

Stealing Trade Secrets and Economic Espionage: An Overview of 18 U.S.C. 1831 and 1832

Charles Doyle
Senior Specialist in American Public Law

January 28, 2013

Congressional Research Service
7-5700
www.crs.gov
R42681

CRS Report for Congress
Prepared for Members and Committees of Congress

c11173008

Summary

Stealing a trade secret is a federal crime when the information relates to a product in interstate or foreign commerce, 18 U.S.C. 1832 (theft of trade secrets), or when the intended beneficiary is a foreign power, 18 U.S.C. 1831 (economic espionage). Section 1832 requires that the thief be aware that the misappropriation will injure the secret's owner to the benefit of someone else. Section 1831 requires only that the thief intend to benefit a foreign government or one of its instrumentalities.

Section 1832 (theft) violations are punishable by imprisonment for not more than 10 years, or a fine of not more than $250,000 (not more than $5 million for organizations), or both. Section 1831 (espionage) violations by individuals are punishable by imprisonment for not more than 15 years, or a fine of the greater of not more than $5 million, or both. Section 1831 violations by organizations are punishable by a fine of not more than the greater of $10 million or three times the value of the stolen trade secret. Maximum fines for both individuals and organizations may be higher when the amount of the gain or loss associated with the offense is substantial. Any attempt or conspiracy to commit either offense carries the same penalties as the underlying crime. Offenders must also be ordered to pay restitution. Moreover, property derived from the offense or used to facilitate its commission is subject to confiscation. The sections reach violations occurring overseas, if the offender is a United States national or if an act in furtherance of the crime is committed within the United States.

Depending on the circumstances, misconduct captured in the two sections may be prosecuted under other federal statutes as well. A defendant charged with stealing trade secrets is often indictable under the Computer Fraud and Abuse Act, the National Stolen Property Act, and/or the federal wire fraud statute. One indicted on economic espionage charges may often be charged with acting as an unregistered foreign agent and on occasion with disclosing classified information or under the general espionage statutes.

P.L. 112-269 set the maximum fines described above. It also instructed the United States Sentencing Commission to examine the sufficiency of federal sentencing guidelines and policies in the area of stealing trade secrets and economic espionage. P.L. 112-236 amended the trade secrets prohibition of 18 U.S.C. 1832 to overcome the implications of the Court of Appeals' *Aleynikov* decision. That decision held that the section did not outlaw the theft of computer code designed to facilitate a company's commercial transactions, because the code did not relate to a product to be placed in the stream of commerce.

This report is available in an abridged version, without footnotes or attribution, as CRS Report R42682, *Stealing Trade Secrets and Economic Espionage: An Abridged Overview of 18 U.S.C. 1831 and 1832* .

Contents

Introduction 1
Stealing Trade Secrets 1
Elements 1
Substantive Offense 2
Attempt 7
Conspiracy 8
Consequences 8
Economic Espionage 8
Foreign Beneficiary 10
Common Procedural Matters 10
Protective Orders 10
Extraterritoriality 11
Prosecutorial Discretion 12
Related Offenses 12
Legislation in the 112th Congress 13
Stealing Trade Secrets 13
Economic Espionage 14

Contacts

Author Contact Information 15

Introduction

The Economic Espionage Act (EEA) outlaws two forms of trade secret theft: theft for the benefit of a foreign entity (economic espionage) and theft for pecuniary gain (theft of trade secrets).[1] Under either proscription, its reach extends to theft from electronic storage.[2] Offenders face imprisonment for not more than 10 years in the case of trade secret theft and not more than 15 years in the case of economic espionage.[3] Individuals may incur fines of not more than the greater of $250,000 or twice the loss or gain associated with the offense for trade secret theft and for economic espionage not more than the greater of $5 million or twice the loss or gain.[4] Organizations are fined more severely, up to the greater of $5 million or twice the gain or loss for trade secret theft, and for economic espionage up to a fine of the greater of $10 million, three times the value of the trade secret, or twice the gain or loss associated with the offense.[5]

A court may assess the same sanctions for attempt or conspiracy to commit either offense.[6] A sentencing court must order the defendants to pay victim restitution, and the government may confiscate any property that is derived from or used to facilitate either offense.[7] The government may seek to enjoin violations, but the EEA creates no explicit private cause of action.[8] Conduct that violates the EEA's proscriptions may also violate other federal prohibitions, however. Some, like the Computer Fraud and Abuse Act, in addition to imposing criminal penalties, do authorize victims to sue for damages and other forms of relief under some circumstances.[9]

Stealing Trade Secrets

Elements

The trade secrets prohibition is the more complicated of the EAA's two criminal offenses. It condemns:

[1] 18 U.S.C. 1831 and 18 U.S.C. 1832, respectively.

[2] "Whoever ... without authorization ... downloads, uploads ... transmits ... or conveys" such [trade secret] information.... " 18 U.S.C. 1831(a)(2), 1832(a)(2).

[3] 18 U.S.C. 1832(a), 1831(a).

[4] 18 U.S.C. 1832(a), 3571(b), 1831(a). Here and elsewhere, 18 U.S.C. 3571(c) provides as general matter that the maximum for a criminal fine of any federal criminal offense is the greater of the standard amount set for the particular offense (e.g., $250,000 for individuals convicted of a felony) or twice the gain or loss resulting from the offense. For purposes of brevity in most instances, this report omits reference to this alternative maximum fine level in most instances. Prior to the passage of P.L. 112-269, Section 1831 punished individuals with a fine of not more than $500,000 and individuals with a fine of not more than the greater of $10 million or twice the amount of the gain or loss associated with the offense; see 18 U.S.C. 1831 (2006 ed.).

