# Your Secrets Are Safe With Us: How Prosecutors Protect Trade Secrets During Investigation and Prosecution

Brian L. Levine<sup>†</sup> Timothy C. Flowers<sup>††</sup>

Abstract

This Article explores the tools that prosecutors use to protect trade secrets during the investigation and the prosecution of a trade secret theft. Among other things, the authors discuss the Department of Justice's use of protective orders, interlocutory appeals, and alternative charges to protect a victim's trade secret information.

### Introduction

Protecting trade secrets has historically been the province of state civil law. In 1996, however, Congress recognized that the theft of trade secrets represented a major threat to the United States economy and that enforcement through state civil actions was often insufficient to deter the most egregious trade secret thefts.<sup>1</sup> The potential for a civil action, for example, might provide little deterrence to a departing employee planning to use the trade secret abroad or to an individual who is effectively judgment proof. Thus, Congress passed the Economic Espionage Act (EEA) to enable the Department of Justice to investigate and criminally prosecute serious instances of trade secret theft.<sup>2</sup>

<sup>&</sup>lt;sup>†</sup> B.A. (1998), University of Pennsylvania; J.D. (2001), New York University School of Law. Brian L. Levine serves as a prosecutor in the Computer Crime and Intellectual Property Section of the United States Department of Justice.

<sup>&</sup>lt;sup>††</sup> B.A. (2006), Wabash College; J.D. (2011), Indiana University's Maurer School of Law. Timothy Flowers serves as a prosecutor in the Computer Crime and Intellectual Property Section of the United States Department of Justice.

This Article reflects the views of the authors only and does not necessarily reflect the views of the United States Department of Justice. The authors would like to thank Christopher S. Merriam and Kendra Ervin for their support and editorial assistance.

<sup>&</sup>lt;sup>1</sup> Economic Espionage Act, 18 U.S.C. §§ 1831-1839 (2012).

<sup>&</sup>lt;sup>2</sup> See United States v. Yang, 281 F.3d 534, 543 (6th Cir. 2002), cert. denied, 537 U.S. 1170 (2003); United States v. Hsu, 155 F.3d 189, 195 (1998).

Since 1996, the threat of trade secret theft has grown considerably.<sup>3</sup> An increasingly global and digitally connected economy has generated numerous opportunities for insiders, hackers, and nation states to become significant threats to United States companies and to the United States economy. For example, in United States v. Liew,<sup>4</sup> executives from a government-controlled Chinese corporation conspired with DuPont insiders to steal secrets related to titanium dioxide, which threatened DuPont's stake in a \$12 billion market.<sup>5</sup> After a two-month jury trial, Walter Liew, the defendant and a former DuPont insider, was convicted and sentenced to fifteen years in prison.<sup>6</sup> In another case, the government reached a \$360 million settlement with employees and executives of Kolon Industries, a South Korean company charged with working with company insiders to steal Kevlar technology valued at hundreds of millions.<sup>7</sup> Recently, the government also accepted guilty pleas from several individuals who hacked into corporate systems and stole trade secrets related to video games and flight simulation software used to train combat helicopter pilots and valued in the nine figure range.<sup>8</sup>

<sup>6</sup> Press Release, Dep't of Justice, Walter Liew Sentenced to Fifteen Years in Prison For Economic Espionage (July 11, 2014), *available at* http://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage.

<sup>7</sup> Press Release, Dep't of Justice, Kolon Industries Inc. Pleads Guilty for Conspiring to Steal DuPont Trade Secrets Involving Kevlar Technology (Apr. 30, 2015), *available at* http://www.justice.gov/opa/pr/kolon-industries-inc-pleads-guilty-conspiring-steal-dupont-trade-secrets-involving-kevlar.

<sup>8</sup> Press Release, Dep't of Justice, Third Member of International Computer Hacking Ring Pleads Guilty to Hacking and Intellectual Property Theft Conspiracy (Jan. 20, 2015), *available at* http://www.justice.gov/opa/pr/third-member-internationalcomputer-hacking-ring-pleads-guilty-hacking-and-intellectual.

<sup>&</sup>lt;sup>3</sup> Combating Economic Espionage and Trade Secret Theft, Hearing Before the S. Judiciary Comm., Subcomm. on Crime and Terrorism, 113 Cong. (2014) (statement of Randall C. Coleman, Assistant Dir., Counterintelligence Div. FBI), http://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft.

<sup>&</sup>lt;sup>4</sup> No. CR-11-00573-1, 4 JSW, 2014 WL 2586329, at \*2 (N.D. Cal. Jun. 9, 2014).

<sup>&</sup>lt;sup>5</sup> Press Release, Dep't of Justice, Two Individuals and Company Found Guilty of Conspiracy to Sell Trade Secrets to Chinese Companies (Mar. 5, 2014), *available at* http://www.justice.gov/usao-ndca/pr/two-individuals-and-company-found-guilty-conspiracy-sell-trade-secrets-chinese; Press Release, Dep't of Justice, U.S. and Chinese Defendants Charged with Econ. Espionage and Theft of Trade Secrets in Connection with Conspiracy to Sell Trade Secrets to Chinese Companies (Feb. 8, 2012), *available at* http://www.justice.gov/opa/pr/us-and-chinese-defendants-charged-economic-espionage-and-theft-trade-secrets-connection.

Preventing and deterring trade secret theft through criminal prosecution is more important than ever. When the Federal Bureau of Investigation (FBI) has been timely alerted to the possibility of a contemporaneous trade secret theft, the FBI has been able to use search warrants, undercover investigations, and other legal tools to prevent trade secrets from leaving the country or even from leaving the company. Even if a trade secret theft is discovered after the fact, the Department of Justice has been able to help victim companies mitigate loss, limit unauthorized use of the trade secret, and deter future thefts.

Despite the potential advantages of federal prosecution, some victims of trade secret theft have been reluctant to involve the Justice Department when investigating suspected thefts. Among other reasons, victims have expressed concern that inviting a criminal investigation and prosecution will increase the likelihood of the trade secret becoming publicly revealed during investigation or at trial.<sup>9</sup> Although understandable, this concern is unfounded. In the almost twenty years since the passage of the Economic Espionage Act, there have been hundreds of federal trade secret theft investigations and prosecutions.<sup>10</sup> Despite these numbers, it does not appear that a federal trade secret being publicly disclosed.

