the information, either because it was in the public domain or because it belonged to him.

The former situation, information in the public domain, is discussed Section IV.B.3.a.vi. (discussing how disclosure affects trade secret status).

The latter situation, when the accused acts under a proprietary claim of right, 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 technology together and their respective ownership interests are unclear. In these circumstances, one party's unilateral action with regard to the trade secret might precipitate a criminal referral from the other party. Such cases are rarely appropriate for criminal prosecution, especially if the putative defendant acted on the advice of counsel. See Section IV.C.4. of this Chapter. Notwithstanding the passage of the EEA, many disputes about trade secrets are still best resolved in a civil forum.

IV.C.6. The First Amendment

The First Amendment is no defense when the defendant's speech itself is the very vehicle of the crime. *See, e.g.*, *United States v. Morison*, 844 F.2d 1057, 1068 (4th Cir. 1988) (rejecting defendant's First Amendment defense and upholding a conviction for a violation of 18 U.S.C. § 793 for stealing

secret government documents, noting that "[w]e do not think that the First Amendment offers asylum ... merely because the transmittal was to a representative of the press"); *United States v. Rowlee*, 899 F.2d 1275 (2d Cir. 1990) (rejecting First Amendment defense against charges of tax evasion conspiracy). In a prosecution similar to the theft of trade secrets under the EEA, the First Amendment was held to provide no defense to a charge under 18 U.S.C. § 2314 for the interstate transportation of stolen computer files:

> In short, the court finds no support for [the defendant's] argument that the criminal activity with which he is charged ... is protected by the First Amendment. Interpreting the First Amendment as shielding [the defendant] from criminal liability would open a gaping hole in criminal law; individuals could violate criminal laws with impunity simply by engaging in criminal activities which involve speech-related activity. The First Amendment does not countenance that kind of end run around criminal law.

United States v. Riggs, 743 F. Supp. 556, 560-61 (N.D. Ill. 1990).

In most instances, if the government can establish that the defendant intended his misappropriation to benefit a third party economically, he should have a hard time claiming that his disclosure of the trade secret was protected by the First Amendment. In other words, where the defendant's motivation was pecuniary, the defendant's argument that he disclosed the trade secret as a public service or to educate the public should be significantly undermined. *See DVD Copy Control Ass'n v. Bunner*, 75 P.3d 1, 19 (Cal. 2003) ("We merely hold that the preliminary injunction does not violate the free speech clauses of the United States and California Constitutions, *assuming* the trial court properly issued the injunction under California's trade secret law. On remand, the Court of Appeal should determine the validity of this assumption.").

Because the First Amendment does not protect speech that is criminal, the government should seek to exclude evidence regarding that defense through an appropriate motion *in limine*.

IV.C.7. Void-for-Vagueness

Several defendants have challenged the EEA on grounds that it is vague or otherwise unconstitutional. Thus far, all such challenges have been rejected.

In *United States v. Hsu*, 40 F. Supp. 2d 623 (E.D. Pa. 1999), the defendant was charged with, among other things, conspiracy to steal trade

secrets in violation of 18 U.S.C. § 1832(a)(5) and attempted theft of trade secrets in violation of 18 U.S.C. § 1832(a)(4). Hsu moved to dismiss, arguing that the EEA was unconstitutionally vague on numerous grounds.

In denying Hsu's motion to dismiss, the court noted that a statute is not unconstitutionally vague just because "Congress might, without difficulty, have chosen 'clearer and more precise language' equally capable of achieving the end which it sought." *Hsu*, 40 F. Supp. 2d at 626 (quoting *United States v. Powell,* 423 U.S. 87, 94 (1975) (citation omitted)). Because the First Amendment was not implicated, Hsu's void-for-vagueness challenge could succeed only if the EEA were vague as applied to his conduct and as applied to "the facts of the case at hand." *Id.* at 626-27. Hsu argued that the First Amendment was implicated because the Bristol-Meyers Squibb "employee who aided the Government 'sting' operation by posing as a corrupt employee [had] a right freely to express himself and exchange information with the defendant, or with anyone else he [thought was] a potential employer." *Id.* at 627. The court disagreed. It noted first that Hsu lacked standing to raise the victim's employee's purported First Amendment rights. *Id.* And even if Hsu had standing, the court said, the employee had knowingly participated in a government sting operation, not in a job interview with a potential employer. *Id.* Therefore, no First Amendment interests were implicated. *Id.*

