University of Dayton Law Review

Volume 25
Number 2 *25th Anniversary Edition (Part 2)*

Article 6

1-15-2000

The Criminalization of Trade Secret Theft under the Economic Espionage Act of 1996: An Evaluation of United States v. Hsu, 40 F.Supp. 2d 623 (E.D. Pa. 1999)

Robin D. Ryan
University of Dayton

NOTES

THE CRIMINALIZATION OF TRADE SECRET THEFT UNDER THE ECONOMIC ESPIONAGE ACT OF 1996: AN EVALUATION OF *UNITED STATES V. HSU*, 40 F. SUPP.2D 623 (E.D. PA. 1999)

Robin D. Ryan[*]

TABLE OF CONTENTS

---

[*] Executive Editor, 2000-2001, University of Dayton Law Review. J.D. expected, May 2001, University of Dayton School of Law; B.A., 1995, Ohio University.

I. INTRODUCTION

With the increasing economic value of intellectual property, it is imperative that trade secrets be protected from both domestic and foreign thieves. The Economic Espionage Act ("EEA") makes it a criminal offense to steal, attempt to steal, or conspire to steal the trade secrets of another.[1] As the EEA's legislative history points out, "a piece of information can be as valuable as a factory is to a business," thus, the EEA is an attempt to provide more protection for trade secrets than is currently given under civil laws.[2] While many states have adopted a version of the Uniform Trade Secrets Act ("UTSA") to protect trade secrets from theft,[3] these civil laws cannot provide the necessary sanctions to deter the theft of trade secrets and the lack of criminal sanctions is an "unacceptable oversight."[4] Often times, companies may not have the resources available to bring a civil suit and even if they do bring suit, "the civil penalties often are absorbed by the offender as a cost of doing business . . . ."[5] Unfortunately, Congress' first attempt at criminal prosecution for trade secret theft may conflict with the constitutional requirement that penal statutes define the crime with sufficient clarity.[6] Therefore, the EEA may be void for vagueness.[7]

The "void for vagueness" issue was raised in the Eastern District of Pennsylvania in *United States v. Hsu*.[8] Kai-Lo Hsu, the defendant, was indicted for conspiring to steal and attempting to steal documents that allegedly contained trade secrets, but which the court later found may not have even contained any trade secrets.[9] The court had great difficulty with

---

[1] 18 U.S.C. § 1832 (1996).

[2] S. REP. NO. 104-359, at 6, 11 (1996).

[3] *Id.* at 11. The Uniform Trade Secrets Act recognizes misappropriation of a trade secret as a tort, in which case, suit would be brought in a civil court. *Id.*

[4] *Id.* at 6, 11.

[5] *Id.* at 11.

[6] The United States Supreme Court has stated that the Fifth and Fourteenth Amendments' due process clauses require that penal statutes be described so that "men of common intelligence" can ascertain the meaning of the statute and what is proscribed. WAYNE R. LAFAVE & AUSTIN W. SCOTT, JR., CRIMINAL LAW § 2.3, at 90-91 (2d ed. 1986).

[7] The "void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." Kolender v. Lawson, 461 U.S. 352, 357 (1983) (internal citations omitted).

[8] 40 F. Supp.2d 623 (E.D. Pa. 1999).

[9] *Id.* at 625, 627-31.

the vague definition of what constituted a trade secret under the EEA.[10] The EEA defines "trade secret" as information that is not "generally known" to, and not being "readily ascertainable" by the "public" when the owner "has taken reasonable measures to keep such information secret."[11] As the court noted, in an era of ever-expanding information availability, such concepts will be hard to define with precision and clarity.[12] It appears that Congress derived the definition of "trade secret" in the EEA from the definition of the same term used in the UTSA,[13] perhaps illustrating, Congress' willingness to be guided by existing law.

This Note argues that, while the particular indictment in *Hsu* can be defended given the facts of the case, the EEA is poorly drafted and vulnerable to constitutional challenges as a criminal statute that is void for vagueness and, in some circumstances, may be overbroad. The EEA's definition of what constitutes a trade secret is problematic in that what is "generally known" or "readily ascertainable" by the "public," and what is considered "reasonable measures" to keep information secret are phrases that lack any consistency and thus promote an ad hoc application of the statute. Because the risk of inconsistency cannot be justified in our criminal justice system, justice requires that penal statutes be drafted so that ordinary people are aware of what conduct is prohibited.[14] The EEA is a fairly new criminal statute and it would be unwise to assume that the EEA's language will withstand a constitutional attack in the criminal context simply because the language was taken from civil statutes that withstood attacks in the civil context.