This Article explores the tools prosecutors use to protect trade secrets during the investigation and prosecution of a trade secret theft. First, this Article examines five tools prosecutors use to ensure that courts enter bullet-proof "protective orders" (essentially confidentiality agreements with the force of a court order) to protect trade secrets during a criminal prosecution. These tools include: (1) Federal Rule of Criminal Procedure 16; (2) 18 U.S.C. § 1835; (3) the availability of an automatic interlocutory

<sup>&</sup>lt;sup>9</sup> H.R. Rep. No. 104-788, at 13 (1996), as reprinted in 1996 U.S.C.C.A.N. 4021, 4032; CHARLES DOYLE, CONG. RESEARCH SERV., R42681, STEALING TRADE SECRETS AND ECONOMIC ESPIONAGE: AN OVERVIEW OF 18 U.S.C. 1831 AND 1832 11 (July 25, 2014), available at https://fas.org/sgp/crs/secrecy/R42681.pdf; see also Robert M. Isackson, To Prosecute or Not to Prosecute? Limiting Exposure of Trade Secrets During Criminal Prosecutions, TRADE SECRETS WATCH BLOG (Feb. 21, 2014), http://blogs.orrick.com/trade-secrets-watch/2014/02/21/to-prosecute-or-not-toprosecute-limiting-exposure-of-trade-secrets-during-criminal-prosecutions.

<sup>&</sup>lt;sup>10</sup> See EXEC. OFFICE OF THE PRESIDENT OF THE UNITED STATES, ADMIN. STRATEGY ON MITIGATING THE THEFT OF U.S. TRADE SECRETS (2013), available at https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin\_strategy\_on\_mitigating\_the\_theft\_of\_u.s.\_trade\_secrets.pdf.

appeal; (4) a writ of mandamus; and (5) the use of alternative charges. Second, this Article discusses how the Department of Justice uses protective orders at every stage of the investigation and prosecution to zealously guard a victim's trade secret information. A prosecutor will often enter into three separate protective orders during a prosecution: (a) a pre-indictment protective order; (b) a pre-trial protective order; and (c) a trial protective order. Each of these protective orders contains powerful provisions designed to keep trade secrets safe.

Federal prosecutors recognize that, if victims are (or even feel) revictimized as a result of an investigation or prosecution, they will not cooperate in future prosecutions, and the criminals will win. Thus, prosecutors recognize that protecting trade secrets throughout the litigation process is paramount. The impressive history of trade secret prosecutions under the Economic Espionage Act demonstrates prosecutors will vigorously protect a victim's trade secrets, and Congress and the courts will do what they can to support them at every stage.

## I. Means to Ensure That Courts Enter Appropriate Protective Orders

## A. Introduction to Trade Secrets

As characterized in the civil context,

[a] trade secret is really just a piece of information (such as a customer list, or a method of production, or a secret formula for a soft drink) that [a company] tries to keep secret by executing confidentiality agreements with employees and others and by hiding the information from outsiders by means of fences, safes, encryption, and other means of concealment, so that the only way the secret can be unmasked is by a breach of contract or a tort.<sup>11</sup>

Not all commercial or business information is trade secret material.<sup>12</sup> According to the EEA, information becomes a trade secret if a company

<sup>&</sup>lt;sup>11</sup> ConFold Pac., Inc. v. Polaris Indus., 433 F.3d 952, 959 (7th Cir. 2006) (citing Learning Curve Toys, Inc. v. PlayWood Toys Inc., 342 F.3d 714, 721-23 (7th Cir. 2003)).

<sup>&</sup>lt;sup>12</sup> United States v. Howley, 707 F.3d 575, 579 (6th Cir. 2013) ("Not all business knowledge is a trade secret.").

takes "reasonable measures" to ensure the information's secrecy and "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."<sup>13</sup>

Congress expressly criminalized the theft of trade secrets with the passage of the EEA in 1996, which occurred "against a backdrop of increasing threats to corporate security and a rising tide of international and domestic economic espionage."<sup>14</sup> In confronting these rising threats, Congress intended the EEA "to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets."<sup>15</sup>

The EEA criminalizes two principal types of corporate espionage.<sup>16</sup> The "economic espionage" provision in 18 U.S.C. § 1831 punishes whoever knowingly misappropriates, or attempts or conspires to misappropriate, trade secrets with the intent or knowledge "that the offense will benefit any foreign government, foreign instrumentality, or foreign agent."<sup>17</sup> By contrast, § 1832 criminalizes economically motivated trade secret thefts and applies to anyone who knowingly engages in the theft of trade secrets, or who attempts or conspires to do so "with the 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."<sup>18</sup> In addition, the trade secret theft must be to the economic benefit of anyone other than the secret's owner, and the accused must intend or know "that the offense will injure any owner of that trade secret."<sup>19</sup> These provisions capture a wide range of criminal activities, and EEA prosecutions in a variety of cases demonstrate that "[t]rade secrets are an integral part of virtually every sector of our economy and are essential to maintaining the health and competitiveness of critical industries operating in the United States."<sup>20</sup>

<sup>&</sup>lt;sup>13</sup> 18 U.S.C. § 1839(3) (2012).

<sup>&</sup>lt;sup>14</sup> United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998).

<sup>&</sup>lt;sup>15</sup> United States v. Yang, 281 F.3d 534, 543 (6th Cir. 2002), *cert. denied*, 537 U.S. 1170 (2003).

<sup>&</sup>lt;sup>16</sup> *Hsu*, 155 F.3d at 195.

<sup>&</sup>lt;sup>17</sup> 18 U.S.C. § 1831 (2012).

<sup>&</sup>lt;sup>18</sup> Id. § 1832.

<sup>&</sup>lt;sup>19</sup> Id.

<sup>&</sup>lt;sup>20</sup> Presidential Statement on the Signing of the Econ. Espionage Act of 1996, 2 PUB. PAPERS 1814 (Oct. 11, 1996), *available at* http://www.gpo.gov/fdsys/pkg/PPP-1996-book2/pdf/PPP-1996-book2-doc-pg1814.pdf.

