# A SECRET NO MORE

## THE RISE OF ECONOMIC ESPIONAGE PROSECUTIONS AND HOW TO LITIGATE THEM

BY GARY S. LINCENBERG
AND PETER J. SHAKOW

Stealing trade secrets from US companies is big business. A competitor can save years of effort and millions in research and development costs by lifting an important source code, design plan, or chemical formula from a company that worked hard to develop it, and unscrupulous businesspeople are finding it more tempting than ever to engage in such thievery. Given the immense value stolen trade secrets can represent to an emerging economy and the increasing ease with which data can secretly be transported across national boundaries, even foreign governments are getting in on the action, or looking the other way while their citizens do so. Indeed, two decades after the end of the Cold War, many nations increasingly view economic strength as more important to national security than military strength, and some see trade secret theft as the quickest way to get there. It is not surprising, then, that the United States has come to see this as a pressing threat to its own national economic security. Trade secret theft arguably costs US businesses billions of dollars a year in lost revenue and millions of jobs. It deincentivizes innovation and creates a drag on our economy. And while foreign spies have long targeted aerospace and defense technologies, economic espionage has now expanded into other vital industries such as high tech, renewable energy, agribusiness, and the financial services sector. (*See* Comm'n on the Theft of Am. Intellectual Prop., Nat'l Bureau of Asian Research, The IP Commission Report 2 (2013), *available at* www.ipcommission.org/report/IP_Commission_Report_052213.pdf.)

Over the last few years, the Department of Justice (DOJ) has signaled that it is ramping up its efforts to combat this threat, raising the specter of additional prosecutions under the Economic Espionage Act of 1996 (EEA or the Act). Passed at the urging of law enforcement, the EEA was touted as a way for federal prosecutors to deal with a new kind of foreign enemy—one dressed in a business suit, not a military uniform. The Act sets out tough penalties for anyone convicted of stealing a trade secret, and tougher ones for those who did so while "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent." (18 U.S.C. §§ 1831–32.) Prosecutions under the EEA were initially slow to develop, however, and it is only in the last few years that trade secret theft cases have started to gain momentum. The Obama White House has made combatting trade secret theft a national priority and created an "IP czar" to coordinate prosecution efforts. The DOJ and FBI have created task forces to address intellectual property (IP) crime. Congress recently amended the EEA to make the crime easier to prosecute and to ratchet up sentences. And while most cases of trade secret theft are still resolved in the civil courts, the number of criminal cases is on an upward trend. Companies and counsel need to take stock of the changes in the criminal law, DOJ priorities, and strategies for litigating these cases. This article serves as a launch pad for doing so.

**GARY S. LINCENBERG** *and* **PETER J. SHAKOW** *are partners at the Los Angeles law firm Bird, Marella, Boxer, Wolpert, Nessim, Drooks, Lincenberg & Rhow, P.C.*

## Historical Context

Before passage of the EEA, federal prosecutions of trade secret theft were rare. There was no "comprehensive federal remedy targeting the theft of trade secrets, compelling prosecutors to shoehorn economic espionage crimes into statutes directed at other offenses," like the Depression-era National Stolen Property Act (NSPA), 18 U.S.C. § 2314. (United States v. Hsu, 155 F.3d 189, 194 (3d Cir. 1998).) Courts grew weary of efforts to stretch existing statutes to cover this conduct, and prosecutions achieved only limited success. Nor were trade secret theft cases prosecuted effectively at the state level. Though almost half the states had criminal statutes to cover trade secret theft, they were "of little assistance [because state authorities] often lacked sufficient resources to pursue espionage prosecutions." (*Id.* at 195 n.7.) This left victims to pursue civil remedies. But those, too, were often of limited value because victims "had to shoulder their own litigation costs, individual defendants were frequently judgment proof, and it proved difficult for the state courts to exercise jurisdiction over lawsuits involving out-of-state defendants." (*Id.*)

When information technology first underwent its meteoric advancement in the 1980s and '90s, those looking to steal trade secrets faced few obstacles: Not only did the growth of the Internet and more powerful data storage devices make it easier to obtain a company's internal secrets, but also the tools available to law enforcement to stop or punish such theft lagged behind the times. Because companies were increasingly relying on technology to run their businesses, it also made those internal trade secrets more critical to the companies themselves. Congress came to recognize that in this new world, existing federal law was inadequate. It presented the EEA as a way to address this new and growing threat.