Part II of this Note provides the background of *Hsu* and the court's rationale for its holding.[15] Part III evaluates the court's decision in *Hsu* and proposes that although the facts of the case support the indictment, there are situations in which the EEA will fall prey to constitutional challenges.[16] Discussed in detail are reasons why the EEA's language is troubling and under what circumstances the statute could be deemed void for vagueness.[17] This Note also proposes changes to the EEA that would

---

[10] *Id.* at 631.

[11] 18 U.S.C. § 1839(3)(A) (1996).

[12] *Hsu*, 40 F. Supp.2d at 630.

[13] *See supra* note 3 and accompanying text. *Compare* UNIF. TRADE SECRETS ACT § 1(4), 14 U.L.A. 438 (1990) and Economic Espionage Act (EEA), 18 U.S.C. §§ 1831-39 (1996).

[14] *See supra* note 6 and accompanying text.

[15] *See infra* notes 19-56 and accompanying text.

[16] *See infra* notes 57-127 and accompanying text.

[17] *See infra* notes 57-127 and accompanying text.

clarify the murky boundaries of the statute.[18] Part IV concludes that although an ad hoc application of the EEA may be justified on some occasions, there are other instances when the EEA may not pass constitutional muster, such as when the indictment is for a completed offense.

II. BACKGROUND

A. Background of the EEA

In 1996, Congress passed the EEA making it a crime to steal, attempt to steal, or conspire to steal, trade secrets for the benefit of anyone other than the owner of the trade secrets.[19] Congress enacted the EEA in response to the growing number of trade secret thefts.[20] The legislative history indicates that federal statutes protected other forms of intellectual property,

---

[18] *See infra* notes 124-27 and accompanying text.

[19] 18 U.S.C. § 1832 (1996). Section 1832 states:

(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.

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than $5,000,000.

Id.

[20] S. REP. NO. 104-359, at 8 (1996).

such as patents and copyrights.[21] Until the enactment of the EEA, prosecutors who sought to charge an alleged offender for stealing or attempting to steal trade secrets were confined to prosecute under fraud or copyright law.[22] These prosecutions were difficult and largely unsuccessful.[23] Similarly, state civil laws provided too little protection which was often in the form of an injunction.[24] In addition to the bare bones protection of the civil laws, once the trade secrets were in the public domain, the damage was irreparable.[25] Furthermore, Congress realized that the well-being and security of the nation depends, in large part, on the stability of American companies and their ability to compete in world-wide markets.[26] For these reasons, Congress protected American companies from misappropriation of trade secrets, from both foreign and domestic thieves, by enacting the EEA.[27]

B. Facts and Procedural History of United States v. Hsu

Targets of a Federal Bureau of Investigation ("FBI") sting operation, the defendant and his co-conspirators made contact with an undercover FBI agent for the purpose of buying Taxol technology pertaining to a highly valuable anti-cancer drug.[28] One of Hsu's alleged co-conspirators requested the trade secret information from undercover FBI Agent John Hartman.[29] The co-conspirator incorrectly believed that Agent Hartman was a technological information broker, and set up a meeting to introduce Hartman to Hsu, the Technical Director of a Taiwanese company.[30] A two-year sting operation ensued.[31] After being told by Agent Hartman that Bristol-Myers Squibb ("Bristol-Myers") would not be forthcoming with information concerning its technology, Hsu allegedly proposed that Hartman find a corrupt employee who would be willing to sell the Taxol

---

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] *Id.* at 5.

[27] *Id.* at 8-9.

[28] United States v. Hsu, 155 F.3d 189, 191-93 (3d Cir. 1998).

[29] *Id.* at 192. For ease of discussion, this Note will only address the defendant Kai-Lo Hsu by name.

[30] *Id.*

[31] *Id.*

technology.[32] On June 14, 1997, Agent Hartman presented a "corrupt" employee, cooperating with the FBI, who displayed documents allegedly containing trade secrets.[33] After extensively questioning the employee about the background, history, and production of the Taxol technology, Hsu was arrested.[34] On July 10, 1997, Hsu was indicted for attempting and conspiring to steal trade secret information from the company.[35]

The complex procedural history of *United States v. Hsu* best demonstrates the infancy of the EEA. The case traveled between the district courts of the Eastern District of Pennsylvania and the appellate court of the Third Circuit with various issues in dispute. The initial suit raised the issue of whether the defendant should have access to the confidential material for preparing his defense, with the district court finding that he should.[36] In an interlocutory appeal, the Third Circuit remanded the case to the district court holding that because legal impossibility is not a defense in attempt and conspiracy cases, the defendant should not have access to the confidential information.[37] On remand, the Eastern District of Pennsylvania denied defendant Hsu's motion to dismiss on void for vagueness grounds.[38] While the district court acknowledged the vagueness of some of the EEA's language, due to Hsu's unquestionably illegal conduct the court denied the defendant's motion to dismiss.[39]