[5] 18 U.S.C. 1832(b), 1831(b).

[6] 18 U.S.C. 1831(a)(4), (5), 1832(a)(4), (5).

[7] 18 U.S.C. 1834, 2323(c)(restitution), 2323(a)(civil forfeiture), 2323(b)(criminal forfeiture).

[8] 18 U.S.C. 1836.

[9] E.g., 18 U.S.C. 1030(g)(computer fraud and abuse), 2520(interception of electronic communications), 2707 (unauthorized access to an electronic communications facility).

I.
(1) Whoever
(2) with intent to convert
(3) a trade secret
(4) related to
(5) a product or service
(6)(a) used in or
(b) intended for use in
(7)(a) interstate commerce or
(b) foreign commerce
(8) to the economic benefit of anyone other than the owner thereof
(9) (a) intending or
(b) knowing
(10) that the offense will injure the owner of that trade secret
(11) knowingly
(12)(a) steals, without authorization appropriates, takes, carries away, conceals, or by fraud, artifice, or deception obtains such information,
(b) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; [or]
(c) (i) receives, buys, or possesses such information,
(ii) knowing the same to have been stolen or appropriated, obtained, or converted without authorization;
or

II.
(1) Whoever
(2) attempts [to do so];
or

III.
(1) Whoever
(2) conspires with one or more other persons to [do so], and
(3) one or more of such persons do any act to effect the object of the conspiracy.[10]

Substantive Offense

Whoever

The term "whoever" encompasses both individuals and organizations. Thus, individuals and organizations may be guilty of the theft of trade secrets. Subsection 1832(b) confirms this intent by establishing a special fine for "organizations" who commit the offense. For purposes of the

[10] 18 U.S.C. 1832; see also, U.S. Department of Justice, *Criminal Resource Manual* §1129 (May, 1999)(language in italics substituted to reflect P.L. 112-235's amendments) ("In order to establish a violation of 18 U.S.C. §1832, the government must prove: (1) the defendant stole, or without authorization of the owner, obtained, destroyed, or conveyed information; (2) the defendant knew this information was proprietary; (3) the information was in fact a trade secret; (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 [*a product or service used in or intended for use in*] interstate or foreign commerce").

federal criminal code, an "organization" is any "person other than an individual."[11] The Dictionary Act supplies examples of the type of entities that may qualify as "persons"—"the words 'person' and 'whoever' *include* corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals."[12]

With Intent to Convert

Conversion is a common law concept which is defined as "[t]he wrongful possession or disposition of another's property as if it were one's own; an act or series of acts of willful interference, without lawful justification, with any chattel in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the chattel."[13] This "intent to steal" element, coupled with the subsequent knowledge and "intent to injure" elements, would seem to ensure that a person will not be convicted of theft for the merely inadvertent or otherwise innocent acquisition of a trade secret.

Trade Secret

An EEA trade secret is any information that "(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) ... derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public."[14] An owner for these purposes is one "in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed."[15]

Whether an owner has taken reasonable measures to ensure the secrecy of his trade information will depend upon the circumstances of the case. Such measures would ordinarily include limiting access to the information and notifying employees of its confidential nature.[16] Inclusion within the definition of "trade secret" of the instruction that the owner take "reasonable measures" to secure the confidentiality of the information does not render the statute unconstitutionally vague as applied to a defendant whose conduct clearly falls with the statute's proscription.[17]

---

[11] 18 U.S.C. 1832.

[12] 1 U.S.C. 1 (emphasis added).

[13] BLACK'S LAW DICTIONARY 381 (9th ed. 2009).

[14] 18 U.S.C. 1839(3)("[T]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").

[15] 18 U.S.C. 1839(4).

[16] *United States v. Chung*, 659 F.3d 815, 825-29 (9th Cir. 2011)(citations omitted)("[R]easonable measures for maintaining secrecy have been held to include advising employees of the existence of a trade secret, limiting access to a trade secret on a 'need to know basis', and controlling plant access. Security measures, such as locked rooms, security guards, and document destruction methods, in addition to confidentiality procedures, such as confidentiality agreements and document labeling, are often considered reasonable measures").

[17] *United States v. Krumrei*, 258 F.3d 535, 539 (6th Cir. 2001); see also, *United States v. Genovese*, 409 F.Supp.2d 253, 257 (S.D.N.Y. 2005)(rejecting the contention that the "not ... generally known ... to the public" element of the definition of a trade secret was unconstitutionally vague as applied when the evidence showed that he clearly understood that the information he downloaded was not generally known).

Construction of the "known or readily ascertainable" element of the secrecy definition is more perplexing. On its face, the EEA suggests that information is secret if it unknown or undiscoverable by the general public, even if it might be known or discoverable within the industry in which the information is relevant. Congress, however, may have intended a more narrow interpretation of "secret," that is, the information is secret only if it is not known to or reasonably ascertainable either by the general public or within the industry in which the information has value.