The court also rejected Hsu's argument that the term "related to or included in a product that is produced for or placed in interstate or foreign commerce" is unacceptably vague. *Id.* Prior First Amendment decisions disapproving of the term "related" had no bearing on the use of "related to or included in" in the EEA, which the court found "readily understandable to one of ordinary intelligence, particularly here, where the defendant appears to be well versed as to [the nature of the technology at issue]." *Id.*

The court also concluded that the EEA's definition of "trade secret" was not unconstitutionally vague as applied to Hsu. As to the requirement that the owner take "reasonable measures" to keep the information secret, the mere use of the word "reasonable" or "unreasonable" does not render a statute vague. *Id.* at 628. The court further noted that these terms were taken "with only minor modifications" from the Uniform Trade Secrets Act, which had been adopted in forty states and the District of Columbia and had also withstood a void-for-vagueness attack. *Id.*

Also preventing Hsu's void-for-vagueness challenge was his own knowledge of the facts at the time of the offense. Hsu knew that Bristol-Meyers Squibb had taken many steps to keep its technology secret. He had

been told on several occasions that the technology was proprietary to Bristol-Meyers Squibb, could not be acquired through a license or joint venture, and could be obtained only through an allegedly corrupt employee. The court therefore held that he could not contend that the term "reasonable measures" was vague as applied to him. *Id.*

Finally, the *Hsu* court concluded that the EEA was not void for vagueness in qualifying that the information not be "generally known to" or "readily ascertainable by" the public. The court concluded that the EEA's use of those terms 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. Nonetheless, Hsu's e-mails, telephone calls, and conversations together showed that he believed that the information he sought could not be acquired through legal or public means. Therefore, the court concluded that the EEA's definition of trade secret was not unconstitutionally vague as applied to Hsu.

Subsequent courts have ruled similarly. *See United States v. Yang*, 281 F.3d 534, 544 n.2 (6th Cir. 2002) (rejecting defendants' argument 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 (S.D.N.Y. 2005) (denying motion to dismiss indictment as vague by defendant who argued that, having found confidential source code on the Internet, he could not know whether the code was generally known to the public or whether the code's owners took reasonable measures to keep it secret, and ruling that the government's allegations established that the defendant was on notice that the code was proprietary and any protective measures had been circumvented). *But see id.* at 258 (stating further that the defendant could argue that he could not have known the victim's protective measures at a later stage of the proceedings).

IV.D. Special Issues

IV.D.1. Civil Injunctive Relief for the United States

The EEA authorizes the government to file a civil action seeking injunctive relief. *See* 18 U.S.C. § 1836(a). Prosecutors should consider seeking injunctive relief to prevent further disclosure of a trade secret by

the defendant or third parties during a criminal investigation, or as part of the judgment at the end of the case.

Prosecutors may even seek injunctive relief in matters that do not warrant criminal prosecution if the victim is unable to do so. Note, however, that most victims can obtain injunctive and monetary relief on their own through state-law statutory and common-law remedies. For an extensive discussion of injunctive relief in civil cases, see 4 Roger M. Milgrim, *Milgrim on Trade Secrets* § 15.02[1].

The civil remedy in § 1836 can be enforced only by the government. Neither that section nor any other section of the EEA creates a private right of action that can be enforced by private citizens. *Cooper Square Realty v. Jensen*, No. 04 Civ. 01011 (CSH), 2005 WL 53284 (S.D.N.Y. Jan. 10, 2005); *Barnes v. J.C. Penney Co.*, No. 3-04-CV-577-N, 2004 WL 1944048 (N.D. Tex. Aug. 31, 2004), *magistrate's findings adopted*, 2004 WL 2124062 (N.D. Tex. Sept. 22, 2004).

IV.D.2. Confidentiality and the Use of Protective Orders

Victims of trade secret theft are often conflicted about whether to report these thefts to law enforcement authorities. They want the thief to be punished, but worry that their trade secret would be disclosed during discovery or trial.