C. The District Court's Rationale, Holding, and Rejection of Hsu's Claims

Hsu claimed that the EEA was unconstitutional on two grounds: 1) overbreadth and 2) vagueness. Hsu argued that the EEA was overbroad because the First Amendment rights of the "corrupt" employee were at issue.[40] Hsu continued by arguing that an employee has the right to communicate with anyone he or she wishes.[41] The district court rejected this argument and pointed out that a statute can only be deemed overbroad

---

[32] *Id.*

[33] *Id.*

[34] *Id.* at 192-93.

[35] *Id.* at 191.

[36] United States v. Hsu, 982 F. Supp. 1022 (E.D. Pa. 1997).

[37] United States v. Hsu, 155 F.3d 189 (3d Cir. 1998).

[38] United States v. Hsu, 40 F. Supp.2d 623, 630-31 (E.D. Pa. 1999).

[39] *Id.*

[40] *Id.* at 627.

[41] *Id.*

or facially unconstitutional if the statute infringes on First Amendment rights.[42] The district court concluded that the First Amendment is not automatically implicated simply because an employee has a right to expression.[43] The court further stated that even if the employee wanted to invoke his or her right, Hsu lacked standing to bring the claim on behalf of the employee.[44] Thus, the facts in *Hsu* did not implicate the First Amendment and the EEA could not be considered overbroad and, therefore, facially unconstitutional.

The district court did, however, entertain Hsu's claim that the EEA is void for vagueness.[45] Although the court found that the statute is not vague in *Hsu*, the court struggled with several key terms in the statute.[46] Hsu argued that "generally known," "readily ascertainable," "reasonable measures," and "related to" were phrases that prevent consistent application of the EEA.[47] The court specifically agreed that "generally known" and "readily ascertainable" were constitutionally problematic given that what is available to the public is never really certain at any given moment but, nevertheless, the court viewed the EEA in light of Hsu's conduct and held the statute constitutional.[48]

Defendant Hsu argued that what is "related to" a trade secret is unconstitutionally vague.[49] Because the defendant only cited to First Amendment cases in support of his vagueness argument and the court had already ruled that the statute is not overbroad, the defendant's vagueness claim was without merit.[50] The court found that regardless of whether "related to" is an ambiguous phrase, Hsu had to have known that the second generation Taxol technology, which Hsu allegedly sought to acquire, was "related to" the first generation of the same technology, which

---

[42] *Id.* at 626-27. When a statute implicates First Amendment rights, the statute can be challenged as overbroad and unconstitutional on its face. United States v. Mazurie, 419 U.S. 544, 550 (1975). Where, as here, there are no First Amendment issues, the statute can be challenged but must be done on vagueness grounds and it must be evaluated as the statute applies to the defendant. *See id.*

[43] *Hsu*, 40 F. Supp.2d at 627.

[44] *Id.* If the "corrupt" employee sought redress for a First Amendment violation, he would have to bring the suit himself. *Id.*

[45] *See id.* at 627-31.

[46] *Id.* at 630-31.

[47] *Id.*

[48] *Id.* at 629-31.

[49] *Id.* at 627-28.

[50] *Id.* at 627. The court reasoned that Hsu raised a vagueness challenge, but that he incorrectly supported his challenge with First Amendment cases, which can only be used in an overbreadth challenge. *Id.*

was a protected trade secret.[51] In finding that Hsu knew or should have known this, the court held that the EEA is neither overbroad nor void for vagueness.[52]

Similarly, the district court rejected Hsu's argument that the EEA is vague in its use of "generally known" and "readily ascertainable."[53] The court found these terms slightly more troubling because what is "generally known" or "readily ascertainable" is difficult to ascertain at any given moment in time.[54] Ultimately, the court focused on the fact that Hsu and his co-conspirators were continuously warned by Agent Hartman that the information was secret and could not be obtained through legal channels.[55] The repeated warnings led the court to conclude that Hsu knew or believed that the information was not "generally known" or "readily ascertainable" and, therefore, those terms are not vague as applied to the defendant.[56]

III. ANALYSIS

A. Indictment Is Proper Based on the Facts of the Case

1. Relevant Facts Lending Support to the Indictment

The Eastern District of Pennsylvania had considerable concerns regarding the EEA's "vaporous" terms[57] but, because of the facts, the court found that the EEA is not void for vagueness.[58] While the particular indictment in *Hsu* can be defended, the *Hsu* court recognized that the EEA is poorly drafted and is vulnerable to constitutional challenges as a criminal statute. The indictment in *Hsu* is proper based on the defendant's conduct preceding the arrest. The indictment arose out of a sting operation in which an FBI agent posed as a broker who allegedly offered to obtain trade

---

[51] *Id.* at 627-28.
[52] *Id.* at 630-31.
[53] *Id.* at 628-31.
[54] *Id.* at 630.
[55] *Id.* at 630-31.
[56] *Id.* at 630.
[57] *Id.*
[58] *Id.* at 630-31.

secret information for the defendant.[59] The agent told the defendant that he could only get the information through illegal channels,[60] which put him on notice that the owner of the trade secrets sought to keep the information secret. These facts clearly support the indictment.