The EEA's definition of "trade secret" is "based largely on the definition of that term in the Uniform Trade Secrets Act."[18] The EEA definition refers to information known to or readily ascertainable by the "public."[19] The Uniform Trade Secrets Act (UTSA) definition, however, refers not to the public but to information known to or readily ascertainable by "other persons who can obtain economic value from its disclosure or use."[20] Speaking in the context of an owner's protective measures, the legislative history indicates that "[s]ecrecy in this context means that the information was not generally known to the public or to the business, scientific, or educational community in which the owner might seek to use the information."[21] The question thus far appears to have divided the lower federal appellate courts.[22]

Related to a Product or Service in Commerce

The trade secret must have an interstate or foreign commerce nexus. More specifically, it must be one "that is related to a product or service used in or intended for use in" such commerce.[23] Congress settled upon this phrase after an appellate court held that earlier language covered only theft of a trade secret related to a product that was, or was intended to be, sold or otherwise placed in the stream of commerce.[24]

---

[18] H.Rept. 104-788, at 12 (1996); *United States v. Chung*, 659 F.3d 815, 825 (9th Cir. 2011).

[19] 18 U.S.C. 1839(3)(B).

[20] UNIF. TRADE SECRETS ACT §1(4), 14 U.L.A. 538 (2005). The Uniform Trade Secrets Act definition of trade secrets reads in its entirety: "'Trade Secret' means information, including a formula, pattern, compilation, program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

[21] H.Rept. 104-788, at 12 (1996).

[22] *United States v. Chung*, 659 F.3d 815, 825 (9th Cir. 2011)("There is some conflict between circuits as to whether that deviation alters the 'readily ascertainable' analysis. *Compare United States v. Lange*, 312 F.3d 263, 267 (7th Cir. 2002)(interpreting 'the public' as not necessarily meaning the '*general* public,' but potentially 'the *economically relevant* public' (emphasis in original), with *United States v. Hsu*, 155 F.3d 189, 196 (3d Cir. 1998) (observing that 'the EEA alters the relevant party from whom proprietary information must be kept confidential'). Because Defendant does not contest that the secret information in this case was readily ascertainable, we need not weigh in on this issue").

[23] 18 U.S.C. 1832(a)(language added by P.L. 112-236 in italics)("Whoever, with intent to convert a trade secret that is related to *a product or service used in or intended for use in* interstate or foreign commerce ... ").

[24] *United States v. Aleynikov*, 676 F.3d 71, 80-2 (2d Cir. 2012)(construing 18 U.S.C. 1832(a) which at the time read: "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 ... ")(P.L. 112-236 struck the language in italics in favor of that quoted in italics in the previous footnote in order to overcome the implications of *Aleynikov*, 158 *Cong. Rec*. S6978 (daily ed. Nov. 27, 2012)(introductory remarks of Sen. Leahy)).

Economic Benefit of Another

Someone other than the trade secret's owner must be the intended beneficiary of the theft or destruction.[25] The thief may be, but need not be, the intended beneficiary.[26] Moreover, a close reading of the statute argues for the proposition that no economic benefit need actually accrue; economic benefit need only be intended. Yet if no economic benefit is intended, there is no violation.[27]

Intent to Injure

The government must prove that the defendant intended to injure the trade secret's owner or that he knew the owner would be injured.[28] However, it need not show actual injury. The section "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."[29] Again, the element addresses the defendant's state of mind, not reality. Nothing in the statute's language demands that the government prove actual injury.

Knowingly

The last of the section's three mens rea requirements demands that the defendant be aware that he is stealing, downloading, or receiving a stolen trade secret. There is some dispute over whether this requires the prosecution to prove that the defendant knew that he was stealing, downloading, or receiving *proprietary information* or that he knew that he was stealing, downloading, or receiving a *trade secret*. The Justice Department has used the section's legislative history to reinforce its understanding of this feature of the section:

> "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).
>
> 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"

[25] 18 U.S.C. 1832(a); *United States v. Hsu*, 155 F.3d 189, 195-96 (3d Cir. 1998); *United States v. Jin*, 833 F.Supp.2d 977, 1016 (N.D. Ill. 2012).

[26] U.S. Department of Justice, Executive Office for United States Attorneys, *Prosecuting Intellectual Property Crimes (Justice Report)* 159 (3d ed. September 2006)("The recipient of the intended benefit can be the defendant, a competitor of the victim, or some other person or entity"), available at http://www.justice.gov/criminal/cybercrime/docs/ipma2006.pdf.

[27] *Id.* ("One who misappropriates a trade secret but who does not intend for anyone to gain economically from the theft cannot be prosecuted under [the section]").

[28] 18 U.S.C. 1832(a); *United States v. Jin*, 833 F.Supp.2d 977, 1018 (N.D. Ill. 2012).

[29] H. Rep. No. 104-788, at 11-12 (1996), quoted in *Justice Report* at 159.