Congress resolved this dilemma by giving the government measures to preserve the confidentiality of trade secrets throughout the prosecution. 142 Cong. Rec. 27,105 (1996). The EEA provides that 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." 18 U.S.C. § 1835. The government has the right to an interlocutory appeal from an order authorizing a trade secret's disclosure. *Id.*; *see also United States v. Ye*, 436 F.3d 1117, 1120-24 (9th Cir. 2006) (discussing extent and limits to interlocutory appeal 18 U.S.C. § 1835 and when mandamus relief in an EEA discovery dispute may be ordered under 28 U.S.C. § 1651).

Prosecutors are therefore strongly encouraged to move the court to take such actions as necessary and appropriate to prevent the trade secret's harmful disclosure. There are a number of ways to accomplish this. Protective orders can limit the amount or degree of disclosure in discovery, permit *in camera* review by the court prior to disclosure, allow or require the submission of redacted documents and sealed exhibits, and allow or require the use of courtroom video monitors to display documents to counsel, the

court, and the jury, but not to the public. *See, e.g., Burlington N.R.R. Co. v. Omaha Pub. Power Dist.*, 888 F.2d 1228, 1232 (8th Cir. 1989) (reviewing contract *in camera* without revealing trade secret); *Canal Refining Co. v. Corrallo*, 616 F. Supp. 1035, 1045 (D.D.C. 1985) (granting plaintiff's motion for protective order to seal separate portions of affidavit designated as exhibit); *Skolnick v. Altheimer & Gray*, 730 N.E. 2d 4, 14 (Ill. 2000) (holding that trial court abused its discretion by refusing to modify a protective order that allowed parties to designate information disclosed in discovery as "confidential").

The use of protective orders was endorsed in *United States v. Hsu*, 155 F.3d 189, 197 (3d Cir. 1998). In the district court, the government moved under 18 U.S.C. § 1835 and Fed. R. Crim. P. 16(d)(1) for a protective order to limit the government's production of documents used in the sting operation to redacted copies of documents relating to the trade secrets at issue. *United States v. Hsu*, 982 F. Supp. 1022, 1023 (E.D. Pa. 1997). The defendants wanted unredacted copies, but were willing to stipulate that they would use the documents only in the criminal litigation and would return or destroy the documents at the case's end. The district court agreed with the defendants' need for unredacted documents. *Id.* at 1029-30.

On the government's interlocutory appeal, the Third Circuit held that 18 U.S.C. § 1835 clearly demonstrates Congress's intent to protect the confidentiality of trade secrets to the fullest extent possible under the law. *Hsu*, 155 F.3d at 197. While recognizing that such protection does not abrogate criminal defendants' constitutional and statutory rights, the court held that the government's proposed order to produce only redacted copies of the targeted documents did not violate the defendants' constitutional rights because "a defendant's culpability for a charge of attempt depends only on 'the circumstances as he believes them to be,' not as they really are," and the actual trade secret documents were irrelevant to that inquiry. *Id.* at 203. Because the indictment did not charge a completed theft, the Third Circuit refrained from addressing the district court's conclusion that in a case charging a completed offense, actual trade secrets must be disclosed to defendants. The Third Circuit characterized this question as "complex," noting that the EEA's definition of trade secret "raises an issue as to whether the information or formula itself is in fact material to the existence of the trade secret." *Id.* at n.15. Thus, the limits of the government's ability to restrict disclosure in a criminal case concerning a completed offense have not yet been addressed.

As to the defendants' claim that they needed to see the trade secrets to prepare their other defenses, including entrapment and outrageous government conduct, the Third Circuit skeptically remanded these issues

to the district court. *Id.* at 205. On remand, the district court held that the defendants were not entitled to receive unredacted trade secret documents under Fed. R. Crim. P. 16(a)(1)(C), and found the unredacted documents to be irrelevant to the defenses of entrapment and outrageous government conduct. *United States v. Hsu*, 185 F.R.D. 192, 198 n.19 (E.D. Penn. 1999). Just as a drug defendant needs no access to the drugs to allege entrapment, neither does an EEA defendant need access to the trade secrets to do the same. *Id.*

The court similarly rejected the defendants' arguments for full disclosure based on the defenses of document integrity and chain of custody. *Id.* at 199 (concluding that those defenses could "be resolved at a later date without the defense viewing the redacted information ... just as chain of custody questions in drug or gun prosecutions can be resolved without having to touch the objects themselves" as well as the claims that the government and Bristol-Meyers waived the confidentiality of the trade secrets when they showed the documents voluntarily during the sting operation).