#### **B.** Introduction to Protective Orders

The need to protect confidential and business information during litigation is not unique to theft of trade secrets cases, nor to criminal prosecution in general. Perhaps the most common mechanism for protecting confidential information during the course of any litigation, civil or criminal, is the protective order. In this context, a protective order is essentially a confidentiality agreement focused on issues likely to arise in litigation and given the force of a court order once entered by the court.<sup>21</sup>

The affected parties (often counsel for the plaintiff and the defendant in a civil case) will generally negotiate the terms of a protective order and present the court with a proposed stipulated order to which all parties agree. To the extent the parties cannot agree upon certain provisions, they often present their respective positions to the court, and the court will resolve any disputed issues. In so doing, courts will try to balance the important need to protect confidential information with the realities of litigation.<sup>22</sup>

## C. Rule 16 of the Federal Rules of Criminal Procedure

Rule 16 of the Federal Rules of Criminal Procedure provides that a court may, at any time, "for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."<sup>23</sup> Rule 16 permits parties to make the required "good cause" showing on an ex parte basis and under seal.<sup>24</sup> "Rule 16(d) applies generally in all criminal cases,"<sup>25</sup> and

<sup>&</sup>lt;sup>21</sup> See DOYLE, supra note 9, at 23; see also Gillard v. Boulder Valley Sch. Dist. Re-2, 196 F.R.D. 382, 385 (D. Colo. 2000) (noting that protective orders are "utilized to limit the discovery or dissemination of confidential or private information"); BLACK'S LAW DICTIONARY (10th ed. 2014) (defining a protective order as "[a] court order prohibiting or restricting a party from engaging in conduct (esp. a legal procedure such as discovery) that unduly annoys or burdens the opposing party or a third-party witness").

<sup>&</sup>lt;sup>22</sup> See United States v. Hsu, 155 F.3d 198, 197 (3d Cir. 1998).

<sup>&</sup>lt;sup>23</sup> FED. R. CRIM. P. 16(d)(1).

<sup>&</sup>lt;sup>24</sup> Id.

<sup>&</sup>lt;sup>25</sup> UNITED STATES DEP'T OF JUST., PROSECUTING INTELLECTUAL PROPERTY CRIMES 207 (4th ed. 2013) [hereinafter PROSECUTING INTELLECTUAL PROPERTY CRIMES].

it is often cited in EEA cases as an alternative basis for authorizing a protective order.<sup>26</sup>

Rule 16(d) is an important tool in criminal litigation. Applicable in all types of criminal cases and in a myriad of other situations, the rule was drafted to be flexible and to provide the court with discretion.<sup>27</sup> District courts are generally familiar with the provision, and a relatively robust body of case law interpreting the provision exists. Rule 16(d), however, has certain limitations. First, because the rule is discretionary, it contains no statutory requirement that a court enter a protective order in any given circumstance.<sup>28</sup> Second, if the district court does not enter a protective order pursuant to Rule 16(d), there may be limitations on a prosecutor's ability to appeal the decision on an interlocutory basis.<sup>29</sup> Despite these limitations, victims and their lawyers have found the civil analogs to Rule 16 sufficient to protect trade secret information while litigating scores of trade secret cases annually.

#### D. 18 U.S.C. § 1835

In enacting 18 U.S.C. § 1835, Congress recognized Rule 16 may, in some circumstances, be insufficient to give victims confidence that their trade secrets will be fully protected during prosecution. Thus, Congress enacted § 1835, which provided that district courts "shall enter such orders and take such other action as may be necessary and appropriate

<sup>&</sup>lt;sup>26</sup> See, e.g., Hsu, 155 F.3d at 193 (noting "the government filed a motion pursuant to 18 U.S.C. § 1835 and FED. R. CRIM. P. 16(d)(1) for a protective order to prevent the disclosure of the Bristol-Myers trade secrets allegedly contained in those documents").

 $<sup>^{27}</sup>$  FED. R. CRIM. P. 16(d)(1) advisory committee notes ("The entire matter is left within the discretion of the court.").

<sup>&</sup>lt;sup>28</sup> See, e.g., In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 93, 122 (2d Cir. 2008) (explaining that Rule 16(d) grants district courts the discretion to establish conditions "under which the defense may obtain access to discoverable information"), cert. denied, 558 U.S. 1137 (2010); see also United States v. Delia, 944 F.2d 1010, 1018 (2d Cir. 1991) (noting that, because the language of Rule 16(d)(1) "is . . . permissive," the district court may "limit or otherwise regulate discovery had pursuant to the Rule").

<sup>&</sup>lt;sup>29</sup> Compare FED. R. CRIM. P. 16(d) (allowing courts to "deny, restrict or defer discovery or inspection, or grant other appropriate relief"), with 18 U.S.C. § 1835 (providing for interlocutory appeal of an order requiring disclosure of trade secret materials).

to preserve the confidentiality of trade secrets."<sup>30</sup> Unlike Rule 16, which generally makes entering protective orders discretionary, § 1835's use of the word "shall," makes entering protective orders to protect trade secrets mandatory.<sup>31</sup> Indeed, courts have interpreted Congress's use of "shall" as a "clear indication . . . that trade secrets are to be protected to the fullest extent during EEA litigation."<sup>32</sup>

Section 1835 further provides, "An interlocutory appeal by the United States shall lie from a decision or order of a district court authorizing or directing the disclosure of any trade secret."<sup>33</sup> Thus, if a district court declines to enter a requested protective order, a prosecutor may immediately appeal that decision to the federal circuit court.<sup>34</sup> Congress created the interlocutory-appeal provision as a specialized tool to ensure that a district court hearing an EEA case will "enter such orders as may be necessary to protect the confidentiality of the information in the case."<sup>35</sup>

Congress's strong language in enacting § 1835 should reinforce to victims that federal criminal courts will take appropriate measures to protect sensitive information. In fact, Congress crafted § 1835 specifically to address companies' reluctance "to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth."<sup>36</sup> If, for the purpose of entering a protective order, a court "always assume[s] that the material at issue is in fact a trade secret"<sup>37</sup> and takes corresponding measures to protect that information, then victims will be more likely to cooperate with law enforcement to capture offenders and deter similar conduct in the future.

Although the universe of cases interpreting § 1835 is limited, this dearth of authority may be due in large part to the government's success

<sup>34</sup> Id.

<sup>35</sup> H.R. Rep. No. 104-788, at 16 (1996), *as reprinted in* 1996 U.S.C.C.A.N. 4021, 4022.

<sup>36</sup> *Id.* at 4032.

<sup>37</sup> 142 Cong. Rec. S12, 213 (daily ed. Oct. 2, 1996) (Manager's Statement).

<sup>&</sup>lt;sup>30</sup> 18 U.S.C. § 1835 (2012).

 $<sup>^{31}</sup>$  Id.

<sup>&</sup>lt;sup>32</sup> *Hsu*, 155 F.3d at 197.

<sup>&</sup>lt;sup>33</sup> 18 U.S.C. § 1835 (2012).

in seeking § 1835 protective orders. In the cases interpreting § 1835, the message is clear: the statute "is designed to protect proprietary economic information and commercial trade secrets."<sup>38</sup> If, during the course of litigation, companies are required to publicly disclose the very material they want to safeguard, then § 1835 would be undermined. The Department of Justice's vigorous prosecution of trade secret theft and protection of the underlying trade secret information prevents this scenario from occurring.