> 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). 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.[30]

The courts have not always agreed. Some insist that the prosecution show that the defendant knew the information "had the general attributes of a trade secret."[31]

Stealing and the Like

A person may be guilty of the theft of a trade secret only if he "knowingly" steals a trade secret, replicates a trade secret, destroys or alters a trade secret, or receives a stolen trade secret. Each of the alternative means of deprivation is cast in a separate subsection. The first subsection covers not only stealing a trade secret, but also concealing it or acquiring it by fraud.[32]

Trade secrets are information and thus can be simultaneously held by an owner and a thief. As a result, the second subsection covers situations where the owner is not necessarily deprived of the information, but is denied control over access to it. It proscribes unauthorized copying, downloading, uploading, or otherwise conveying the information. It also outlaws alteration or destruction of a trade secret.[33] The Justice Department has argued that this second means of

---

[30] *Justice Report* at 156-57 (some citations omitted); see also, *United States v. Chung*, 633 F.Supp.2d 1134, 1143 (C.D.Cal. 2009), aff'd, 659 F.3d 815 (9th Cir. 2011)("It is not explicitly clear from the language of section 1831(a)(3)[which corresponds to section 1832(a)(3)] whether the word 'knowingly' modifies the 'trade secret' element of the offense. The Government argues that it does not, and therefore it does not have to prove that Mr. Chung knew that the information he possessed was a trade secret. Mr. Chung contends that the Government must prove that he had such knowledge. The Court agrees with Mr. Chung").

[31] *United States v. Jin*, 833 F.Supp.2d 977, 1011-14 (N.D. Ill. 2012); *United States v. Chung*, 633 F.Supp.2d 1134, 1145 (C.D.Cal. 2009), aff'd on other grounds, 659 F.3d 815 (9th Cir. 2011); but see, *United States v. Krumrei*, 258 F.3d 535, 539 (6th Cir. 2001)(indicating that the government must show that the defendant knew the information was proprietary and thus by implication indicating that the government need not meet the higher standard of showing that he knew the information constituted a trade secret).

[32] 18 U.S.C. 1832(a)(1)(" ... [K]nowingly – (1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information").

[33] 18 U.S.C. 1832(a)(2)("[K]nowingly ... (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or (continued...)

misappropriation includes instances where a faithless employee, former employee, or cyber intruder commits the trade secret to memory and subsequently acts in manner necessary to satisfy the other elements of the offense.[34] It makes the point with some trepidation, however:

> 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."[35]

The third subsection outlaws the knowing receipt of stolen trade secret information.[36] Conviction requires proof that a trade secret was stolen or converted in violation of one of the other subsections and that the defendant knew it.[37]

Attempt

Defendants who attempt to steal a trade secret face the same penalties as those who succeed.[38] Attempt consists of intent to commit the offense and a substantial step towards the attainment of that goal.[39] This would indicate that the information which the defendant seeks to steal need not be a trade secret, as long as he believes it is.[40]

(...continued)

conveys such information").

[34] *Justice Report* at 155 ("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 case law. 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"). See also, *Twenty-Sixth Annual Survey of White Collar Crime: Intellectual Property Crimes*, 49 AMERICAN CRIMINAL LAW REVIEW 929, 934 (2012).

[35] *Justice Report* at 155.

[36] 18 U.S.C. 1832(a)(3)(" ... [K]nowingly ... (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization").

[37] 18 U.S.C. 1832(a)(3); *United States v. Jin*, 833 F.Supp.2d 977, 1015 (N.D.Ill. 2012).

[38] 18 U.S.C. 1832(a).

[39] *United States v. Hsu*, 155 F.3d 189, 202-203 (3d Cir. 1998); *United States v. Lange*, 312 F.3d 263, 268 (7th Cir. 2002); *United States v. Yang*, 281 F.3d 534, 543 (6th Cir. 2002).

[40] *United States v. Hsu*, 155 F.3d at 203 ("It naturally follows that the government need not prove that an actual trade secret was used during the EEA investigation, because the defendant's culpability for a charge of attempt depends only on the 'circumstances as he believes them to be,' not as they really are"); *United States v. Yang*, 281 F.3d at 543-44 ("The Yangs believed that the information Lee was providing was trade secrets belonging to Avery. They attempted to steal that information. The fact that they actually did not receive a trade secret is irrelevant"); but see *United States v. Lange*, 312 F.3d at 269 ("But it is far less clear that [the] sale of information already known to the public could be deemed a substantial step toward the offense, just because the defendant is deluded and does not understand what a trade secret is.... We need not pursue the subject beyond noting the plausibility of the claim and its sensitivity to the facts – what kind of data did the employee think he stole, and so on. For it is not necessary to announce a definitive rule (continued...)

Conspiracy

Defendants who conspire to steal a trade secret also face the same penalties as those who commit the substantive offense.[41] "In order to find a defendant guilty of conspiracy, the prosecution must prove.... that the defendant possessed both the intent to agree and the intent to commit the substantive offense. In addition, the government must prove that at least one conspirator committed an overt act, that is, took an affirmative step toward achieving the conspiracy's purpose."[42] It is no defense that circumstances, unbeknownst to conspirators, render success of the scheme unattainable, as for example when the defendants plotted to steal information that was not in fact a trade secret.[43]

Consequences

Individual offenders face imprisonment for up to 10 years and fines of up to $250,000.[44] The court may fine an organization up to $5 million upon conviction.[45] Both individuals and organizations face a higher maximum fine if twice the gain or loss associated with the offense exceeds the statutory maximum (i.e., $250,000/$5 million).[46] A sentencing court must also order the defendant to pay restitution to the victims of the offense.[47] Property derived from, or used to facilitate, commission of the offense may be subject to confiscation under either civil or criminal forfeiture procedures.[48] The Attorney General may sue for injunctive relief, but there is no explicit private cause of action.[49]

Economic Espionage

The EEA's economic espionage and theft of trade secret offenses share many of the same elements.[50] There are four principal differences. The theft of a trade secret must involve the intent to benefit someone other than the owner.[51] It must involve an intent to injure the owner.[52] And, it must involve a trade secret "that is related to or included in a product that is produced for or placed in interstate or foreign commerce."[53] Economic espionage, on the other hand, must involve

(...continued)

about how dangerous the completed acts must be in trade secret cases: the judge was entitled to (and did) find that Lange had real trade secrets in his possession").