Finally, the court disagreed that the unredacted documents could help the defendants prove that the documents' information was in the public domain. After *in camera* review by a court-appointed technical advisor who had taken an oath of confidentiality, the court concluded that the largest category of redactions, consisting of "specific examples of experimental conditions," satisfied the statutory definition of a trade secret contained in 18 U.S.C. § 1839(3). After reviewing this category of redactions *in camera* and consulting with the expert, the court held that the redactions were proper to avoid disclosure of trade secrets. *Id.* at 200. The court did, however, order the disclosure of certain redacted information that fell outside the EEA's definition of a trade secret. *Id.*

Taken together, the appellate and trial courts' opinions in *Hsu* suggest that courts will recognize and respect Congress's directive to preserve the confidentiality of trade secrets throughout the criminal process.

Before trial, the defense has no right to take depositions of the government's expert witnesses to determine what the government will claim is a trade secret and why. *See United States v. Ye*, 436 F.3d 1117 (9th Cir. 2006).

During trial, courts can limit the public disclosure of information without violating the defendant's right to a public trial under the Sixth Amendment. The right to a public criminal trial is not absolute and may be limited in certain circumstances. *See Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 599-600 (1980) (Stewart, J. concurring); *see also Gannett v.*

DePasquale, 443 U.S. 368, 419-33 (1979) (Blackmun, J., concurring in part and dissenting in part) (tracing the history of the right to a public trial and citing cases where that right has been limited); *State ex rel. La Crosse Tribune v. Circuit Court*, 340 N.W.2d 460, 466-67 (Wis. 1983) (discussing court's inherent power to limit the public nature of trials).

Before requesting that a courtroom be sealed, prosecutors should comply with the procedures in the federal regulations and Department of Justice guidelines requiring the Deputy Attorney General's prior approval. *See* 28 C.F.R. § 50.9; USAM 9-5.150. The regulations create a strong presumption against sealing courtrooms and provide for such action "only when a closed proceeding is plainly essential to the interests of justice." 28 C.F.R. § 50.9. A prosecutor who wants to close a judicial proceeding in a case or matter under the supervision of the Criminal Division should contact the Criminal Division's Policy and Statutory Enforcement Unit, Office of Enforcement Operations at (202) 305-4023. In cases or matters supervised outside of the Criminal Division, the prosecutor should contact the supervising division. USAM 9-5.150.

For a helpful discussion of the use of protective orders in civil cases and a collection of relevant cases, see 3 Roger M. Milgrim, *Milgrim on Trade Secrets* § 14.02[5]-[7].

IV.D.3. Extraterritoriality

Federal criminal laws are generally presumed not to apply to conduct outside the United States or its territories unless Congress indicates otherwise. *See, e.g., United States v. Corey*, 232 F.3d 1166, 1170 (9th Cir. 2000). Congress made an exception for the EEA. The EEA expressly applies to conduct outside the United States if (1) the offender is a citizen or permanent resident alien of the United States, or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States. 18 U.S.C. § 1837.

IV.D.4. Department of Justice Oversight

Before Congress passed the EEA, the Attorney General promised that all EEA prosecutions during the EEA's first five years would be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General of the Criminal Division. This requirement was codified at 28 C.F.R. § 0.64-5 and applied to the filing of complaints, indictments, and civil proceedings, but not to search warrant applications or other investigative measures.

The approval requirement for § 1832 prosecutions lapsed after the five-year period expired on October 11, 2001, so federal prosecutors may now prosecute 18 U.S.C. § 1832 offenses without prior approval. However, the Attorney General strongly urges consultation with the Computer Crime and Intellectual Property Section (CCIPS) before filing § 1832 charges because of CCIPS's experience in handling these complex cases and its access to valuable information and resources. CCIPS can be reached at (202) 514-1026.

In contrast, the Attorney General renewed the prior approval requirement for initiating prosecutions under 18 U.S.C. § 1831. Approval must be obtained from the Assistant Attorney General for the Criminal Division, through the Counterespionage Section. USAM 9-2.400, 9-59.000. The Counterespionage Section can be reached at (202) 514-1187..