## The Act's Provisions

The EEA consists of nine separate statutes in Title 18. Section 1831 punishes theft of trade secrets where the offender intends to benefit a foreign government or its agent; this is generally known as "economic espionage." It reads, in relevant part:

> Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains a trade secret . . . shall, except as provided in subsection (b), be fined not more than $5,000,000 or imprisoned not more than 15 years, or both.

Section 1832 is the general trade secret theft statute, and does not require proof of any intent to benefit a foreign government or agent. It reads, in relevant part:

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for

> use in interstate or foreign commerce, 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 . . . steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information . . . shall, except as provided in subsection (b), be fined under this title or imprisoned not more than 10 years, or both.

Each of these statutes also specifically prohibits the attempt and conspiracy to commit the offense and subjects organizational defendants to larger criminal fines. (18 U.S.C. §§ 1831(a)(4)–(5), (b); 1832(a)(4)–(5), (b).) Other elements of the Act permit the government to seek criminal forfeiture of proceeds of the offense (*id.* § 1834), orders to preserve the confidentiality of the trade secrets at issue (*id.* § 1835), and civil injunctive relief (*id.* § 1836). The EEA provides for extraterritorial jurisdiction if the offender is a citizen or permanent resident alien of the United States (or an organization organized under US law) or if an act in furtherance of the offense was committed in the United States. (*Id.* § 1837.) Finally, the Act does not "preempt or displace any other remedies, whether civil or criminal, provided by [federal or state] law for the misappropriation of a trade secret." (*Id.* § 1838.) The EEA, in other words, is not an exclusive remedy.

## The Growth of Trade Secret Prosecutions

Despite early predictions that the DOJ would bring dozens of prosecutions a year under these new statutes, cases were initially slow to materialize. That now appears to be changing. The FBI reports that its investigations of trade secret theft are up 29 percent since 2010, and the DOJ reports that over the last three fiscal years it has investigated and prosecuted 40 trade secret and economic espionage cases (nearly double the number of cases brought in a similar timeframe earlier in the decade). (Exec. Office of the President, Administration Strategy on Mitigating the Theft of U.S. Trade Secrets 7 (2013) [hereinafter Administration Strategy], *available at* http://tinyurl.com/coxgogr; *see also* U.S. Dep't of Justice, PRO IP Act Annual Report FY2010, at 17 (2010); U.S. Dep't of Justice, PRO IP Act Annual Report FY2011, at 18 (2011); U.S. Dep't of Justice, PRO IP Act Annual Report FY2012, at 16 (2012); *cf.* R. Mark Halligan, Reported Criminal Arrests and Convictions under the Economic Espionage Act of 1996 (2003), *available at* http://tradesecretshomepage.com/indict.html.) Even the rarer § 1831 prosecutions, which allege benefit to a foreign government, instrumentality, or agent, appear to be on the rise. Only four such cases were brought during the first 12 years after passage; five more have been charged since 2010, including a high-profile prosecution that went to trial in San Francisco earlier this year.

A number of factors appear to have contributed to this rise in EEA cases. First, both the White House and the attorney general have publicly stated that prosecution of trade secret theft is a high priority and have taken steps to promote enforcement efforts. In 2009, President Obama named, and the Senate confirmed, the first US intellectual property enforcement coordinator. This "IP czar" is housed within the executive office of the president and has been allocated staff and resources to coordinate the efforts of various agencies and departments, including the DOJ. In 2010, the attorney general established a Task Force on Intellectual Property, chaired by the deputy attorney general, to focus the department's IP crime enforcement efforts, including prosecution under the EEA. The FBI has formed an Economic Espionage Unit, assigned hundreds of agents to investigate allegations of IP theft, and is developing partnerships and regional working groups with academia and defense contractors "to enhance their understanding of the threat posed to their programs and personnel by foreign intelligence services and foreign competitors." (*See Counterintelligence Strategic Partnerships*, FBI, http://tinyurl.com/o9cnqeu (last visited Sept. 8, 2014).) In 2013, the Obama administration issued a first-of-its-kind written strategy for combatting economic espionage. This *Administration Strategy* is a broad-reaching interagency plan that counts "enhanc[ing] domestic law enforcement operations" as one of its key planks. (Administration Strategy, *supra*, at 7–10.) The full extent of this increased focus and coordination has yet to be seen, but these efforts by the executive branch suggest that prosecutions for trade secret theft will increase over the next several years.