[41] 18 U.S.C. 1832(a).

[42] *United States v. Martin*, 228 F.3d 1, 10-11 (1st Cir. 2000); cf., *United States v. Chung*, 659 F.3d 815, 828-29 (9th Cir. 2011).

[43] *United States v. Hsu*, 155 F.3d at 203-204; *United States v. Yang*, 281 F.3d at 544.

[44] 18 U.S.C. 1832(a), 3571.

[45] 18 U.S.C. 1832(b).

[46] 18 U.S.C. 3571(d).

[47] 18 U.S.C. 1834, 2323(c), 3663A(a), (c). See generally, CRS Report RL34138, *Restitution in Federal Criminal Cases*.

[48] 18 U.S.C. 1834, 2332(a), (b). See generally, CRS Report 97-139, *Crime and Forfeiture*.

[49] 18 U.S.C. 1836.

[50] 18 U.S.C. 1831, 1832.

[51] 18 U.S.C. 1832(a).

[52] *Id*.

[53] *Id.*

an intent to benefit a foreign entity or at least involve the knowledge that the offense will have that result.[54] It does not require an intent to injure the owner.[55] And, it applies to any trade secret, notwithstanding the absence of any connection to interstate or foreign commerce.[56] Finally, economic espionage is punished more severely. The maximum term of imprisonment is 15 years rather than 10 years, and the maximum fine for individuals is $5 million rather than $250,000.[57] For organizations the maximum fine is the greater of $10 million or three times the value of trade secret rather than $5 million.[58] As in the case of stealing trade secrets, the maximum permissible fine may be higher if twice of the amount of the gain or loss associated with the offense exceeds the otherwise applicable statutory maximum.[59]

Section 1831 condemns:

I.

(1) Whoever
(2) intending or knowing the offense will benefit
(3) (a) a foreign government,
(b) a foreign instrumentality, or
(c) a foreign agent
(4) knowingly
(5)(a) steals, without authorization appropriates, takes, carries away, conceals, or by fraud, artifice, or deception obtains a trade secret,
(b) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; [or]
(c) (i) receives, buys, or possesses a trade secret,
(ii) knowing the same to have been stolen or appropriated, obtained, or converted without authorization;

or

II.

(1) Whoever
(2) attempts [to do so];

or

III.

(1) Whoever
(2) conspires with one or more other persons to [do so], and
(3) one or more of such persons do any act to effect the object of the conspiracy.[60]

---

[54] 18 U.S.C. 1831(a)("Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent ... "); *United States v. Jin*, 833 F.Supp.2d 977, 1019 (N.D.Ill. 2012).

[55] *Id.*

[56] *Id.*; *United States v. Aleynikov*, 676 F.3d 71, 79 (2d Cir. 2012)("Thus there is a limitation – [a nexus to] interstate or foreign commerce – in the statute Aleynikov is charged with violating, a limitation that does not appear in the otherwise parallel foreign espionage statute").

[57] 18 U.S.C. 1831(a), 1832(a).

[58] 18 U.S.C. 1831(b), 1832(b).

[59] 18 U.S.C. 3571(d).

[60] 18 U.S.C. 1831; see also *United States v. Chung*, 633 F.Supp.2d 1134, 1146 (C.D.Cal. 2009), aff'd, 659 F.3d 815 (9th Cir. 2011)("Accordingly, under section 1831(a)(3), the Government must prove five elements: (1) Mr. Chung intended to benefit a foreign government; (2) Mr. Chung knowingly possessed trade secret information; (3) Mr. Chung knew the (continued...)

Foreign Beneficiary

A casual reader might conclude that any foreign entity would satisfy Section 1831's foreign beneficiary element.[61] Section 1839's definition of foreign agent and foreign instrumentality, however, makes it clear that an entity can only qualify if it has a substantial connection to a foreign government. The definition of foreign instrumentality refers to foreign governmental control or domination.[62] The description of a foreign agent leaves no doubt that the individual or entity must be the agent of a foreign government.[63]

The theft of a trade secret demands an intent to confer an economic benefit.[64] Economic espionage is not so confined. Here, "benefit means not only economic benefit but also reputational, strategic, or tactical benefit."[65] Moreover, unlike the theft offense, economic espionage may occur whether the defendant intends the benefit or is merely aware that it will follow as a consequence of his action.[66] As in the case of trade secret theft, however, the benefit need not be realized; it is enough that defendant intended to confer it.[67]

Common Procedural Matters

Protective Orders

It would be self-defeating to disclose a victim's trade secrets in course of the prosecution of a thief. Consequently, the EEA authorizes the trial court to issue orders to protect the confidentiality of trade secrets during the course of a prosecution and permits the government to appeal its failure to do so.[68] The government may not appeal an order to reveal information it has already

(...continued)

information was obtained without authorization; (4) the information Mr. Chung possessed was, in fact, a trade secret; and (5) Mr. Chung knew the information was a trade secret"); U.S. Department of Justice, Criminal Resource Manual §1124 ("In order to establish a violation of 18 U.S.C. §1831, the government must prove: (1) the defendant stole or, without authorization of the owner, obtained, destroyed, or conveyed information; (2) the defendant knew this information was proprietary; (3) the information was in fact a trade secret; and (4) the defendant knew the offense would benefit or was intended to benefit a foreign government, foreign instrumentality, or foreign agent").