## E. Interlocutory Appeal

As noted above, § 1835 allows the government to file "[a]n interlocutory appeal . . . from a decision or order of a district court authorizing or directing the disclosure of any trade secret."<sup>39</sup> Although the provision is rarely invoked, it permits "prompt judicial review of a district court decision provides an essential added layer of protection against the disclosure of trade secrets."<sup>40</sup>

*United States v. Hsu* demonstrates the interlocutory-appeal provision in action.<sup>41</sup> Shortly after the EEA was enacted in 1996, an FBI sting operation arrested three members of a Taiwanese company and charged them with conspiring to steal from Bristol-Myers Squib "the processes, methods, and formulas for manufacturing Taxol, an anti-cancer drug produced . . . and regarded by the company as a highly valuable trade secret."<sup>42</sup> An FBI agent, posing as a technology broker, communicated repeatedly with one of the defendants about obtaining manufacturing and distribution techniques related to Taxol.<sup>43</sup> These clandestine communications resulted in a face-to-face encounter, during which the undercover FBI agent, still posing as a technology broker, warned another eventual

<sup>&</sup>lt;sup>38</sup> United States v. Roberts, No. 3:08-CR-175, 2010 WL 1010000, at \*6 (E.D. Tenn. Mar. 17, 2010) (issuing a § 1835 protective order to seal seven photographs containing trade secret material).

<sup>&</sup>lt;sup>39</sup> 18 U.S.C. § 1835.

<sup>&</sup>lt;sup>40</sup> PROSECUTING INTELLECTUAL PROPERTY CRIMES, *supra* note 25, at 207.

<sup>&</sup>lt;sup>41</sup> 155 F.3d 189, 194 (3d Cir. 1998).

<sup>&</sup>lt;sup>42</sup> *Hsu*, 155 F.3d at 191-92.

<sup>&</sup>lt;sup>43</sup> *Id.* at 192.

defendant about Bristol-Myers's unwillingness to share its then-secret technology.<sup>44</sup> Despite the agent's warning, that defendant directed the agent to make deals with Bristol-Myers employees to obtain proprietary information related to Taxol without the company's authorization.<sup>45</sup>

Law enforcement continued to communicate with the defendants over the next fourteen months, discussing the transfer of trade secret information and negotiating prices.<sup>46</sup> One of the defendants reportedly offered an undercover FBI agent \$400,000 in cash, stock, and royalties for the disclosure of the Taxol secrets.<sup>47</sup> The defendants were ultimately arrested after a meeting in Philadelphia, during which they—along with an unidentified scientist—discussed the Taxol technology, reviewed Bristol-Myers documents labeled "CONFIDENTIAL," and discussed several aspects of Taxol production.<sup>48</sup> The defendants were charged with the attempted theft of trade secrets and conspiring to steal trade secrets, among other charges.<sup>49</sup>

Shortly thereafter, the defendants, arguing that "unique constitutional and procedural requirements . . . dictate[] full access to the documents shown to them during the investigation,"<sup>50</sup> sought an order directing the disclosure of Bristol-Myers's trade secrets, "but only to select members of the defense team."<sup>51</sup> By contrast, the Government filed a motion under § 1835 and Federal Rule of Criminal Procedure 16(d), seeking a protective order preventing disclosure of Bristol-Myers's trade secrets—namely, seeking a remedy in which the trial judge would conduct an *in camera* review of proposed redactions before finalizing exhibits for trial.<sup>52</sup> The Government also maintained that the defendants had no need to review the trade secrets at issue because the indictment charged only

<sup>44</sup> Id

<sup>45</sup> Id.

<sup>46</sup> Id.

- <sup>47</sup> Id.
- <sup>48</sup> *Id.* at 192-93.
- 49 *Id.* at 193.
- <sup>50</sup> Id.
- <sup>51</sup> Id.
- <sup>52</sup> Id.

the inchoate crimes of attempt and conspiracy.<sup>53</sup> The district court agreed with the defendants, but encouraged the Government—because of the novel and important questions of law at issue<sup>54</sup>—to pursue an interlocutory appeal, which the Government did.<sup>55</sup>

The Third Circuit reversed the district court and held that under the circumstances, the defendants had no need to access Bristol-Meyers's trade secrets.<sup>56</sup> The opinion contains strong language describing the scope and purposes of the EEA in general and Section 1835 in particular.<sup>57</sup> The court noted the "wide[] variety of technological and intangible information" covered under the EEA's definition of trade secrets.<sup>58</sup> The court also noted that "public policy require[s] protection" of the portions of documents at issue.<sup>59</sup> *Hsu* recognized that trade secrets "must not be generally known to, or readily ascertainable by, the general public."<sup>60</sup> Therefore, if trade secrets "are disclosed or revealed, they are destroyed."<sup>61</sup>

Because Rule 16 of the Federal Rules of Criminal Procedure "enable[] the defendants to obtain documents in the government's possession that

 $^{57}$  Id. at 196-201 (discussing the EEA's framework, congressional intent, and application to the defendants' theories of the case).

<sup>58</sup> *Id.* at 196 ("[T]he EEA protects a wider variety of technological and intangible information than current civil laws.").

<sup>59</sup> Id. at 205.

<sup>60</sup> Id. at 196.

<sup>&</sup>lt;sup>53</sup> *Hsu*, 155 F.3d at 193.

<sup>&</sup>lt;sup>54</sup> See United States v. Hsu, 982 F. Supp. 1022, 1022 n.1 (E.D. Pa. 1997), *rev'd*, 155 F.3d 189 (3d Cir. 1998) ("Inasmuch as this motion raises unsettled and important questions of law, we encourage the Government to seek further clarification of them from our Court of Appeals.").

<sup>&</sup>lt;sup>55</sup> Hsu, 982 F. Supp. at 1022 n.1.

<sup>&</sup>lt;sup>56</sup> Hsu, 155 F.3d at 204 ("[T]he Taxol trade secrets in the Bristol-Myers documents are not 'material' to the preparation of the defendants impossibility defense, because proof that the defendants sought to steal actual trade secrets is not an element of the crimes of attempt or conspiracy under the EEA.").