Second, Congress recently amended the EEA to make the statute a more powerful and attractive tool for prosecutors. The Foreign and Economic Espionage Penalty Enhancement Act of 2012, for example, increased potential fines for violations of § 1831 tenfold for individuals (from $500,000 to $5 million). (18 U.S.C. § 1831(a), (b).) Congress also recommended, and the US Sentencing Commission adopted, higher guideline ranges for those defendants who knew or intended the trade secret to be transmitted outside of the United States, even if they did not know or intend that the trade secret would benefit a foreign government. (*See* U.S. Sentencing Guidelines Manual § 2B1.1(b)(13)(A).) The amendments also broadened the definition of "trade secret" under the EEA to

***Despite early predictions that DOJ would bring dozens of prosecutions a year under the new statutes, cases were slow to materialize. That now appears to be changing.***

include goods or services that are *used or intended for use* in interstate or foreign commerce, not just those products physically "placed" in the stream of commerce. Each of these changes makes it easier to prosecute or punish trade secret theft, and Congress has indicated it will continue to consider legislation aimed at increasing enforcement in this area.

A third factor that suggests prosecutions will continue to rise is a global business environment in which the United States continues to lose business income and employment to its foreign competitors, and in which there is substantial public and corporate pressure to stem those losses. We now live in a world where employees are expected to have enormous amounts of company information at their fingertips, and on devices that are built for transportability, making it easier than ever to steal trade secrets. Global competition—including from companies based in countries such as China and Russia, where trade secret protections are not vigorously enforced—creates enormous demand for such information, which can dramatically reduce costs of production and offers other significant business advantages. Private companies that suspect they have been victims of trade secret theft—especially those with the resources to conduct sophisticated internal investigations and the contacts to prod the government into action—have already begun to pressure local US attorney's offices to bring criminal charges against alleged violators. Behind many of the major federal criminal cases involving theft of trade secrets is a big company with the resources and incentive to promote the prosecution—Motorola, DuPont, Boeing, Bristol-Myers Squibb, and Korn/Ferry International, to name just a few. Indeed, defense attorneys have pointedly noted the hand-in-glove working relationship that appears to have developed in some of these cases between the company's lawyers and the government, raising questions about fairness and objectivity. Nevertheless, these pressures and relationships will continue to encourage EEA investigations and prosecutions in the years ahead.

## Defense Theories and Real-World Results

Thus far, relatively few economic espionage or trade secret theft cases have gone to trial. But some of the strategies employed by defense counsel in those trials—and in pretrial maneuvering—have proven successful and are worth consideration by those facing similar charges.

**Jurisdictional issues can knot up a case.** Congress understood that EEA prosecutions would often involve foreign individuals and foreign companies, so it built into the law a broad extraterritoriality provision. That hasn't stopped foreign defendants, however, from defending against EEA charges on jurisdictional grounds. The very first case charging violations of § 1831, in fact, was also the first instance in which the United States sought extradition from Japan for someone accused of a white-collar crime. (United States v. Okamoto, No. 1:01-cr-210-DDD (N.D. Ohio May 8, 2001).) There, a Japanese national resisted extradition after he was accused in 2001 of misappropriating genetically engineered cells and other materials from the Cleveland Clinic Foundation. In 2004, the Tokyo High Court sided with Professor Okamoto and denied the DOJ's extradition request. The case remains unresolved more than 10 years later.

Jurisdictional headaches can influence EEA prosecutions even when the individual defendants are United States citizens, or were arrested here. In *United States v. Liew*, for example, the government charged multiple defendants in connection with the alleged theft from DuPont of the chemical formula for titanium dioxide, a compound that allows manufacturers to make whites brighter, an important application in such fields as paint, plastics, and paper. (No. 3:11-CR-573 (N.D. Cal. Feb. 7, 2012)). In addition to Walter Liew, a naturalized American from Malaysia who was accused (and later convicted) of stealing this information from DuPont, the government charged several affiliated Chinese companies (the "Pangang" companies) that were alleged to be the ultimate beneficiaries of Liew's efforts. The Pangang companies successfully argued, however, that the government was never able to effectuate service of the indictment. (*See, e.g.*, Order Granting Specially Appearing Defendants' Motion to Quash Service of Indictment, *Liew*, No. 3:11-CR-573 (N.D. Cal. July 23, 2012), ECF No. 176; Order Granting Motion to Quash, *Liew*, No. 3:11-CR-573 (N.D. Cal. Apr. 8, 2013), ECF No. 293.) In part, this was because the Chinese government was unwilling to serve the Pangang companies under the terms of a mutual legal assistance agreement with the United States—hardly a surprising result since the Pangang companies are alleged to be state-owned. The trial went forward in 2014 without any of the Pangang companies as served defendants.