IV.E. Penalties

IV.E.1. Statutory Penalties

IV.E.1.a. Imprisonment and Fines

Reflecting the more serious nature of economic espionage sponsored by a foreign government, the maximum sentence for a defendant convicted under 18 U.S.C. § 1831 is 15 years' imprisonment and a fine of $500,000 or twice the monetary gain or loss, or both, whereas the maximum sentence for a defendant convicted under 18 U.S.C. § 1832 is 10 years' imprisonment and a fine of $250,000 or twice the monetary gain or loss, or both. *See* 18 U.S.C. §§ 1831(a)(4), 1832(a)(5). Similarly, organizations can be fined up to $10 million for violating § 1831 or $5 million for violating § 1832. 18 U.S.C. §§ 1831(b), 1832(b).

IV.E.1.b. Criminal Forfeiture

The EEA provides criminal forfeiture. It directs that the sentencing court

> shall order ... that the person forfeit to the United States—
>
> (1) any property constituting, or derived from, any proceeds the person obtained, directly or indirectly, as the result of such violation; and
>
> (2) any of the person's property used, or intended to be used, in any manner or part, to commit or facilitate the commission of such violation, if the court in its discretion so determines, taking

into consideration the nature, scope, and proportionality of the use of the property in the offense.

18 U.S.C. § 1834(a). Forfeiture of proceeds is mandatory, while forfeiture of instrumentalities is discretionary. 18 U.S.C. § 1834(a)(1)-(2).

As a procedural matter, the government should allege forfeiture in the indictment. For additional discussion of forfeiture in intellectual property infringement cases, see Chapter VIII of this Manual.

IV.E.1.c. Restitution

The Mandatory Victims Restitution Act of 1996 ("MVRA"), codified at 18 U.S.C. § 3663A, requires the court to order restitution in all convictions for, among others, any "offense against property, including any offense committed by fraud and deceit," and "in which an identifiable victim or victims has suffered a physical injury or pecuniary loss." *See* 18 U.S.C. § 3663A(c)(1)(A)(ii), (B). For cases involving "damage to or loss or destruction of property of a victim of the offense," the MVRA requires that the defendant return the property to its owner. If return of the property is "impossible, impracticable, or inadequate," the MVRA requires the defendant to pay an amount equal to the property's value on the date of its damage, destruction, or loss, or its value at the time of sentencing, whichever is greater, less the value of any part of the property that is returned. *See* 18 U.S.C. § 3663A(b)(1).

The theft of trade secrets meets § 3663A's definition of property offenses that require restitution. Section 3663A's legislative history indicates that restitution is required in "violent crimes, *property* and *fraud* crimes under title 18, product tampering, and certain drug crimes." S. Rep. No. 104-179, at 14 (1995), *reprinted in* 1996 U.S.C.C.A.N. 924, 927 (emphasis added). The misappropriation of trade secrets is essentially the theft of property. *Cf. Carpenter v. United States*, 484 U.S. 19, 28 (1987) (holding that newspaper's confidential information qualified as "property"); *Matter of Miller*, 156 F.3d 598, 602 (5th Cir. 1998) (defining misappropriation of proprietary information as the "wrongful taking and use of another's property"); *Westinghouse Elec. Corp. v. U.S. Nuclear Regulatory Comm'n*, 555 F.2d 82, 95 (3d Cir. 1977) (describing "property in the form of its proprietary information"). Accordingly, the theft of trade secrets should qualify as an "offense against property" under § 3663A for which the defendant must make restitution.

As noted, the mandatory restitution statute also applies to any offense where "an identifiable victim has suffered a physical injury or a pecuniary loss." 18 U.S.C. § 3663A(c)(1)(B). Restitution must be ordered "to each

victim in the full amount of each victim's losses as determined by the court and without consideration of the economic circumstances of the defendant." 18 U.S.C. § 3664(f)(1)(A). Thus, to the extent a court has already calculated the loss or injury actually suffered by a victim of trade secret theft in determining the offense level under U.S.S.G. § 2B1.1, the same amount could be used for restitution under the MVRA. For additional discussion of restitution in intellectual property infringement cases, see Chapter VIII of this Manual.

IV.E.2. Sentencing Guidelines

Issues concerning the sentencing guidelines are covered in Chapter VIII of this Manual.