<sup>&</sup>lt;sup>61</sup> See In re Iowa Freedom of Info. Council, 724 F.2d 658, 662 (8th Cir. 1983) (stating that disclosed or revealed information destroys a trade secret); *accord Hsu*, 155 F.3d at 196 ("The EEA, however, indicates that a trade secret must not be generally known to, or readily ascertainable by, the general public, rather than simply those who can obtain economic value from the secret's disclosure or use.").

are material to the preparation of their defense, or are intended for use by the government as evidence in chief at trial,"<sup>62</sup> the court carefully fashioned a remedy.<sup>63</sup> It directed "the district court to conduct an *in camera* review to determine whether the documents have been properly redacted to exclude only confidential information and to assess whether what was redacted is 'material' to the defense."<sup>64</sup> The district court following *Hsu*'s strong language in favor of trade secret protections prohibited the defense from receiving un-redacted documents, and thus limited the universe of people with access to Bristol-Myers's trade secrets.<sup>65</sup>

*Hsu* is one of only two appellate decisions interpreting §  $1835.^{66}$ However, the limited use of § 1835's automatic interlocutory appeal provision suggests § 1835's effectiveness in safeguarding trade secrets. Indeed, § 1835's interlocutory appeal provision likely deters some defendants from pressing for disclosure where it is unnecessary and encourages district courts to err on the side of protecting trade secrets.

## F. Writ of Mandamus

Section 1835 has generally provided sufficient protection of a company's trade secrets during litigation. But even the courts that have narrowly interpreted § 1835's protections have protected trade secrets on alternative grounds.<sup>67</sup> In *United States v. Ye*,<sup>68</sup> the other appellate decision interpreting § 1835, the court declined interlocutory jurisdiction

<sup>62</sup> Hsu, 155 F.3d at 205.

<sup>&</sup>lt;sup>63</sup> *Id.* at 205-06.

<sup>&</sup>lt;sup>64</sup> *Id.* at 205.

<sup>&</sup>lt;sup>65</sup> United States v. Hsu, 185 F.R.D. 192, 198 (E.D. Pa. 1999) ("We reject Hsu's argument because we fail to see how the defense needs the precise formula and information contained in the redactions to raise an effective entrapment or outrageous government conduct defense.").

<sup>&</sup>lt;sup>66</sup> PROSECUTING INTELLECTUAL PROPERTY CRIMES, *supra* note 25, at 207 (noting that, since the EEA was passed in 1996, only *Hsu* and *United States v. Ye* have invoked the interlocutory-appeal provision).

<sup>&</sup>lt;sup>67</sup> See United States v. Ye, 436 F.3d 1117, 1121 (9th Cir. 2006).

<sup>&</sup>lt;sup>68</sup> 436 F.3d 1117 (9th Cir. 2006).

but agreed with the Government that a more extraordinary remedy—a writ of mandamus—was necessary to protect company secrets.<sup>69</sup>

*Ye* addressed two defendants who were arrested "while attempting to board a flight to China."<sup>70</sup> While executing the arrest, federal agents seized multiple items including technical schematics, design methodologies, design scripts, microprocessor specifications, and other items suspected to be trade secrets from four Silicon Valley companies.<sup>71</sup> Charged with committing economic espionage,<sup>72</sup> the defendants sought—after the Government provided more than 8,800 pages of materials describing each allegedly stolen trade secret via a pretrial protective order—the opportunity to conduct pre-trial depositions to determine "what exactly is . . . alleged to be the trade secret and why it is a trade secret in advance of trial."<sup>73</sup>

Protective orders were at the heart of *Ye*.<sup>74</sup> The parties negotiated and executed a protective order before the defendants designated an expert to review the trade secret materials provided by the Government.<sup>75</sup> The protective order specifically provided that "Ye's counsel has not yet selected an expert to undertake assignment of reviewing any confidential or trade secret information"<sup>76</sup> with the parties acknowledging that the protective order "may be subsequently modified in such a way as to provide for the disclosure of confidential and trade secret information to … Ye's expert under … restricted circumstances."<sup>77</sup> Indeed, the protective order explicitly contemplated "a further request … [to] disclos[e]

<sup>&</sup>lt;sup>69</sup> *Ye*, 436 F.3d at 1121, 1124.

<sup>&</sup>lt;sup>70</sup> *Id.* at 1119.

<sup>&</sup>lt;sup>71</sup> See id.

 $<sup>^{72}</sup>$  Id. at 1119 n.1 (The defendants were charged with conspiring to commit economic espionage in violation of 18 U.S.C. § 1831(a)(5), possessing stolen trade secrets in violation of 18 U.S.C. § 1832(a)(5) and engaging in the foreign transportation of stolen property in violation of 18 U.S.C. § 2314.).

<sup>&</sup>lt;sup>73</sup> *Id.* at 1119.

<sup>&</sup>lt;sup>74</sup> See id.

<sup>&</sup>lt;sup>75</sup> Id.

<sup>&</sup>lt;sup>76</sup> Protective Order, United States v. Ye, No. CR-5-01-408 PVT, at 2 (N.D. Cal. Jan. 15, 2002) (ECF No. 13).

<sup>&</sup>lt;sup>77</sup> Id.

[information] to an expert hired by . . . Ye in preparation for the trial in this case."<sup>78</sup>

Based on the modification provision, the defendants eventually sought—and the district court granted—permission to depose experts about the trade secrets at issue.<sup>79</sup> The Government moved for reconsideration, offering the sworn declaration of a company counsel who stated that ordering depositions would discourage the reporting of intellectual property crimes because "[r]equiring victims to subject themselves to aggressive pre-trial questioning by defense counsel constitutes revictimization of sorts."<sup>80</sup>

In language that may resonate with any company facing trade secret thefts, the company counsel went on to state that the court's ruling had "extremely disturbing connotations for companies . . . that invent valuable intellectual property" because "allowing pre-trial discovery and examination of [corporate] witnesses is a substantial, intrusive, disturbing and unprecedented step that places . . . proprietary information at risk and shifts a substantial burden to the victim in a criminal case."<sup>81</sup> In addition, the counsel pointed out that a "public airing of our secrets in the context of sworn deposition testimony" might "result in the destruction of all economic value inherent in the trade secrets."<sup>82</sup> Despite these compelling statements, the district court denied the Government's motion for reconsideration and concluded the protective order permitted the depositions.<sup>83</sup>

The Government sought an immediate interlocutory appeal.<sup>84</sup> On interlocutory appeal, the Ninth Circuit held, "§ 1835 does not provide us with jurisdiction over this appeal because the government had already disclosed all of the relevant trade secret materials prior to the making

<sup>&</sup>lt;sup>78</sup> *Id.* at 6.

<sup>&</sup>lt;sup>79</sup> *Ye*, 436 F.3d at 1119-20.

<sup>&</sup>lt;sup>80</sup> Brief for the United States at 11, United States v. Ye, 436 F.3d 1117 (9th Cir. 2006) (No. 05-10073).

 $<sup>^{81}</sup>$  Id. at 12.

<sup>&</sup>lt;sup>82</sup> Id.