The government has run into similar problems in the *Kolon Industries* case. There, a Korean manufacturer stands accused of stealing the science behind Kevlar (another product of DuPont). When the government indicted Seoul-based Kolon Industries in August 2012, though, the company's US-based counsel specially appeared and prevailed on a motion to quash for ineffective service. As of this writing in September 2014, the question of service is still being litigated (in May 2014 Kolon's attorneys won a second motion to quash service; three months later, the government successfully moved for issuance of a new set of summonses that it will again attempt to serve), effectively stalling any momentum the DOJ hoped to generate with its high-profile charges. (United States v. Kolon Indus. Inc., 926 F. Supp. 2d 794 (E.D. Va. 2013) (granting initial motion to quash); Order Granting Motion to Quash, *Kolon Indus.*, No. 3:12-CR-137 (E.D. Va. May 2, 2014), ECF No. 132; Order Granting Motion for Issuance of New Summonses, *Kolon Indus.*, No. 3:12-CR-137 (E.D. Va. August 14, 2014), ECF No. 135.)

**What's in a "trade secret"?** Often, the battle in EEA cases is whether the subject information actually constitutes a "trade secret." This argument has taken a variety of forms. In *United States v. Jin*, the defendant was caught trying to board a plane to China with thousands of documents from her former employer, Motorola. Jin argued that the documents related to a technology that was so old and outdated that it had no independent economic value (an essential attribute of a

trade secret). (833 F. Supp. 2d 977, 1009–10 (N.D. Ill. 2012).) The defendant in *United States v. Lange*, a disgruntled former employee of an airline parts manufacturer, offered for sale on the Internet (for $100,000) all the specifications of certain brake assembly components that a competitor would need to build the parts to FAA certification standards. (312 F.3d 263, 265 (7th Cir. 2002).) His defense was that this information could be obtained legally merely by reverse engineering the brake assemblies. (*Id.* at 269.) In his 2014 trial, Walter Liew argued that DuPont's "secret formula" for titanium dioxide had been in the public realm for years, and so did not meet the definition of "trade secret." All three of these defendants were ultimately convicted, but this area should still be fertile ground for potential defense argument, particularly given the rapid obsolescence of technology and because "[w]hether information qualifies as a trade secret is a fact-specific inquiry that requires an ad-hoc evaluation of all the surrounding circumstances." (*Jin*, 833 F. Supp. 2d at 1006 (internal quotation marks omitted).)

**Key distinctions between definitions of "trade secret."** To better craft potential defense themes, it is important to understand the EEA's definition of a trade secret, and how it differs from what is used in the civil context. 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).)

Although this definition is based on the Uniform Trade Secrets Act (UTSA), and courts handling EEA cases have looked to civil precedent to help them interpret it, there are important differences in language that appear to expand the definition beyond what is protected civilly.

Both the EEA and UTSA definitions require reasonable efforts on the part of the owner to maintain the secrecy of the information. Both require that the information derive independent economic value from being kept secret. But the EEA arguably permits prosecutions for a much broader array of information. A valid defense under the UTSA is that the information alleged to be a "trade secret" is generally known to or readily ascertainable by "other persons who can obtain economic value from its disclosure or use." (*See* UTSA § 1(4).) In the case of airline brake assembly specifications, for example, this might include other engineers or those with a professional interest in the physics of such devices. If that information can be reverse engineered by a competitor airplane parts manufacturer, then the information would not be considered a "trade secret" in a civil case. Under the EEA, on the other hand, all the government must show is that the information was not generally known to or readily ascertainable by "the public." Writing in dicta, the Third Circuit has contrasted that language to that of the UTSA and opined that the EEA's use of "the public" should mean "the general public" and not just those who might benefit economically from the secret's disclosure. (United States v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998).) In other words, if the average person on the street can't reverse engineer the brake assemblies, then that information is a trade secret for purposes of the EEA no matter what engineers at Boeing or Lockheed could do. Judge Easterbrook in the Seventh Circuit, on the other hand, has suggested the EEA's use of the phrase "the public" is merely shorthand for the UTSA's more specific definition. *Lange*, 312 F.3d at 268. Both courts were writing in dicta, but the contrasting opinions set the stage for this dispute to arise in future cases. The Third Circuit's expansive view has been adopted by more trial courts, but Judge Easterbrook's opinion, of course, holds more promise for defense counsel. The latter also seems more fair; after all, why should a defendant be subject to criminal prosecution for stealing information that would not even constitute a trade secret in the civil arena?