The defendant was charged only with conspiracy and attempt to steal trade secrets.[61] Addressing the issue of inchoate offenses, or incomplete offenses, such as conspiracy and attempt,[62] the Third Circuit, following well-established principles, made it clear that "the defendant's culpability for a charge of attempt depends only on the circumstances as the defendant *believes* them to be and not as they really are."[63] In considering the government's burden of proof for inchoate offenses, the Third Circuit stated that the government only needs to 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."[64]

Thus, the difference between inchoate or attempted crimes and completed crimes is that for an inchoate offense, such as attempted theft, the defendant needs only to believe that the documents are trade secrets. For completed offenses, theft, for example, the defendant's belief that a crime had been committed is insufficient to sustain a conviction;[65] the government must prove that the defendant's conduct was *actually* illegal.[66]

2. Inchoate Crimes and the Doctrines of Impossibility

For inchoate crimes, the government can satisfy its burden of proof by demonstrating beyond a reasonable doubt that the defendant made a

---

[59] United States v. Hsu, 155 F.3d 189, 192-93 (3d Cir. 1998).

[60] *Id.* at 192.

[61] *Hsu*, 40 F. Supp.2d at 625.

[62] *Hsu*, 155 F.3d at 203.

[63] *Hsu*, 40 F. Supp.2d at 629 (citing *Hsu*, 155 F.3d 189, 203-04 (3d Cir. 1998)).

[64] *Hsu*, 155 F.3d at 203 (emphasis added).

[65] LAFAVE & SCOTT, *supra* note 6, § 6.2(c)(1). If a defendant intends "to do something which he believed was against the law but which in fact was not unlawful, then he cannot be said to have engaged in a criminal attempt." *Id.*

[66] *Id.*

substantial step toward the commission of a crime.[67] The proper inquiry is whether the defendant's conduct would have constituted commission of a crime if the circumstances were as he or she believed them to be.[68] The circumstances do not have to be, in reality, what the defendant believes them to be in order to be indicted and convicted for an inchoate crime.[69] The justification for the requirement that the defendant merely believe that he or she is committing a crime is based on "the actor's intention to break the law and a demonstrated willingness to act on that intention, as shown by the externalization of intent."[70] In *Hsu,* for example, the defendant argued that although he believed that the documents contained trade secrets, it was *legally impossible* to conspire and attempt to steal trade secrets unless the documents used in the sting operation did, in fact, contain trade secrets.[71] However, the question of whether the documents used in the sting contained trade secrets is one of *factual impossibility*,[72] which is never a defense to an attempt charge because the defendant who attempts to commit a crime has the same mental state as a defendant who completes the crime.[73] The line between *legal impossibility* and *factual impossibility* is often blurred.[74] The Third Circuit stated that *legal impossibility* is not a defense for Hsu because Congress intended to draft "a comprehensive solution to economic espionage" and certainly would not want "the courts to thwart that solution by permitting defendants to assert . . . legal impossibility."[75]

---

[67] ROLLIN M. PERKINS & RONALD N. BOYCE, CRIMINAL LAW ch. 6, § 3(A)(5), at 628 (3d ed. 1982).

[68] *Id.* at 632.

[69] United States v. Hsu, 40 F. Supp.2d 623, 628 (E.D. Pa. 1999).

[70] PAUL H. ROBINSON, CRIMINAL LAW § 11.1, at 628 (1997).

[71] *Hsu*, 40 F. Supp.2d at 625 n.1.

[72] United States v. Hsu, 155 F.3d 189, 199 (3d Cir. 1998).

[73] LAFAVE & SCOTT, *supra* note 6, § 6.3(a)(2).

[74] *Id.* Factual impossibility exists when "what the defendant intends to accomplish is proscribed by the criminal law, but he is unable to bring about that result because of some circumstances unknown to him when he [or she] engaged in the attempt . . . ." *Id.* § 6(a)(3). This is different from legal impossibility. Legal impossibility exists if the accused had completed an act which he attempted to do and yet would not be guilty of a criminal offense because his conduct was not proscribed by law. *Id.*

[75] *Hsu*, 155 F.3d at 202.