<sup>&</sup>lt;sup>83</sup> *Id.*; see also Ye, 436 F.3d at 1120 ("The government's motion for reconsideration was denied, and the government now brings this interlocutory appeal/petition for mandamus.").

<sup>&</sup>lt;sup>84</sup> Ye, 436 F.3d at 1120.

of the order at issue."<sup>85</sup> But *Ye* ultimately relied on an alternative basis for protecting trade secrets—a writ of mandamus under the All Writs Act.<sup>86</sup>

In issuing the writ, the Ninth Circuit concluded that extraordinary circumstances "lean[ed] strongly in favor of granting mandamus relief."<sup>87</sup> According to the court, the district court's order was "'wholly unauthorized' and 'constitute[d] a clear and very substantial departure from the fundamental principles governing criminal pretrial and trial procedures in federal court."<sup>88</sup> The Government had "no alternative means of relief and [would] suffer harm that is not correctable on appeal" because the Government was effectively left with no meaningful recourse if the expert decided to disclose the trade secrets.<sup>89</sup> Finally, the district court's order raised (but did not answer) the question of whether, in light of the EEA, Rule 16 ever "empowers a court to authorize discovery depositions . . . in order to ensure fairness and efficiency and effectively control the dissemination of important trade secrets."<sup>90</sup>

The court in *United States v.*  $Hsu^{91}$  focused on § 1835's strong presumption in favor of protecting trade secrets, even going so far as to characterize trade secret protections as vital public interests.<sup>92</sup> *Ye* went one step further, applying an extraordinary remedy to prevent a threat of disclosure.<sup>93</sup> Both cases demonstrate that federal appellate courts place an extremely high value on the protection of trade secrets during criminal prosecution and will go to substantial lengths to protect secrets, even going beyond the express provisions of the EEA. Each case also demonstrates that the Department of Justice will find creative solutions to ensure a victim company's secrets are kept safe throughout prosecution.

<sup>&</sup>lt;sup>85</sup> *Id.* at 1119.

<sup>&</sup>lt;sup>86</sup> Id.; 28 U.S.C. § 1651 (2012).

<sup>&</sup>lt;sup>87</sup> Ye, 436 F.3d at 1124.

<sup>&</sup>lt;sup>88</sup> Id. (citing In re United States, 878 F.2d 153, 159 (5th Cir. 1989)).

<sup>&</sup>lt;sup>89</sup> Id.

<sup>&</sup>lt;sup>90</sup> Id.

<sup>91 155</sup> F.3d 189 (3d Cir. 1998).

<sup>92</sup> Hsu, 155 F.3d at 197.

<sup>&</sup>lt;sup>93</sup> Ye, 436 F.3d at 1124.

#### G. Alternative Charges

In the unlikely event all of the aforementioned procedural mechanisms fail, the prosecution still has additional arrows in its quiver to prevent the disclosure of trade secrets during litigation. The prosecution may elect to narrow its case to those charges that do not require the prosecution to prove the information taken by the defendant actually constituted a trade secret.<sup>94</sup> For example, if the government charges the defendant with alternate charges provided in the statute, "attempt to steal trade secrets" or "conspiracy to steal trade secrets," then the government need not show that the information taken by the defendant was actually a trade secret—only that the defendant *believed* the information taken was confidential or proprietary information to which the defendant had no claim.<sup>95</sup> At least one court of appeals has expressed skepticism regarding whether a defendant facing attempt and conspiracy charges would need access to trade secret materials at all, given that a defendant "can be

<sup>&</sup>lt;sup>94</sup> United States v. Liu, 716 F.3d 159, 169-70 (5th Cir. 2013); see also 18 U.S.C. § 1832(a)(4)-(5) (2012).

<sup>&</sup>lt;sup>95</sup> Liu, 716 F.3d at 170 ("[T]he relevant inquiry in a conspiracy case . . . is whether the defendant entered into an agreement to steal, copy, or receive information that he believed to be a trade secret—that is, did the defendant believe that the information he conspired to obtain was proprietary and was being taken for the economic benefit of someone other than the owner."); see also United States v. Krumrei, 258 F.3d 535, 539 (6th Cir. 2001) (finding that it was sufficient for the Government to show that the defendant knew the trade secret represented "confidential information to which he had no claim"); Hsu, 155 F.3d at 203 ("The government can satisfy its burden under § 1832(a)(4) by proving beyond a reasonable doubt that the defendant sought to acquire information which he or she believed to be a trade secret, regardless of whether the information actually qualified as such."); United States v. Roberts, No. 3:08-CR-175, 2009 WL 5449224, at \*7 (E.D. Tenn. Nov. 17, 2009) ("[A] defendant must know that the information he or she seeks to steal is proprietary, meaning belonging to someone else who has an exclusive right to it, but does not have to know it meets the statutory definition of a trade secret."); United States v. Genovese, 409 F. Supp. 2d 253, 258 (S.D.N.Y. 2005) (discussing circumstances that would indicate that EEA defendant knew the information was proprietary); H.R. Rep. No. 104-788, at 12 (1996), as reprinted in 1996 U.S.C.C.A.N. 4021, 4030 ("It is not necessary that the government prove that the defendant knew his or her actions were illegal, rather the government must prove that the defendant's actions were not authorized by the nature of his or her relationship to the owner of the property and the defendant knew or should have known that fact."); DAVID QUINTO, TRADE SECRETS LAW AND PRACTICE 307 (2d ed. 2012) ("[T]he government need not prove that the defendant knew that the stolen information fit the legal definition of a trade secret.").

guilty of attempt and conspiracy to steal trade secrets even if the documents contained no confidential information at all."<sup>96</sup> Thus, a prosecutor charging attempt or conspiracy can avoid the need to prove the existence of a trade secret at trial, thus obviating the need to disclose trade secret information to the defense.

Similarly, the government can pursue other charges that do not require proof of a trade secret.<sup>97</sup> This pursuit is consistent with § 1838 of the EEA, which provides that the EEA does not "preempt or displace any other remedies, whether civil or criminal, provided by United States, Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret."<sup>98</sup> A defendant may face alternative federal charges or state charges, or both.

Another option is to charge the defendant with the unlawful access of a protected computer used to obtain information.<sup>99</sup> This crime, codified in the Computer Fraud and Abuse Act at 18 U.S.C. § 1030, punishes unauthorized access of "information," including but not limited to trade secret information.<sup>100</sup> Violations of § 1030 are felonious when they are committed for "commercial advantage or private financial gain," to further any tortuous or criminal act, or if the information's value exceeds \$5000.<sup>101</sup>

Under § 1030, the government may bring charges for unlawfully accessing or attempting to access a protected computer to commit fraud.<sup>102</sup> This charge applies

where the defendant "knowingly and with intent to defraud" accessed or attempted to access a protected computer without authorization, or in excess of authorized access, and by means of such conduct furthered the intended

<sup>&</sup>lt;sup>96</sup> Hsu, 155 F.3d at 204.