## Vagueness Challenges

Civil trade secret disputes also provide greater procedural protections for defendants than are afforded to the accused under the EEA. Under the UTSA, which has been adopted by most states, a plaintiff must identify the allegedly misappropriated trade secret with reasonable particularity in its complaint, or risk dismissal. (*See, e.g.*, Cal. Civ. Proc. Code § 2019.210; *see also* Brescia v. Angelin, 90 Cal. Rptr. 3d 842 (Ct. App. 2009).) To avoid a demurrer at the initial pleading stage, then, plaintiffs must "describe the subject matter . . . with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies." (Diodes, Inc. v. Franzen, 67 Cal. Rptr. 19, 24 (Ct. App. 1968).) A civil defendant can get the case dismissed, then, even before discovery commences if the trade secret at issue is not described with sufficient particularity.

In a criminal case under the EEA, on the other hand, the federal government need not clearly identify the trade secret at issue for the defendant before seeking an indictment, much less before executing a search warrant, subpoenaing documents, or interviewing potential witnesses. Indeed, the government can affirmatively *withhold* from the defense key information about the trade secrets at issue pursuant to confidentiality or protective orders as provided in 18 U.S.C. § 1835. A number of defendants have sought to highlight the unfairness of this distinction. In *United States v. Case*, for

example, the indictment alleged theft of trade secrets from Eaton Industries, a manufacturing company. The charges dutifully tracked the language of the general trade secret theft statute, but gave no more than a broad outline of the secrets alleged to have been stolen. The defense cried foul, arguing that when the indictment provides no meaningful context through which the defendant can identify the specific trade secret he or she is accused of stealing, merely reciting the statutory language fails to provide the constitutionally required notice of the alleged offense. The court agreed, dismissing the trade secret theft charges because the government had failed to plead the trade secrets with sufficient particularity. What the government failed to allege about these trade secrets, the court explained, went to the very core of the criminality under the statute:

> [I]n a case where the government's stated position is that these defendants stole Eaton's "entire working product," that is, an "entire universe" of information, some of which were trade secrets, some of which were "proprietary" and some of which are proposed to be presented to the jury as "other materials," this purported limitation of the generic word "trade secret" is so broad as to be meaningless and thus, is ineffectual.

(United States v. Case, No. 3:06-CR-210, 2007 WL 1746399, at *1, *3–4 (S.D. Miss. June 15, 2007).)

In *Liew*, where the defendant was charged with having passed DuPont's titanium dioxide formula to companies controlled by the Chinese government, the defense moved to dismiss on similar grounds, citing *Case*. While denying the motion to dismiss, the court did order a bill of particulars requiring the government to detail the secrets purportedly at issue. (Order Denying Joint Motion to Dismiss Second Superseding Indictment and/or to Strike Trade Secrets Nos. 1 and 5 and Counts 3, 5, and 8 and Granting in Part and Denying in Part Joint Motion for Bill of Particulars at 12, United States v. Liew, No. 11-CR-573-2-JSW (N.D. Cal. June 11, 2013), ECF No. 338.)

## Independent Economic Value

Another hotly debated issue in EEA prosecutions is whether the misappropriated information has independent economic value. To what degree, for example, does the information confer a competitive advantage on its owner? Is there a customer base associated with the stolen information? To what cost and effort did the owner go to develop the secret information? Courts that have opined in this area generally interpret the requirement liberally. In *United States v. Chung*, for example, some of the purloined documents related to a Boeing project to build antennas for the space shuttle. The documents at issue listed the tasks and time required to integrate the new antenna system. Even though Boeing was the sole-source contractor for this project, the Ninth Circuit found independent economic value in the information because it "could assist a competitor in understanding how Boeing approaches problem-solving and in figuring out how best to bid on a similar project in the future . . . by underbidding Boeing on tasks at which Boeing appears least efficient." (United States v. Chung, 659 F.3d 815, 827 (9th Cir. 2011).)