[61] 18 U.S.C. 1831(a)(" ... [I]ntending or knowing the offense will benefit (3) (a) a foreign government, (b) a foreign instrumentality, or (c) a foreign agent ... ").

[62] 18 U.S.C. 1839(1)("As used in this chapter – (1) the term 'foreign instrumentality' means 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").

[63] 18 U.S.C. 1839(1)("As used in this chapter ... (2) the term 'foreign agent' means any officer, employee, proxy, servant, delegate, or representative of a foreign government").

[64] 18 U.S.C. 1832(a)("Whoever, with the intent to convert a trade secret ... to the economic benefit of anyone other than the owner ... ").

[65] H.Rept. 104-788, at 11 (1996).

[66] 18 U.S.C. 1832(a)("Whoever, with the intent to convert a trade secret ... to the economic benefit of anyone other than the owner ... "); 1831(a)("Whoever, intending or knowing that the offense will benefit ... ").

[67] *Id*.

[68] 18 U.S.C. 1835; *United States v. Hsu*, 155 F.3d 189, 193-94 (3d Cir. 1998).

disclosed to the defendant.[69] Nevertheless, in such instances, appellate review of a district court's disclosure order may be available through a writ of mandamus.[70]

Extraterritoriality

The Supreme Court has said on a number of occasions that "[i]t is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States'"[71] With this in mind, Congress specifically identified the circumstances under which it intended the economic espionage and theft of trade secrets provisions to apply overseas.[72] Either offense may be prosecuted as long as the offender is a U.S. national or an act in furtherance of the offense is committed within this country.[73]

The legislative history indicates that these are the only circumstances under which violations abroad may be prosecuted.[74] This may mean that foreign conspirators may not be charged unless some overt act in furtherance of the scheme occurs in the United States.[75] It may also preclude prosecution when trial would have been possible in the absence of an express provision. For example, in the absence of the limiting provision, the courts would likely conclude that Congress

[69] *United States v. Ye*, 436 F.3d 1117, 1120-121 (9th Cir. 2006)("The plain language of the EEA indicates that the government can file an interlocutory appeal pursuant to §1835 only where a district court's order actually directs or authorizes the disclosure of a trade secret.... Here, the district court's order did not provide for the disclosure of any trade secret materials. In its opening brief in this court, the government acknowledges that it had already turned over all relevant trade secret materials and documents.... Because the purpose of the district court's order was only to clarify exactly which materials the government contends constitute the protected trade secrets, and all relevant materials had already been turned over, the district court's order does not direct or authorize the 'disclosure' of trade secrets as required by the plain language of §1835").

[70] *Id.* at 1121-124. Mandamus relief is a discretionary remedy ordinarily only available when the petitioner can show: the absence of any other form of relief, a clear right to issuance of the writ, and that recourse to this extraordinary form of relief is appropriate under the circumstances, *Cheney v. United States District Court*, 542 U.S. 367, 380-81 (2004). The lower federal appellate courts sometimes describe these requirements in greater detail, see e.g., *Lewis v. Ayers*, 681 F.3d 992, 998 (9th Cir. 2012)("In *Bauman*, we established five guidelines to determine whether mandamus is appropriate in a given case:(1) whether the petitioner has no other means, such as a direct appeal to obtain the desired relief; (2) whether the petitioner will be damaged or prejudiced in any way not correctable on appeal; (3) whether the district court's order is clearly erroneous as a matter of law; (4) whether the district court's order is an oft repeated error or manifests a persistent disregard of the federal rules; and (5) whether the district court's order raises new and important problems or issues of first impression"); *In re Jones*, 680 F.3d 640, 642 (6th Cir. 2012)(essentially the same).

[71] *Morrison v. National Australia Bank Ltd*., 130 S.Ct. 2869, 2877 (2010), quoting *EEOC v. Arabian American Oil Co*., 449 U.S. 244, 248 (1991) and *Foley Bros., Inc. v. Filardo*, 336 U.S. 281 (1949). See generally, CRS Report 94-166, *Extraterritorial Application of American Criminal Law*.

[72] H.Rept. 104-788, at 14 (1996).

[73] 18 U.S.C. 1837 ("This chapter also applies to conduct occurring outside the United States if - (1) the offender is a natural person who 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").

[74] H.Rept. 104-788, at 14 (emphasis added)("To ensure that there is some nexus between the ascertaining of such jurisdiction and the offense, however, extraterritorial jurisdiction exists *only* if [an overt act occurs within the United States or the offender is a U.S. national]").