3. Hsu's Vagueness and Overbreadth Arguments

While the claims ultimately failed, Hsu argued that the EEA is both vague and overbroad.[76] Where, as here, the First Amendment is not implicated, the void for vagueness doctrine may be raised, but a general claim of overbreadth may not.[77] The nature of the defendant's attack, whether it is based on vagueness or overbreadth, determines his or her burden of proof. When dealing with a void for vagueness attack, the defendant must show that the statute is unconstitutional as applied specifically to the facts at hand.[78] This case-by-case method of attack, however, is not consistent and invites a risk of irregularity among the federal courts. On the other hand, a statute may be deemed overbroad and, thus, facially unconstitutional, only if the First Amendment is implicated.[79] Cases that do not implicate the First Amendment may be challenged for ambiguity, but it must be done on a case-by-case basis by employing the void for vagueness doctrine.[80]

In the present case, the district court rejected Hsu's claim that the EEA is overbroad because there are no First Amendment implications.[81] Hsu tried to use the Bristol-Myers employee who was in on the sting operation to show that there was a First Amendment issue.[82] He argued that the employee had a First Amendment right to communicate whatever he wanted, to whomever he wanted.[83] The district court flatly rejected this argument because Hsu did not have standing to raise a First Amendment claim on behalf of another.[84] Furthermore, had this not been a sting operation, the employee would not have been free to communicate such information to Hsu because it is illegal to do so under section 1832(a) of the EEA.[85]

The void for vagueness doctrine determines to what extent the administration of our laws "make[] possible the deprivation sub silentio of

---

[76] *Hsu*, 40 F. Supp.2d at 627.

[77] *See id.* at 626-27.

[78] *Id.*; *see also* United States v. Mazurie, 419 U.S. 544, 550 (1975).

[79] *Hsu*, 40 F. Supp.2d at 627; *see also Mazurie*, 419 U.S. at 550.

[80] RONALD D. ROTUNDA & JOHN E. NOWAK, TREATISE ON CONSTITUTIONAL LAW: SUBSTANCE AND PROCEDURE § 20.9 (2d ed. 1992). "The void for vagueness doctrine applies to all criminal laws, not merely those that regulate speech or other fundamental constitutional rights." *Id.*

[81] *Hsu*, 40 F. Supp.2d at 627-28.

[82] *Id.*

[83] *Id.*

[84] *Id.*

[85] *See* 18 U.S.C. § 1832(a) (1996).

the rights of particular citizens . . . ."[86] When the doctrine is invoked, a court must weigh the interests affected and the underlying purpose of the statute against the potential deprivation that could result if the statute is applied.[87] The required definiteness in statutes varies depending upon the rights and sanctions involved; thus, it follows that more precision is required where either the First Amendment is implicated or, as in this case, where criminal penalties may result.[88] The defendant challenging the statute bears the burden of proving that the statute is vague and the proof offered must be sufficient to "overcome the strong presumption of constitutionality" that is normally given to congressional enactments.[89] While this may be an uphill battle, a defendant will successfully meet his or her burden if it can be shown that, as applied to that particular defendant, the statute would leave a reasonable person guessing as to what is proscribed by the statute, or if application of the statute would lead to discriminatory and arbitrary prosecution.[90]

The *Hsu* court concluded that the defendant knew, or at a minimum believed, that he was in the process of stealing trade secrets.[91] The defendant and one of his co-conspirators were told on several occasions that there was no way to get the information they sought through legal channels, at which time, the defendant allegedly inquired into the possibility of paying a corrupt employee for the information.[92] Evidence such as e-mails, telephone conversations, and taped in-person meetings all tend to prove that the defendant was well aware of the nature of his conduct.[93] In fact, in many of these conversations, the defendant was "unambiguously told" that his venture was illegal.[94] Therefore, because Hsu is charged with inchoate offenses, conspiracy and attempted theft, and he believed that he was about to steal valuable trade secrets, the EEA is not vague as applied to the defendant.

---

[86] Anthony G. Amsterdam, *The Void-for-Vagueness Doctrine in the Supreme Court*, 109 U. PA. L. REV. 67, 81 (1960).

[87] NORMAN J. SINGER, SUTHERLAND STATUTORY CONSTRUCTION § 21.16 (5th ed. 1992).

[88] *Id.*

[89] *Id.*

[90] *See* PERKINS & BOYCE, *supra* note 67, ch. 1, § 1(C) n.12.

[91] United States v. Hsu, 40 F. Supp.2d 623, 630-31 (E.D. Pa. 1999).