In *Jin*, the defense argued that documents relating to Motorola's iDEN or "push-to-talk" technology was outdated and nearly obsolete by the time Jin sought to take it with her to China. The court found this information had some "actual or potential" economic value, though, because Motorola had a near monopoly over iDEN systems and there were still some subscribers to the technology. The stolen documents could conceivably have been used by competitors to develop their own iDEN systems, which could then be offered at lower cost. Though these dangers "might be illusory," and while Motorola's corner on the market was "[m]aybe not a terribly valuable monopoly, in view of technological advances that would soon make iDEN obsolete," the court found these secrets to contain enough independent economic value to land Jin in prison for four years. (United States v. Jin, 733 F.3d 718, 721 (7th Cir. 2013).)

Whether a particular piece of information has independent economic value, however, is not always clear cut, and will depend on the specific facts and circumstances. Particularly in an era where technology is so rapidly made obsolete, attorneys are well served to at least explore a defense based on lack of independent economic value.

**Reasonable efforts to protect the trade secret from disclosure.** A number of cases have also examined whether the owner of the trade secret took "reasonable measures" to keep the information secret. Congress cautioned that owners should not be required to take "heroic measures" for their efforts to be deemed reasonable, but companies need to be able to articulate some common sense efforts to maintain the secrecy of the information.

Courts have not been formalistic in their approach here, however, and have most often found this element met no matter how sparse the owner's effort. Consider *United States v. Nosal*, a case out of the Northern District of California, in which an executive search firm specialist was convicted under § 1832 of the EEA for misappropriating source lists, names, and contact information from the proprietary database of his former employer, Korn/Ferry International. (No. CR-08-0237-EMC, 2013 WL 4504652, at *17 (N.D. Cal. Aug. 15, 2013).) The information Nosal obtained was not encrypted or separately password protected on Korn/Ferry's "Searcher" database, and could be printed out and/or e-mailed to people outside the firm. Nor did the firm have any policies against employees taking such lists or information home with them at night. Nevertheless, the court found the firm had taken "reasonable steps" to protect these source lists from public disclosure because the database was protected by a firewall and antivirus software (true of nearly every company's IT systems today); because when a source list was run, a dialogue box would appear stating, "This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only"; and because of anecdotal testimony (but no written

policies) that the firm did not permit source lists to be sent outside the company. (*Id.* at *16–17.) The trial judge acknowledged that, "[t]o be sure, there is evidence in the record that [Korn/Ferry] did not take every conceivable step to protect" the source lists, but nevertheless found there was enough to constitute "reasonable steps" to protect it. (*Id.* at *17.)

There are a number of reasons why defense counsel should nevertheless explore whether the company's efforts satisfy this burden. In *Jin*, for example, defense counsel successfully obtained revealing documents from the company about its security provisions, its efforts to enforce those provisions, and even its internal investigation of the defendant, all in the context of trying to ascertain whether Motorola took "reasonable measures" to protect its trade secrets. (*See* Hanjuan Jin's Motion to Compel Production of Subpoenaed Documents, *Jin*, No. 08-CR-192 (N.D. Ill. May 25, 2010), ECF No. 91; Minute Entry Ordering Production of Certain Subpoenaed Documents, *Jin*, No. 08-CR-192 (N.D. Ill.), ECF No. 107.) Moreover, as jurors become increasingly familiar with protecting their own information (resetting passwords in the wake of the Heartbleed virus, for instance, or increasing their Facebook security settings), they may come to expect more of companies in this area than the court did of Korn/Ferry. Armed with the right information, defense counsel might be able to argue that the company regularly failed to enforce its own security policies, that it meted out disparate punishment for perceived security violations, or even that measures taken to protect the "secrets" at issue paled in comparison to what it did to protect other important information. Even if a judge or jury ultimately finds a company's efforts were "reasonable," by demonstrating that the efforts were not extensive or well-enforced, a defense attorney can emphasize that the "trade secret" at issue could not have been very important to the company, or that the government is trying to criminalize mere workplace transgressions. This can benefit the defense at every stage of the proceeding—from preindictment negotiations to pretrial motions to trial and even sentencing.

**Must it be a trade secret, or is it enough if the defendant believes it is a trade secret?** Finally, in cases charging conspiracy and attempt, the government need not prove that the information at issue actually constituted a trade secret, just that the defendant *thought* it did. Because the gravamen of those offenses is the agreement or intent to commit the underlying offense (along with a substantial step or overt act in furtherance), whether the information a defendant seeks to steal actually meets the definition of a trade secret is almost immaterial. (*See, e.g.*, United States v. Hsu, 155 F.3d 189, 202–04 (3d Cir. 1998) (denying defense motion to review documents containing alleged trade secrets because it did not matter whether they constituted trade secrets); *Nosal*, 2013 WL 4504652, at *12 (finding defendants could still be guilty of conspiracy even if the information at issue did not constitute a trade secret and the object of the conspiracy was therefore impossible); United States v. Liew, No. 11-CR-573-JSW (N.D. Cal. June 11, 2013), ECF No. 338 (same). *Accord* United States v. Liu, 716 F.3d 159, 170 (5th Cir. 2013); United States v. Yang, 281 F.3d 534, 544 (6th Cir. 2002); United States v. Martin, 228 F.3d 1, 13 (1st Cir. 2000).)