[75] 18 U.S.C. 1837 (emphasis added)("This chapter also applies to conduct occurring outside the United States if - (1) the *offender* is a natural person who 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").

intended to allow prosecution of overseas offenses of foreign nationals that have an impact within the United States.[76]

Prosecutorial Discretion

For five years after passage of the Economic Espionage Act, neither economic espionage nor trade secret violations of its provisions could be prosecuted without the approval of senior Justice Department officials. Prosecutors must still secure approval before bringing charges of economic espionage, but approval is no longer necessary for the prosecution of theft of trade secret charges.[77]

Related Offenses

Conduct that violates the Economic Espionage Act may violate other federal criminal provisions as well. In the case of trade secret offenses, potentially corresponding offenses include violations of the Computer Fraud and Abuse Act, the National Stolen Property Act, and the federal wire fraud statute. The Computer Fraud and Abuse Act outlaws accessing certain computers or computer systems without authorization or in excess of authorization, with the intent to defraud.[78] The National Stolen Property Act outlaws the interstate transportation of tangible stolen property

[76] *Ford v. United States*, 273 U.S. 593, 623 (1927)("A man who outside of a country willfully puts in motion a force to take effect in it is answerable at the place where the evil is done"); *United States v. Yousef*, 327 F.3d 56, 96-7 (2d Cir. 2003)("Moreover, assertion of jurisdiction is appropriate under the 'objective territorial principle,' because the purpose of the attack was to influence United States foreign policy and the defendant intended their actions to have an effect – in this case a devastating effect – on and within the United States"); *United States v. Felix-Guiterrez*, 940 F.2d 1200, 1205 (9th Cir. 1991)(Felix's actions created a significant detrimental effect in the United States ... "). See also *The Extraterritorial Application of the Economic Espionage Act of 1996*, 23 HASTINGS INTERNATIONAL AND COMPARATIVE LAW REVIEW, 527, 553-54 (2000)("If a foreign company possesses no operations in the U.S. and engages in trade secret theft against a U.S. entity entirely outside the U.S., Then EEA cannot apply. In that respect, the extraterritorial jurisdiction under the EEA may fall short of the jurisdictional reach applied under a 'pure' effects test in antitrust law – where the Sherman Act can reach conduct entirely extraterritorial in nature").

[77] U.S. Department of Justice, *Criminal Resource Manual* §1122 ("Prior to passage of the EEA, the Attorney General assured Congress in writing that for a period of five years, the Department of Justice would require that all prosecutions brought under the EEA must first be approved by the Attorney General, the Deputy Attorney General, or the Assistant Attorney General to the Criminal Division. (See October 1, 1996 letter from Attorney General Janet Reno to Chairman Orrin Hatch, Criminal Resource Manual at 1123). This requirement expired on October 11, 2001. Subsequently, the Attorney General renewed the prior requirement for initiating prosecutions under 18 U.S.C. §1831.... The requirement was not extended for cases under 18 U.S.C. §1832 ... ").

[78] 18 U.S.C. 1030(a)(4), (e)(2)("(a) Whoever ... (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period ... shall be punished as provided in subsection (c) of this section.... (e) As used in this section ... (2) the term 'protected computer' means a computer - (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States"); e.g., *United States v. Koo,* 770 F.Supp.2d 1115, 1118 (D.Ore. 2011)(defendant indicted for computer fraud and abuse and for trade secrets violations); see generally, CRS Report 97-1025, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws*.

or the knowing receipt of such property.[79] The federal wire fraud statute outlaws the use of wire communications in execution of a scheme to defraud.[80]

In addition in the case of economic espionage violations, a defendant may be subject to prosecution under the general espionage statutes or with failure to register as the agent of a foreign power. Foreign agents, other than diplomatic personnel, must register with the Attorney General; failure to do so is generally a felony.[81] The general espionage laws are only likely to be triggered if the trade secret information is also classified information or is national defense information.[82]

Legislation in the 112th Congress

Congress amended the EEA twice during the 112th Congress. The Theft of Trade Secrets Clarification Act of 2012 clarified the trade secrets jurisdiction element.[83] The Foreign and Economic Espionage Act of 2012 increased the maximum fine levels for economic espionage.[84] It also directed the United States Sentencing Commission to reexamine its treatment of economic espionage and the overseas transmission of stolen trade secrets.[85]

Stealing Trade Secrets

On November 27, 2012, Senator Leahy introduced, and the Senate passed by unanimous consent, the Theft of Trade Secrets Clarification Act (S. 3642).[86] The proposal reworded the jurisdictional

[79] 18 U.S.C. 2314 ("Whoever 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.... shall be fined under this title or imprisoned not more than ten years or both ... "); 18 U.S.C. 2315("Whoever receives, possesses, conceals, stores, barters, sells, or dispose of any goods, ware, or merchandise, securities, or money of the value of $5,000 or more ... which have crossed a State of United States boundary after being stolen ... knowing the same to have been stolen ... shall be fined under this title or imprisoned not more than ten years, or both"); see also, *United States v. Aleynikov*, 676 F.3d 71, 76-9 (2d Cir. 2012)(stolen, intangible computer source code is neither a good, ware, nor merchandise for purposes of the National Stolen Property Act).

[80] 18 U.S.C. 1343 ("Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire ... any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined under this title or imprisoned not more than 20 years, or both ... "); e.g., *United States v. Hsu*, 155 F.3d 189, 193 (3d Cir. 1998)(defendant indicted for wire fraud and trade secrets violations); *United States v. Koo,* 770 F.Supp.2d 1115, 1118 (D.Ore. 2011)(same); see generally, CRS Report R41930, *Mail and Wire Fraud: A Brief Overview of Federal Criminal Law*.

[81] 18 U.S.C. 951(a)("Whoever, other than a diplomatic or consular officer or attaché, acts in the United States as an agent of a foreign government without prior notification to the Attorney General if required in subsection (b), shall be fined under this title or imprisoned not more than ten years, or both"); e.g., *United States v. Chung*, 659 F.3d 815, 819 (9th Cir. 2011)(defendant indicted for economic espionage and unregistered foreign agent violations).