IV.F. Other Charges to Consider

When confronted with a case that implicates confidential proprietary information, prosecutors may wish to consider the following crimes in addition to or in lieu of EEA charges:

- **Disclosing government trade secrets, 18 U.S.C. § 1905**, which punishes government employees and contractors who, *inter alia*, "divulge" or "disclose" government trade secrets. *United States v. Wallington*, 889 F.2d 573 (5th Cir. 1989) (affirming defendant's conviction for running background checks on several people whom the defendant's friend suspected of dealing drugs). Defendants face a fine, a year in prison, and removal from office or employment.
- **Unlawfully accessing or attempting to access a protected computer to obtain information, 18 U.S.C. § 1030(a)(2), (b)**, for access to a computer used for interstate or foreign commerce or by or for a financial institution or the United States government, 18 U.S.C. § 1030(e)(2). The term "information" is to be construed broadly and need not be confidential or secret in nature. S. Rep. No. 104-357, pt. IV(1)(B), at 7 (1996). "'[O]btaining information' includes merely reading it. There is no requirement that the information be copied or transported." *Id.* A violation is a misdemeanor unless it was committed for commercial advantage or private financial gain, to further any tortious or criminal act, or if the information's value exceeds $5,000. *See* 18 U.S.C. § 1030(c)(2).

- **Unlawfully accessing or attempting to access a protected computer to commit fraud, 18 U.S.C. §1030(a)(4), (b)**, where the defendant "knowingly and with intent to defraud," accessed or attempted to access a protected computer without authorization, or in excess of authorized access, and by means of such conduct furthered the intended fraud and obtained anything of value, "unless the object of the fraud and the thing obtained" was computer time worth less than $5,000. What constitutes "fraud" under § 1030(a)(4) is defined broadly. *See* 132 Cong. Rec. 7,189 (1986) ("The acts of 'fraud' that we are addressing in proposed section 1030(a)(4) are essentially thefts in which someone uses a [protected computer] to wrongly obtain something of value from another"); *see also Shurgard Storage Centers, Inc., v. Safeguard Self Storage, Inc.* 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000) (holding that the word "fraud" as used in § 1030(a)(4) simply means "wrongdoing" and does not require proof of the common-law elements of fraud). EEA charges, which generally involve some level of deception and knowing wrongdoing, will often qualify as fraud. Harming a victim's "goodwill and reputation" provides a defendant with something of "value." *See, e.g., In re America Online, Inc.*, 168 F. Supp. 2d 1359, 1380 (S.D. Fla. 2001).

- **Mail or wire fraud**, **18 U.S.C. §§ 1341, 1343, 1346**, for schemes that use the mail or wires to defraud another of property or to deprive them of the intangible right of honest services, which often cover the misappropriation of confidential and proprietary information. *See, e.g.*, *United States v. Martin*, 228 F.3d 1, 16-19 (1st Cir. 2000) (affirming mail and wire fraud convictions for schemes to obtain confidential business information under both theories).

  First, a scheme to defraud another of property includes intangible property, such as confidential, nonpublic, prepublication, and proprietary information. *Carpenter v. United States*, 484 U.S. 19 (1987) (holding that financial journalist's trading on information gathered for his newspaper column defrauded the newspaper of its right to the exclusive use of the information); *United States v. Wang*, 898 F. Supp. 758, 760 (D. Colo. 1995) (holding that 18 U.S.C. § 1343 applies not just to physical goods, wares, or merchandise, but also to confidential computer files transmitted by wire); *United States v. Seidlitz*, 589 F.2d 152 (4th Cir. 1978) (holding that data the defendant downloaded from his former employer's computer system qualified as property under the wire fraud statute and a trade secret).

Second, a scheme to defraud may include the defendant's deprivation of the victim's intangible right to the defendant's honest services, under 18 U.S.C. § 1346. Under § 1346, the defendant is charged not with fraudulently obtaining proprietary information, but rather with breaching his fiduciary duty of loyalty to his employer by misappropriating the proprietary information. *Id.* The government need not, however, prove that the defendant realized financial gain from the theft or attempted theft. *See, e.g., United States v. Kelly*, 507 F. Supp. 495 (E.D. Pa. 1981) (holding that a private employee may be convicted for mail fraud for failing to render honest and faithful services to his employer if he devises a scheme to deceive, mislead, or conceal material information, in case where the defendants violated their employer's policy by extensively using the employer's computer facilities for their own gain and had attempted to conceal their actions from the employer). Section 1346 covers all employees, not just those who work for a government. *See United States v. Martin*, 228 F. 3d 1, 17 (1st Cir. 2000); *United States v. Frost*, 125 F.3d 346, 365 (6th Cir. 1997).