[92] United States v. Hsu, 155 F.3d 189, 192 (3d Cir. 1998).

[93] *Hsu*, 40 F. Supp.2d at 630-31.

[94] *Id.* at 631.

B. Given Different Facts, the EEA May Not Withstand Constitutional Attack

Because the defendant in *Hsu* knew, or at a minimum believed, that he was stealing trade secrets,[95] his indictment is well-founded; however, under different circumstances, the EEA is vulnerable to the vagueness attack. In *Hsu,* it is clear that the defendant was breaking the law, therefore, the language of the EEA was not really tested for constitutional infractions. But where a defendant's conduct is not clearly illegal, the language of the EEA will be more closely scrutinized. Congress faced a difficult task when it sought to define an inherently vague term such as "trade secret"[96] because it needed to protect traditional proprietary business information while accommodating "the new technological methods" involved with trade secrets.[97] The definition provided in the statute includes words that are vague, and although Congress is not required to draft a perfect statute, the statute as drafted is cause for concern. Specifically, phrases such as "related to," "reasonable measures," "generally known," and "not being readily ascertainable" cause alarm.

1. "Related to" a Trade Secret

In *Hsu,* the relationship in question was between the first and second generation of a drug.[98] Even a person who is completely ignorant about biotechnology can ascertain that these two technologies are related. Because Hsu engaged in a detailed discussion of Taxol technology,[99] it is unlikely that he was unaware of an association between the first and second

---

[95] *Id.* at 630-31.

[96] The EEA defines "trade secret" as:

> 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) (1996).

[97] Spencer Simon, *The Economic Espionage Act of 1996,* 13 BERKELEY TECH. L.J. 305, 311 (1998).

[98] *Hsu,* 40 F. Supp.2d at 627.

[99] United States v. Hsu, 155 F.3d 189, 193 (3d Cir. 1998).

generations. Thus, in this case, it was not unreasonable to hold Hsu responsible for knowing that the two generations of the technology were related. There may, however, be more uncertainty about the relationship of two pieces of information where the information is not so clearly related. For example, the identities of the engineers or researchers may constitute a trade secret if the owner of the secret has taken "reasonable measures" to keep their identities secret and if there is independent economic value in keeping them secret.[100] The EEA does not indicate how closely related information must be to the trade secret to constitute a violation of the statute.[101] Phrases such as "related to" require courts to subjectively determine the meanings of such phrases.[102] This methodology is problematic because there is no way for a company trying to gain a legitimate competitive advantage to evaluate whether they are engaging in illegal conduct.[103] Fearing amenability to the EEA, companies may shy away from acting in ways that are perfectly legal.[104]

2. "Reasonable Measures"

Secondly, the EEA requirement that a trade secret owner take "reasonable measures" to keep the information secret creates concern.[105] This phrase exudes vagueness because there could be many standards for determining what is a "reasonable measure." The statute simply does not indicate to courts whether the measures taken to keep information secret should be guided by standards of the scientific community, the judicial community, or the public. The determinations as to what is a "reasonable measure" will vary greatly from case to case and the line between reasonable measures and unreasonable measures will become further blurred.

Would a company be taking "reasonable measures" to keep information secret if it put the information in sealed package marked

---

[100] 18 U.S.C. § 1839(3) (1996).

[101] The EEA simply prohibits anyone "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." from appropriating such trade secret. 18 U.S.C. § 1832(a) (1996).

[102] *See* Amsterdam, *supra* note 86, at 93.

[103] *See id.* at 80.

[104] *See id.*

[105] The definition of "trade secret" dictates that in order for a trade secret to be protected, the "owner thereof [must have] taken reasonable measures to keep such information secret." 18 U.S.C. § 1839(3)(A) (1996).

"CONFIDENTIAL" and put the package in an executive officer's filing cabinet or desk drawer? This might be deemed reasonable by one court, but another court might require that the cabinet or desk drawer be locked. Another court might go further and require that for the attempt at secrecy to be reasonable, the company would not be able to let more than two people know of the location of the confidential information. On the other hand, it may simply be enough to have the information in a file folder stamped "CONFIDENTIAL." Again, language such as "reasonable measures" begs for ad hoc application that, although has been acceptable in the civil context for years, leaves an unjust amount of uncertainty in the criminal context. Although words and phrases of "inherent discontrol,"[106] such as "reasonable," do not automatically make a statute vague, use of such language increases the risk of continuing irregularity regarding the application of the statute, not to mention the risk of forum shopping.[107]

3. "Generally Known" and "Not Being Readily Ascertainable"