These decisions might not end the debate, however. A number of circuits have yet to rule on this issue, and the Seventh Circuit explicitly left open the possibility of going the other way. It is far from clear, Judge Easterbrook wrote,

> that sale of information already known to the public could be deemed a substantial step toward the offense, just because the defendant is deluded and does not understand what a trade secret is. Selling a copy of *Zen and the Art of Motorcycle Maintenance* is not attempted economic espionage, even if the defendant thinks that the tips in the book are trade secrets . . . .

(United States v. Lange, 312 F.3d 263, 268–69 (7th Cir. 2002).)

Judge Easterbrook's comments were dicta here, too, but given the right set of facts, some defendants might find in them a winning argument.

## Intent to Benefit a Foreign Government

To prove economic espionage under § 1831, the government must prove that the defendant acted with the intent or knowledge that his or her offense would benefit a foreign government, instrumentality, or agent. It is generally agreed that "benefit" in this context should be construed broadly to include not just economic benefit, but also strategic, reputational, or tactical benefits. How that definition plays out in the real world, however, is another hotly litigated area of the law, at least in the limited number of § 1831 cases that have gone to trial.

In *United States v. Lee*, the defendants were engineers employed by a semiconductor company, NetLogic Microsystems. An FBI investigation uncovered that they had unauthorized copies of NetLogic documents on their home computers, that they had set up their own competing corporation in the People's Republic of China (PRC), and that they intended to apply for a small business grant from the Chinese government to help their company get off the ground. The crux of the prosecution's argument was that the Chinese government must have expected something in return for that loan. Indeed, before trial, the court was led to believe the government would introduce evidence that the grant constituted venture capital, giving the PRC a vested interest in the company. When no such evidence was introduced (the grant implied no equity stake in the company for the Chinese government), federal prosecutors argued that an indirect benefit to the government of China—increased tax revenue, an enhanced technical sector, or the like—should be enough. The court disagreed: "Section 1831 does not penalize a defendant's intent to personally benefit or an intent to bestow benefits on the economy of a country that might be realized from operating a company in a foreign country." (United States v. Lee, No. CR 06-0424, 2010 WL 8696087, at *6 (N.D. Cal. May 21, 2010).) The government also contended

that because Lee's company received substantial funding from the Chinese government, the company itself was an instrumentality of the PRC. That argument, too, was rejected.

Whether a company is under the "substantial control" of the government (and therefore an instrumentality thereof) is not determined solely by funding source. The legislative history is clear that this test is not meant to be "mechanistic or mechanical":

> The simple fact that the majority of the stock of a company is owned by a foreign government will not suffice under this definition, nor for that matter will the fact that a foreign government only owns 10 percent of a company exempt it from scrutiny. *Rather the pertinent inquiry is whether the activities of the company are, from a practical and substantive standpoint, foreign government directed.*

(142 Cong. Rec. S10,885 (daily ed. Sept. 18, 1996) (emphasis added).)

There was no suggestion in the written record in *Lee* that the defendants' company would have been directed by the government of the PRC; indeed, the court specifically found that "[t]here was no evidence that any of Defendants' conduct was solicited, sponsored, coordinated by a representative of the PRC," nor was there any evidence "that Defendants intended to or were required as a condition of the grant to transfer any technology to the PRC." (*Lee*, 2010 WL 8696087, at *7–8.)