Mail and wire fraud convictions stemming from the theft of trade secrets have been upheld even when charges under the National Transportation of Stolen Property Act, 18 U.S.C. §§ 2314-15, *see infra*, were rejected. *See, e.g.*, *Abbott v. United States*, 239 F.2d 310 (5th Cir. 1956) (affirming § 1341 conviction, but finding insufficient evidence to sustain conviction under 18 U.S.C. § 2314 because government failed to prove market value of map or how or who caused the map to be transported). The mail and wire fraud statute's broader scope results from its concern for the theft of "property" generally, as compared to the NTSP Act's focus on the arguably narrower class of "goods, wares and merchandise" used in § 2314 and § 2315. *See, e.g., Wang*, 898 F. Supp. at 760 (holding that 18 U.S.C. § 1343 applies to items other than physical goods, wares, and merchandise).

For a more detailed discussion of 18 U.S.C. §§ 1341 and 1343, refer to Title 9, Chapter 43 of the U.S. Attorneys' Manual, and contact the Fraud Section of the Criminal Division at (202) 514-7023 for further information and guidance.

- **Criminal copyright infringement**, **17 U.S.C. § 506 and 18 U.S.C. § 2319**, when the defendant stole and reproduced or distributed copyrighted information. The Copyright Act does not preempt trade secret or related charges if the defendant stole

confidential copyrighted material. *See Wang*, 898 F. Supp. at 760-61 (holding that Copyright Act did not preempt wire fraud prosecution for stealing confidential copyrighted material); *Association of Am. Med. Colls. v. Princeton Review, Inc.*, 332 F. Supp. 2d 11, 22-24 (D.D.C. 2004) (analyzing issue and collecting cases).

- **Interstate transportation and receipt of stolen property or goods**, the International Transportation of Stolen Property Act (hereinafter "ITSP Act"), which punishes "[w]hoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud," **18 U.S.C. § 2314**, and "[w]hoever receives, possesses, conceals, stores, barters, sells, or disposes" stolen property that has crossed a state or federal boundary after being stolen, **18 U.S.C. § 2315**.

  At least one court has held that the ITSP Act does not apply to the theft of trade secrets or other proprietary and confidential information unless the information is of a type bought, sold, or transferred in a legitimate or black market. In an unpublished district court opinion, the court held that "goods," "wares," and "merchandise" do not include every item "related to commerce," but rather only "those things that are bought and sold in the marketplace." *United States v. Kwan*, No. 02 CR.241 (DAB), 2003 WL 22973515, at *6 (S.D.N.Y. Dec. 17, 2003). Because the government had not proved that the victim's travel industry "proprietary information includ[ing] hotel contact lists, hotel rate sheets, travel consortium contact lists, travel consortium rate sheets, and cruise operator rate sheets," were the type of goods, wares, or merchandise that were ever bought, sold, or traded in a market, "legal or otherwise," the *Kwan* court vacated the defendant's ITSP conviction. *Id.* at *1, *6.

  Assuming that particular stolen items qualify as goods, wares, or merchandise, the courts agree that sections 2314 and 2315 apply when a defendant steals a tangible object—for example, a piece of paper or a computer disk—that contains intellectual property. *See, e.g.*, *United States v. Martin*, 228 F.3d 1, 14-15 (1st Cir. 2000); *United States v. Walter*, 43 M.J. 879, 884 (N.M. Ct. Crim. App. 1996) ("[C]ourts will include intangible property under the [ITSP] act when tied to tangible property and when the intangible property possesses some business value."); *United States v. Brown*, 925 F.2d 1301, 1308 n.14 (10th Cir. 1991) (holding that even though § 2314