The *Hsu* court struggled with "generally known" and "not being readily ascertainable" for two reasons. First, what is known and available to the public continuously changes.[108] Second, four biotechnical experts examined the documents used in the sting operation to determine if the information constituted trade secrets, and each of the four disagreed about the public availability of the information in the documents.[109] After the sting operation concluded, two Bristol-Myers scientists reviewed the documents that were used in the sting for the purpose of redacting all confidential information.[110] Between the two, there was disagreement as to whether some of the information was trade secrets or public information.[111] A third scientist from Bristol-Myers examined the documents and concluded that over one hundred pages that were redacted as trade secrets by the other two scientists were actually public information and should be

---

[106] Amsterdam, *supra* note 86, at 93. Phrases of "inherent discontrol" lack predictability and uniformity and can lead to a vast disparity in caselaw between district courts. This is the opposite effect intended by uniform laws such as the EEA.

[107] *Id.* If there is no uniformity in the way district courts apply a statute, a party to a suit may be more likely to shop around for a forum that agrees with that party's position. Like disparity in case law between district courts, the practice of forum shopping also has the opposite effect intended by a uniform law such as the EEA.

[108] United States v. Hsu, 40 F. Supp.2d 623, 630 (E.D. Pa. 1999).

[109] *Id.* at 629.

[110] *Id.*

[111] *Id.*

unredacted.[112] In light of these disagreements, the district court employed, at the urging of the Third Circuit, a fourth scientist who found that yet another ten pages should be unredacted.[113] All four scientists were considered to be experts in the field, yet they could not agree on the status of the documents.[114]

While the status of the documents used in the sting is irrelevant to the defendant's indictment,[115] the issue is that there is a requirement that penal statutes be drafted so as to give notice of the conduct that is proscribed and to do so in a way that is understandable by people of ordinary intelligence.[116] But how can people of ordinary intelligence be charged with the task of determining whether, say, technological information is "generally known" or "readily ascertainable" by the public if experts cannot agree on it? In an environment where the flow of information is constantly growing, what is "generally known" is never really certain.[117]

Furthermore, the scope of what is "generally known" or "readily ascertainable" depends upon how "public" is defined. The EEA could be referring to the general scientific public, the scientific public in a particular field, the academic public, or even the general public.[118] Under the statute as it is currently drafted, it is impossible to know who the "public" is because the EEA lacks clarity and the legislative history is silent. The *Hsu* court was able to dodge this textual ambiguity because the defendant was aware that Bristol-Myers sought to keep the information secret from all members of the public, regardless of the genre.

C. Void for Vagueness and Choate Crimes

There are situations when the statute might be vulnerable to a void for vagueness challenge. The EEA prohibits attempts of theft as well as thefts that have been carried out.[119] Because only the former was at issue in

---

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.* The district court agreed with the government that the defendant's culpability only depends "on the circumstances as the defendant *believes* them to be and not as they really are." *Id.* (citing United States v. Hsu, 155 F.3d 189, 203-04 (3d Cir. 1998)). For this reason, it is irrelevant whether trade secret information versus "dummy" information was used in the sting operation.

[116] *See* ROTUNDA & NOWAK, *supra* note 80, § 20.9.

[117] *Hsu*, 40 F. Supp.2d at 630.

[118] *Id.*

[119] 18 U.S.C. § 1832 (1996).

Hsu,[120] it is of particular concern how the statute will play out when a defendant is charged with the completed crime of theft under the EEA. In its decision, the *Hsu* court points out that because the defendant "is charged *only* with the inchoate offenses of attempt and conspiracy (rather than completed offenses), we put aside our considerable disquiet about the EEA's language . . . ."[121]

1. Void for Vagueness and Hypothetical Situations

In cases involving completed theft, courts will have to evaluate the language that the *Hsu* court put aside because a defendant's belief that he or she is committing a crime may not be enough to establish culpability. But until the EEA is tested in a case involving a completed theft, one can only speculate about the future constitutional status of the EEA. The following hypotheticals illustrate dilemmas that could confront courts in the future. Mr. X enlists the help of a disgruntled employee at Acme Company to assist him in stealing Acme's secret formula for its popular beverage. Mr. X agrees to pay the employee two hundred thousand dollars for any information about Acme's trade secret. The employee sells information to Mr. X disclosing that Acme obtains one of the ingredients for the formula from a large manufacturer in Switzerland. Mr. X is arrested for stealing a trade secret on the grounds that this information is closely "related to" the formula. But is it? There are no guidelines or standards to help courts determine how remote information can be and yet still be classified as "related to" the economic advancement of the company.