In *Jin*, the defendant was convicted in a bench trial of stealing trade secrets from her employer, Motorola, because she downloaded and removed hundreds of documents relating to its "push-to-talk" technology, but the judge rejected the economic espionage charges, finding a lack of evidence that Jin intended to benefit the PRC. During its investigation of the case, the government discovered that the defendant had been in job negotiations with Sun Kaisens, a China-based competitor of Motorola that develops telecommunications technology for the Chinese military. As summarized by the court, the government's argument was that "Jin knew her conduct would benefit the PRC because Sun Kaisens develops telecommunications technology for the Chinese military, Jin knew that Sun Kaisens developed telecommunication projects for the Chinese military, and the trade secrets pertained to telecommunications technology." (United States v. Jin, 833 F. Supp. 2d 977, 1019 (N.D. Ill. 2012).) The judge, however, was unconvinced that she planned to give the trade secrets to Sun Kaisens, let alone the Chinese government, and found that the prosecutors' "inferential chain from the facts to the Government's conclusion fails to establish the required proof beyond a reasonable doubt." (*Id.*) In particular, the court cited the lack of evidentiary connection between the outdated technology at issue and the kinds of technology the Chinese military was seeking. Without a more direct connection to the government of the PRC, the court found, Jin's actions did not rise to the level of economic espionage.

Finally, in *Liew*, which went to trial in early 2014, the defendants were accused of passing trade secrets to companies allegedly controlled by the government of the PRC. Because the government was unable to serve the China-based companies as defendants in the case, it relied on its cross-examination of the defense's expert, the testimony of a former low-ranking employee of one of the companies, and other indirect evidence that the companies were state-owned and controlled. Liew suggested such evidence was insufficient, and also contended that there was no evidence he intended to benefit the Chinese government (as opposed to the country more generally). Clearly, the jury did not agree, as it convicted him of intending to benefit a foreign government. But this issue is likely to continue to arise in defense of EEA allegations, in part because it is one of the few areas with precedent favorable to the defense.

Defense victories on this front might be more symbolic than practical, however, given recent changes to the sentencing guidelines. Economic espionage cases are often charged along with a theft of trade secrets count (or wire fraud, mail fraud, or the Computer Fraud and Abuse Act), all of which are generally governed by section 2B1.1 of the Sentencing Guidelines. The Sentencing Commission recently added a two-level enhancement to be applied when the defendant knew or intended that the trade secret would be transported or transmitted out of the United States. (*See* U.S. Sentencing Guidelines Manual § 2B1.1(b)(13) (effective Nov. 1, 2013).) This permits an enhanced sentence even without any proof of intent to benefit a foreign government. Instead, all a prosecutor must show is intent to take the trade secret beyond the borders of the United States (and even that must be proven only by a preponderance of the evidence).

## Use of the EEA by Victim Corporations

The EEA can be a powerful tool for companies that believe they have been victimized. Having the federal government take on the responsibility (and cost) of prosecuting trade secret theft comes with a number of advantages over civil litigation. As noted above, private civil plaintiffs must plead trade secret violations with more specificity than is required of the government. Nor do private companies have the same powers to subpoena and interview witnesses as federal law enforcement. The advantages of bringing in the feds are particularly visible where the perceived thief is a company outsider or foreign national, over whom the company might have little or no leverage. These advantages need to be balanced, however, against the possible downsides of getting the government involved. The pace and scope of an investigation and prosecution, for example, will be largely beyond the company's control. Civil cases may be stayed and remedies therefore delayed. And the attention generated by a federal prosecution might also elevate the profile of the theft and add to a victim company's public relations woes.

The EEA can also create havoc for companies that stumble into charges themselves. It is commonplace for engineers, for instance, to move from one company to a competitor, and to bring their knowledge base with them. Indeed, they might well have been recruited to their new employer because of expertise or experience developed at a prior company. Bringing that expertise across is no crime, but corporations have faced immense penalties for encouraging or even tolerating employees who bring with them tangible materials containing trade secrets from their old employer. Boeing, for example, was fined hundreds of millions of dollars in 2006 and was barred from bidding on billions worth of government contracts after it was discovered the defense giant used confidential documents from Lockheed to shape its bid for a NASA rocket launcher contract. Boeing supervisors had encouraged an engineer recently hired away from Lockheed to bring hundreds of confidential documents with him when he came over. A cautious corporation will have in place (and enforce) policies specifically forbidding the use of competitor trade secrets—not only to discourage this behavior from occurring in the first place, but also to give the company the best possible shot at avoiding criminal charges or other draconian measures in the event it does.

## Conclusion

Congress has long concluded that federal criminal resources should be used to enforce the trade secrets of private corporations. But the debate must continue as to whether Congress has tipped the balance too heavily in favor of the government in these cases, whether criminal defendants should be denied protections afforded to civil litigants in trade secret cases, and whether the law gives too much power to corporations at the expense of entrepreneurs. As more of these cases get litigated, prepared and creative defense counsel will give courts plenty of opportunities to moderate or pare back these institutional advantages. Time will tell if they are successful. ■