does not apply to theft of intangible property through intangible means, § 2314 would apply to the theft of a piece of paper bearing a chemical formula, even if the paper's intrinsic value were insignificant and the item's overall value was almost wholly derived from the intangible intellectual property contained in the chemical formula) (citing *United States v. Stegora*, 849 F.2d 291, 292 (8th Cir. 1988)) (dictum); *United States v. Lyons*, 992 F.2d 1029, 1033 (10th Cir. 1993) (holding that the defendant's theft of "software in conjunction with the theft of tangible hardware distinguishes this case from *Brown*. *Brown* recognizes that the theft of intangible intellectual property in conjunction with the theft of tangible property falls within the ambit of § 2314."); *United States v. Lester*, 282 F.2d 750 (3d Cir. 1960) (holding that originals and copies of geophysical maps made by defendants on the victim's own copying equipment, with the victim's own supplies, are covered under § 2314); *United States v. Seagraves*, 265 F.2d 876 (3d Cir. 1959) (facts similar to *Lester*); *United States v. Greenwald*, 479 F.2d 320 (6th Cir. 1973) (original documents containing trade secrets about fire retardation processes); *cf. Hancock v. Decker*, 379 F.2d 552, 553 (5th Cir. 1967) (holding that state conviction for theft of 59 copies of a computer program was supported by similar federal court rulings under § 2314) (citing *Seagraves*, 265 F.2d at 876).

Courts are divided, however, on whether the ITSP Act applies to a defendant who transfers intangible property through intangible means, such as electronic data transmission or copying from one piece of paper to another. One view is that it does not. In *Brown*, the defendant was charged with transporting (by means unknown) the source code of a computer program from Georgia to New Mexico, but the government could not prove that the defendant had copied the source code onto the victim's diskettes or that he possessed any of the victim's tangible property. *Brown*, 925 F.2d at 1305-09. The Tenth Circuit held that 18 U.S.C. § 2314 did not cover "[p]urely intellectual property," such as the source code appropriated by the defendant: "It can be represented physically, such as through writing on a page, but the underlying, intellectual property itself, remains intangible" and thus "cannot constitute goods, wares, merchandise, securities or moneys which have been stolen, converted or taken within the meaning of §§ 2314 or 2315." *Id.* at 1307-08. In reaching its decision, the court relied on *Dowling v. United States*, 473 U.S. 207 (1985), which held that property that is "stolen" only in the sense that it is copyright infringing does not fall under the ITSP Act. *See also supra* Chapter

II.F. (discussing application of *Dowling* to charging 18 U.S.C. § 2314 for intellectual property crimes).

The Second Circuit reached the opposite result in *United States v. Bottone*, 365 F.2d 389 (2d Cir. 1966), which pre-dates *Dowling*. The defendants in *Bottone* removed papers describing manufacturing processes from their place of employment and made copies outside the office. They returned the originals and then transported the copies in interstate commerce. In upholding defendants' convictions under 18 U.S.C. § 2314, Judge Friendly stated that:

> when the physical form of the stolen goods is secondary in every respect to the matter recorded in them, the transformation of the information in the stolen papers into a tangible object never possessed by the original owner should be deemed immaterial. It would offend common sense to hold that these defendants fall outside the statute simply because, in efforts to avoid detection, their confederates were at pains to restore the original papers to [their employer] and transport only copies or notes, although an oversight would have brought them within it.

365 F.2d at 393-94.

More recent cases have adopted similar reasoning, notwithstanding *Dowling* and *Brown*, approving of ITSP prosecutions for theft of intangible property by intangible means. *See, e.g.*, *United States v. Kwan*, No. 02 CR.241 (DAB), 2003 WL 21180401, *3 (S.D.N.Y. 2003) (denying the defendant's motion to dismiss, because in determining what would be considered "goods, wares, or merchandise," the Second Circuit "long considered stolen items' commercial nature to be more significant than their tangibility."); *United States v. Farraj*, 142 F. Supp. 2d 484, 488 (S.D.N.Y. 2001) ("The text of § 2314 makes no distinction between tangible and intangible property, or between electronic and other manner of transfer across state lines."); *United States v. Riggs*, 739 F. Supp. 414, 420-21 (N.D. Ill. 1990) (rejecting defendant's "disingenuous argument that he merely transferred electronic impulses [albeit impulses containing computerized text files belonging to Bell South] across state lines. This court sees no reason to hold differently simply because [defendant] stored the information inside computers instead of printing it out on paper. In either case, the information is in a transferrable, accessible, even salable form.").

- **State and local charges.** Many states have laws that specifically address the theft of information. If a state lacks a specific trade-secret law, its general theft statutes may apply.