Further, assume that Acme created and sold a variation of its beverage, but later stopped producing it. The formula for the discontinued beverage was boxed up, labeled and sent to Acme's warehouse for storage. Acme hired an independent cleaning service to keep the warehouse clean and organized. One of the cleaning persons finds the formula and sells it to a competitor. Assuming that the discontinued formula was based in large part on the existing formula, the fact that persons other than employees of Acme had consistent access to the information could mean that the trade secret was "readily ascertainable." Similarly, it is unclear from the text of the EEA how many members of the public must *know* the information before it can be said that the information is "generally known" by the

---

[120] *Hsu*, 40 F. Supp.2d at 631.

[121] *Id.*

public. In the preceding hypothetical, if one or two cleaning persons gain knowledge of the information, plausible arguments could be made both for and against the information being "generally known." Again, Congress gave no guidance to help courts that may face a similar issue.

2. Overbreadth and a Hypothetical Situation

The *Hsu* Court correctly found that the facts of the case presented no First Amendment issues, which precluded the defendant from arguing that the EEA is generally overbroad.[122] However, there may be instances when the First Amendment is implicated by the EEA. Reconsider the example of Acme storing its old formula in a warehouse. Suppose a reporter, doing an article on carcinogens in beverages, approaches one of the cleaning persons and explains that he has received a tip from a reliable source that Acme is knowingly using carcinogens in its beverages. Knowing that he can perform a great service for the public if he obtains any variation of the formula and confirms that Acme's beverages cause cancer, the reporter offers to pay the cleaning person to find the information. If the reporter is arrested for stealing a trade secret under the EEA, he may have a plausible First Amendment argument. In this case, the EEA would be challenged, not as it applied to the reporter, but as a facially unconstitutional statute.[123] A determination of the EEA as overbroad would void the statute and require Congress to address the issue.

D. How the EEA Could Be Adapted to Prevent Constitutional Challenges

While Congress has the extremely difficult task of drafting statutes that will offer sufficient protection, it must at the same time draft statutes no more broadly than necessary. An examination of specific portions of the EEA reveals that there is much room for improvement in the statute's construction. Section 1839(3) of the EEA defines "trade secret" as all forms of business information that an owner has taken "reasonable measures" to keep secret, so long as it has value by not being "generally

---

[122] *Id.* at 627.

[123] *See supra* note 79 and accompanying text. It could not be denied that a reporter writing an article implicates the First Amendment, therefore the reporter could make an overbreadth argument, as opposed to relying on the void for vagueness doctrine.

known" to or "readily ascertainable" by the public.[124] It lists the types of information that are deemed "trade secrets," and although the list is not exhaustive, it gives guidance as to what types of information are protected.[125]

The EEA's definition of "trade secret" demonstrates a congressional attempt to aid courts in the interpretation of the statute, however, the definition falls short of providing adequate guidance. It merely states that "reasonable measures" must be taken to keep the information secret.[126] Congress could have given more meaning to the phrase had it also given a non-exhaustive list of what types of measures are considered reasonable. For example, the statute could have specified that "reasonable measures" includes securing the information in a locked area or limiting the number of people having access to the information. This would give guidance to interpreting the "reasonable measures" provision of the EEA because courts could compare the measures taken by the owner of the trade secrets to the kinds of measures indicated in the statute to see if the measures taken were sufficient.

Similarly, Congress could have included a brief explanation of how information is "readily ascertainable" by the public. The only clarification given is that, in order to be protected, the information cannot be available to the public "through proper means."[127] "Proper means" could refer to means that are legal, but it could also imply that one should not employ means that are unethical; the EEA is not clear. This illustrates that Congress' attempt to give clarification to the EEA resulted in further confusion.

IV. CONCLUSION

The Eastern District of Pennsylvania's decision in *United States v. Hsu*, although only determinative of the defendant's motion to dismiss, is important for future prosecutions under the EEA. The EEA may not prove to be problematic when a defendant is prosecuted for an inchoate offense, such as attempt or conspiracy, however, completed offenses may raise constitutional issues because it will be necessary for the court to confront

---

[124] 18 U.S.C. § 1839(3) (1996).

[125] *Id.*

[126] *Id.*

[127] *Id.* § 1839(3)(B). For trade secrets to be protected, it is necessary that "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." *Id.*

the language of the EEA. The *Hsu* court was able to dodge explicit terms in the statute because the defendant's conduct combined with his mental state was sufficient to sustain an indictment.

The definition of "trade secret," as defined by the EEA, creates constitutional problems because it fails to give adequate notice as to what is proscribed by the statute. The difficulty in determining the meaning of such phrases as "related to," "reasonable measures," "generally known," and "readily ascertainable" give little guidance of the legislative intent behind the EEA and may cause otherwise law-abiding citizens to engage in illegal conduct. Thus, for the reasons detailed in this Note, the EEA may be void for vagueness and fall prey to constitutional challenges in future cases.