[82] 18 U.S.C. 798, outlaws the unauthorized disclosure of classified information relating to communications intelligence; 18 U.S.C. 1924 outlaws the unauthorized retention of classified information; and 18 U.S.C. 793, 794 outlaw the unauthorized gathering or transmitting national defense information; see generally CRS Report RS21900, *The Protection of Classified Information: The Legal Framework*.

[83] P.L. 112-236 (S. 3642), 126 Stat. 1627 (2012), amending, 18 U.S.C. 1832(a).

[84] Section 2, P.L. 112-269 (H.R. 6029), 126 Stat. 2442 (2013), amending, 18 U.S.C. 1831(a), (b).

[85] Section 3, P.L. 112-269 (H.R. 6029), 126 Stat. 2442-443 (2013).

[86] 158 *Cong. Rec.* S6979 (daily ed. Nov. 27, 2012).

element of the trade secret provision to cover secrets relating to products or services used or intended for use in interstate or foreign commerce. Senator Leahy explained that:

> A recent decision of the Second Circuit in United States v. Aleynikov casts doubt on the reach of the statute. A jury in that case found the defendant guilty of stealing computer code from his employer. The court overturned the conviction, holding among other thing that the trade secret did not meet the interstate commerce prong of the statute, even though the defendant had copied the stolen code from his office in New York to a server in Germany; downloaded the code to his home computer in New Jersey; then flew to his new job in Illinois with the stolen source code in his possession; and the code was used in interstate commerce.
>
> The court held that the Economic Espionage Act provision applies only to trade secrets that are part of a product that is produced to be placed in interstate commerce. Because the company's proprietary software was neither placed in interstate commerce nor produced to be placed in interstate commerce, the law did not apply – even though the stolen source code was part of the financial trading system that was used in interstate commerce every day.[87]

The House passed the measure shortly thereafter under suspension of the rules,[88] and the President signed it into law on December 28, 2012.[89]

Economic Espionage

On August 1, 2012, the House passed the Foreign and Economic Espionage Penalty Enhancement Act of 2012 (H.R. 6029), under suspension of the rules.[90] The Senate Judiciary Committee had previously reported favorably a similar proposal as the Economic Espionage Penalty Enhancement Act (S. 678).[91] Unlike the Senate bill, the House legislation would have increased the penalties for violations of 18 U.S.C. 1831 (economic espionage). Under the House-passed proposal the maximum term of imprisonment would have increased from not more than 15 years to not more than 20 years.[92] Section 1831 previously punished individual defendants with a fine of not more than the greater of $500,000 or twice the loss or gain associated with the offense and punished organizational defendants with a fine of not more than the greater of $10 million or twice the loss or gain.[93] The House bill would have amended it to permit a fine for an offending individual of not more than the greater of $5 million or twice the loss or gain and to permit a fine for an offending organization of not more than the greater of $10 million, three times the value of the stolen trade secret, or twice the gain or loss associated with the offense.[94]

Neither proposal would have changed the maximum terms of imprisonment (not more than 10 years) or the maximum fines for trade secret violations ($250,000 for individuals; $5 million for organizations).[95] Both would have instructed the United States Sentencing Commission to

---

[87] 158 *Cong. Rec*. S6968 (daily ed. Nov. 27, 2012).

[88] 158 Cong. Rec. H6849 (daily ed. Dec. 18, 2012).

[89] P.L. 112-236, 126 Stat. 1627 (2012).

[90] 158 *Cong. Rec*. H5619 (daily ed. August 1, 2012); see also, H.Rept. 112-610.

[91] Reported favorably without printed report and placed on the calendar, 157 *Cong. Rec.* S8460 (daily ed. December 8, 2011).

[92] H.R. 6029, §2(a)(1), proposed 18 U.S.C. 1831(a).

[93] 18 U.S.C. 1831(a), (b).

[94] H.R. 6029, §§2(a)(2), 2(b), proposed 18 U.S.C. 1831(a), (b).

[95] 18 U.S.C. 1832(a), (b), 3571(b). Under existing law, a defendant, individual or organizational, may be fined up to twice the loss or gain association with the offense when that amount exceeds the statutory maximum, 18 U.S.C. (continued...)

reexamine the treatment of economic espionage and overseas transmission of stolen trade secrets under the Commission's sentencing guidelines.

The legislation is a reaction to reports of increased foreign predatory action and of "sensitive US economic information and technology ... targeted by the intelligence services, private sector companies, academic and research institutions, and citizens of dozens of countries."[96]

The Senate agreed to the House-passed proposal, but not before removing the provision that would have increased the length of the maximum prison term.[97] The House agreed to the Senate amendment under suspension of the rules.[98] The President signed the proposal on January 14, 2013.[99]

Author Contact Information

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968

(...continued)

3571(c).

[96] H.Rept. 112-610, at 2 (2012), quoting Office of the National Counterintelligence Executive, *Foreign Spies, Stealing US Economic Secrets in Cyberspace, Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, at i (Oct. 2011).

[97] 158 *Cong. Rec.* S8230 (daily ed. Dec. 19, 2012).

[98] 158 *Cong. Rec*. H7455 (daily ed. Dec. 30, 2012).

[99] P.L. 112-269, 126 Stat. 2442 (2013).