<sup>&</sup>lt;sup>97</sup> PROSECUTING INTELLECTUAL PROPERTY CRIMES, *supra* note 25, at 224 ("When confronted with a case that implicates confidential proprietary information, prosecutors may wish to consider other crimes in addition to or in lieu of EEA charges.").

<sup>98 18</sup> U.S.C. § 1838 (2012).

<sup>99</sup> See 18 U.S.C. § 1030 (2012).

<sup>&</sup>lt;sup>100</sup> See S. Rep. No. 104-357, at 7 (1996) (explaining that "information" must be construed broadly).

<sup>&</sup>lt;sup>101</sup> 18 U.S.C. § 1030(c)(2) (2012).

<sup>&</sup>lt;sup>102</sup> *Id.* § 1030(a)(4), (b).

fraud and obtained anything of value, unless the object of the fraud and the thing obtained was computer time worth less than \$5000.<sup>103</sup>

As Congress stated, "[t]he acts of 'fraud' that we are addressing [under this section] are essentially thefts in which someone uses a [protected computer] to wrongly obtain something of value from another."<sup>104</sup> Because EEA cases typically involve some level of deception and related wrongdoing, they will often qualify as fraud.<sup>105</sup>

Charges for mail fraud or wire fraud frequently can be asserted in theft of trade secret cases. These charges capture schemes using the mail or wires to defraud another of property or confidential and proprietary information.<sup>106</sup> For example, in *United States v. Howley*, the Sixth Circuit affirmed a defendant's wire-fraud convictions for emailing photographs containing company trade secrets.<sup>107</sup> The statutes not only apply to physical property but also to confidential information transmitted by wire.<sup>108</sup>

Depending on the conduct at issue, defendants may also face a wide array of other charges. If a defendant stole, reproduced, or distributed copyrighted information, the defendant may face charges of criminal copyright infringement under 17 U.S.C. § 506 and 18 U.S.C. § 2319.<sup>109</sup> It is common for a prosecutor to consider a criminal copyright infringement charge, for instance, where a defendant steals the source code to valuable software.<sup>110</sup> Since source code usually contains sufficient

<sup>108</sup> See, e.g., United States v. Wang, 898 F. Supp. 758, 760 (D. Colo. 1995) (holding 18 U.S.C. § 1343 applies not just to physical goods but also to confidential computer files transmitted by wire).

<sup>109</sup> 17 U.S.C. § 506 (2012); 18 U.S.C. § 2319 (2012).

<sup>110</sup> See Rouse v. Walter & Assocs., LLC., 513 F. Supp. 2d 1041, 1055 (S.D. Iowa 2007) ("It is settled that computer programs are entitled to copyright protection. This protection extends not only to the 'literal' elements of computer software[,] the source code and object code[,] but also to a program's nonliteral elements, including its

<sup>&</sup>lt;sup>103</sup> See Prosecuting Intellectual Property Crimes, supra note 25, at 225-26.

<sup>&</sup>lt;sup>104</sup> 132 Cong. Rec. 7,189 (1986).

<sup>&</sup>lt;sup>105</sup> PROSECUTING INTELLECTUAL PROPERTY CRIMES, *supra* note 25, at 226.

<sup>&</sup>lt;sup>106</sup> 18 U.S.C. §§ 1341, 1343, 1346 (2012).

<sup>&</sup>lt;sup>107</sup> 707 F.3d 575, 581(6th Cir. 2013) (citations omitted) ("No evidence suggests that Goodyear gave Roberts or Howley permission to take photographs. Quite the opposite: The men promised not to take pictures, yet they took them anyway. They then transmitted those pictures electronically. Those acts alone may constitute a material misrepresentation under the wire-fraud statute.").

originality and is fixed in a tangible medium, the code is generally copyright protected whether or not the copyright has been registered.<sup>111</sup>

Moreover, a defendant may be charged with the interstate transportation and receipt of stolen property or goods under certain circumstances, for example, if the defendant steals a hard-copy schematic or thumb drive containing confidential information.<sup>112</sup> In addition, a defendant who exports or imports items on the United States Munitions List without obtaining a license from the Secretary of State may face charges under the Arms Export Control Act<sup>113</sup> and the International Traffic in Arms Regulations.<sup>114</sup> Finally, a defendant who makes false statements to law enforcement can be charged under 18 U.S.C. § 1001, which has been applied in the EEA context, where a defendant made a false statement that "his boss . . . had given him permission to take work documents home."<sup>115</sup>

<sup>112</sup> See United States v. Agrawal, 726 F.3d 235, 253 (2d Cir. 2013) ("[T]here is no question as to such physical identity or prior physical taking. At the moment Agrawal removed . . . [the] code from . . . [the company's] office and transported it across state lines, the code was in the tangible form of thousands of sheets of paper."), cert. denied, 134 S. Ct. 1527 (2014); United States v. Martin, 228 F.3d 1, 14-15 (1st Cir. 2000) ("[Section] 2314 does *apply* when there has been 'some tangible item taken, however insignificant or valueless it may be, absent the intangible component." (quoting United States v. Brown, 925 F.2d 1301, 1308 n.14 (10th Cir. 1991))); see also 18 U.S.C. § 2314 (2012) (punishing "[w]hoever transports, transmits, or transfers in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of \$5,000 or more, knowing the same to have been stolen, converted or taken by fraud"); 18 U.S.C. § 2315 (2012) (punishing "[w]hoever receives, possesses, conceals, stores, barters, sells, or disposes" stolen property that has crossed a state or federal boundary after being stolen). Although courts agree these provisions cover the transportation of stolen tangible property, there is some disagreement over whether the statutes cover the transportation of intangible property. See Agrawal, 726 F.3d at 252-53 ("Had Agrawal stolen the code in intangible form, ... and only later copied it onto paper or some other tangible medium, that would not be enough to 'transform the intangible property into a stolen good' so as to state an NSPA offense." (quoting United States v. Aleynikov, 676 F.3d 71, 78 (2d Cir. 2012))); United States v. Brown, 925 F.2d 1301, 1307 (10th Cir. 1991) (holding that 18 U.S.C. § 2314 did not cover "[p]urely intellectual property").

<sup>113</sup> 22 U.S.C. § 2778 (2015).

<sup>114</sup> 22 C.F.R. §§ 120-30 (2015).

structure, sequence, organization, user interface, screen displays, and menu structures." (quoting Schoolhouse, Inc. v. Anderson, 275 F.3d, 726, 728 (8th Cir. 2002))).

<sup>&</sup>lt;sup>111</sup> See 17 U.S.C. § 102(a) (2012); Feist Publ'ns, Inc. v. Rural Tel. Co., 499 U.S. 340, 345-46 (1991).

<sup>&</sup>lt;sup>115</sup> United States v. Chung, 659 F.3d 815, 830 (9th Cir. 2011).

# II. How Prosecutors Use Protective Orders to Protect Trade Secrets

As in *Ye*, prosecutors commonly use protective orders during a criminal prosecution as one method to protect a victim's trade secrets. The three general types of protective orders apply: pre-indictment, post-indictment, and during trial.

### A. Pre-Trial Protective Orders

Although there are crucial differences in how prosecutors use them, pre-indictment and post-indictment protective orders share several similarities. Pre-indictment protective orders are intended to facilitate information exchanges that may lead to the early resolution of a case. Since there is neither an indictment nor a complaint, there is often no court case. Consequently, a pre-indictment protective order is perhaps more appropriately described as a protective agreement in which the parties generally stipulate to jurisdiction in a particular United States district court in the event of a dispute. At this stage, the subject of the investigation—who has not yet been charged—may not be permitted to view or handle the trade secret materials, though his counsel generally will be able to do so.

Post-indictment protective orders, by contrast, are generally more exhaustive because of the government's extensive production of discovery materials. In discovery, the government typically designates certain documents as needing to be protected, and the protective order sets forth the requirements for the treatment of those materials. For both types of protective orders, the prosecution expects the confidentiality of the designated documents provided or shown to the defense to be zealously guarded. Depending on the nature of the trade secrets, the protective order may require the defense attorney to have certain security clearances before being provided access to trade secret information.

Defense experts, who are often drawn from the field or practice relating to the trade secret, may be in a position to compete with the victim or to consult with the victim's competitors. Therefore, the government and the victim must have the ability to assess that threat before permitting the expert to review trade secret materials. Protective orders may require experts and other third parties to be vetted by the prosecution before they are afforded access to designated materials. Third parties may also be asked to sign on to the protective order, so there is no doubt they understand the requirements of the order and consent to the court's jurisdiction over them. The defendant may or may not be permitted to review some or all of the trade secret materials depending on the circumstances and the perceived risk.

Both pre-indictment and post-indictment protective orders may place certain restrictions on those permitted to access the trade secrets. For example, the recipient of trade secret information may be limited to reviewing the materials at the United States Attorney's Office or the local FBI office. If the recipient is permitted to take protected documents outside of government facilities, he will typically have to take steps to ensure their protection. These steps may include making these documents accessible only in secure areas and on protected computers. In addition, pretrial protective orders typically include provisions instructing those with access to the trade secrets to return or destroy the protected information if the case is resolved before trial.

#### **B.** Trial Protective Order

A trial protective order generally incorporates the protections and terms of the post-indictment protective order, but it also addresses how the trade secrets will be protected during trial.<sup>116</sup> If not addressed in advance, there is a risk at this stage that trade secrets could be disclosed to spectators or end up in the public record. The potential disclosure to jurors is less of a concern because the government can strike jurors who could potentially misuse sensitive information and can implement techniques to limit what is shown to the jury. If the case goes to trial, the government can request the district court to instruct the jury not to discuss or disclose any of the trade secret material they hear or see during the proceedings.<sup>117</sup>

The government has a wide range of options for protecting trade secrets during trial. Witnesses are typically able to convey the value or

<sup>&</sup>lt;sup>116</sup> See 18 U.S.C. § 1835 (2012).

<sup>&</sup>lt;sup>117</sup> See, e.g., United States v. Hsu, 155 F.3d 189, 193 n.3 (3d Cir. 1998).

confidentiality of particular trade secrets without providing critical details of a company's secrets.

With that in mind, options to protect trade secret information during trial include preparing redacted copies of trial exhibits,<sup>118</sup> filing trial exhibits under seal, moving or turning off courtroom displays,<sup>119</sup> presenting testimony at an appropriate level of generality, limiting where spectators may sit in the courtroom,<sup>120</sup> limiting note taking, and closing off the courtroom for limited periods of time.<sup>121</sup>

After trial, defense counsel will generally be required to return or destroy trade secrets documents and to file a sworn declaration with the court indicating he has done so. The prosecutor and the victim may closely review the transcript and any exhibits to ensure the appropriate redactions have been made so the public record does not include trade secret information or otherwise violate the protective order.<sup>122</sup>

## Conclusion

In passing the Economic Espionage Act, Congress recognized that victim companies must be absolutely certain their trade secrets and other sensitive business information will be protected during a criminal investigation and prosecution, so they will refer matters to law enforcement and cooperate with the government in the prosecution of these

<sup>&</sup>lt;sup>118</sup> Id. at 193 (ordering *in camera* review to determine which redactions were warranted).

<sup>&</sup>lt;sup>119</sup> United States v. Roberts, No. 3:08-CR-175, 2010 WL 1010000, at \*9 (E.D. Tenn. Mar. 17, 2010) ("[S]even photographs and any exhibits containing the seven photographs shall be displayed to the jury in such a way that public cannot also see them.").

<sup>&</sup>lt;sup>120</sup> See, e.g., Protective Order, United States v. Yeh, 3:08-CR 00096 (N.D. Tex. Dec. 19, 2013) (ECF No. 28) (ordering trial spectators in the gallery to sit several rows back from counsel's table, such that it would be impossible for spectators to see the details of trade secret information displayed on the screens in the courtroom).

<sup>&</sup>lt;sup>121</sup> See United States v. Aleynikov, No. 10 Cr. 96(DLC), 2010 WL 5158125, at \*1 (S.D.N.Y. Dec. 14, 2010) ("Over the course of the eight day trial, the courtroom was closed on seven occasions, most of them lasting no longer than 20 minutes."), *rev'd on other grounds*, 676 F.3d 71 (2d Cir. 2012).

<sup>&</sup>lt;sup>122</sup> See id. (ordering the parties after trial to "review the transcript to determine whether more of the trial transcript could be placed in the public record").

matters. Thus, Congress provided prosecutors with a significant range of tools to protect trade secrets before, during, and after trial. A prosecutor's goal is always to do justice, and doing justice requires that victim companies not feel re-victimized during a prosecution. Prosecutors have and will employ every tool in their toolbox to zealously guard these trade secrets. To date, no trade secret has lost its trade secret status or otherwise became known as a result of a federal trade secret investigation or prosecution. American Journal of Trial Advocacy [Vol. 38:461

484