Bloomberg BNA

Corporate Law & Accountability Report™

CORPORATE GOVERNANCE

Trade Secret Traps for the Unwary: Potential Corp. Criminal Liability as U.S. Trade Secrets Enforcement Accelerates



BY COLLEEN A. CONRY, ALEXANDRE H. RENE AND ANTHONY C. BIAGIOLI

A criminal statute can quickly evolve from a fringe enforcement priority to a central prosecutorial weapon. Take, for instance, the Foreign Corrupt Practices Act. Originally used to prosecute straightforward bribery of foreign officials, it has launched numerous industrywide investigations of less obvious misconduct. Although companies may now know to protect themselves against the familiar threat of an FCPA investigation, they should also be asking: what's next? The answer may involve a trade secrets statute.

Colleen Conry, a partner and co-leader of Ropes & Gray's government enforcement group, focuses her practice on representing companies and individuals in government investigations on a variety of issues. Alexandre Rene is a partner in Ropes & Gray's government enforcement group with extensive experience representing corporate entities and their executives in connection with litigation and investigations. Anthony Biagioli, an associate in the government enforcement group at Ropes & Gray, has focused his practice on matters involving anti-corruption, theft of trade secrets, and antitrust and securities enforcement actions. Ropes & Gray associates Holly Caldwell and Patrick Roy also contributed substantially to this article.

The U.S. government is intensifying trade secrets enforcement. This emphasis springs from the perception that U.S. companies—and their valuable intellectual property—are under attack from foreign individuals, companies and governments. In its enforcement efforts, the government is targeting not just individuals but companies, including Korean and Chinese companies.[1]

As a result, companies should think hard about their potential exposure for actual or attempted trade secrets theft. Any misconduct by an employee or other agent, loosely within the scope of that person's employment, may subject the company to liability. Thus, a generally compliant company with even one noncompliant employee or consultant may face investigation, criminal prosecution or a civil lawsuit for theft of trade secrets. Trade secret theft may be particularly tempting to employees when the employer might value a competitor's method of production, machine or component design,

[1] *See, e.g.*, Indictment, United States v. Kolon Indus., Inc., No. 3:12-cr-00137, ECF No.3 (E.D. Va. Aug. 21, 2012) (South Korean chemical company Kolon); Indictment, United States v. Liew, No. 3:11-cr-00573, ECF No.64 (N.D. Cal. Feb. 7, 2012) (Chinese state-owned company Pangang); Indictment, United States v. Sinovel Wind Group Co., Ltd., No. 3:13-cr-00084, ECF No. 25 (W.D. Wisc. June 27, 2013) (Chinese manufacturer of wind turbines).

 ISSN 2330-6300

price list, customer list or any other secret information about a competitor's business.[2] And trade secret theft may be particularly likely when companies hire employees or consultants who formerly worked at competitors—which is increasingly common, given frequent labor mobility in the modern economy.[3]

To address these risks, companies should strongly consider developing and enforcing internal compliance policies and procedures aimed at respecting third-party trade secrets.

I. A New Focus on Trade Secret Theft

The government's primary tool to prosecute thefts of trade secrets is the Economic Espionage Act of 1996 (''EEA''), which criminalizes misappropriation of trade secrets with intent to benefit a foreign government (18 U.S.C. § 1831)[4] or any other entity (18 U.S.C. § 1832).[5] Although thefts to benefit foreign governments may grab headlines and violate § 1831,[6] misappropriation by anyone, anywhere can violate § 1832.[7]

The PRO-IP Act of 2008 built on existing law by creating an Intellectual Property Enforcement Coordinator position within the White House and requiring the Department of Justice (''DOJ'') and Federal Bureau of Investigations to provide an annual report on intellectual property enforcement efforts.[8] This law signaled a new focus on protecting IP rights. In furtherance of those efforts, in 2010 the Attorney General started a new DOJ Task Force on Intellectual Property, with 15 new assistant U.S. attorneys and 20 FBI special agents dedicated to combatting IP crimes.[9] FBI trade secret theft investigations have increased by 29 percent since 2010[10] and 39 percent since 2009.[11] Further, the number of reported EEA decisions, including final dispositions, has grown steadily. In the first six years after the EEA's enactment in 1997, there were 10 EEA prosecutions in which a court issued at least one opinion. Over the next six years (2003 to 2008), there were an additional 21 such prosecutions. During the last five years (2009-2013), there were an additional 43.[12]

Several prosecutions are especially noteworthy. Just last year, a Virginia-based cybersecurity firm accused the Chinese military of conducting cyberattacks against it and more than 100 other companies in order to steal

---

[2] *See* 18 U.S.C. § 1839(3) (defining ''trade secret'' to mean information whose owner has taken reasonable measures to keep secret and which ''derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public'').

[3] *See, e.g.*, E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc., 803 F. Supp. 2d 469 (E.D. Va. 2011) (noting that South Korean company, Kolon Industries, was charged under § 1832 because its consultant who used to work for DuPont allegedly passed along trade secrets at Kolon's request).

[4] The statute provides for a fine of not more than $5 million or imprisonment for not more than 15 years for

> [w]ho[m]ever, 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; without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys a trade secret; receives, buys, or possesses a trade secret, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

18 U.S.C. § 1831(1)-(3) (1996). The statute also criminalizes any attempt or conspiracy to commit one of the above acts. *Id.* § 1831(4), (5). Organizations can be fined up to $10 million or three times the value of the stolen trade secret. *Id.* § 1831(b).

[5] The statute provides for a fine or imprisonment for up to 10 years for

> [w]ho[m]ever, 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; without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization.

18 U.S.C. § 1832(1)-(3) (1996). The statute also criminalizes any attempt or conspiracy to commit one of the above acts. *Id.* § 1832(4), (5). Organizations shall be fined not more than $5 million.

[6] *See, e.g.*, Verdict Form, United States v. Liew, No. 11-cr-00573, ECF No. 804 (N.D. Cal. Mar. 5, 2014); United States v. Chung, 659 F.3d 815 (9th Cir. 2011) (concerning a former Boeing engineer convicted under § 1831 for sending technological aircraft information to China); *see also* United States v. Hanjuan Jin, 833 F. Supp. 2d 977 (N.D. Ill. 2012) (dealing with a defendant charged under §§ 1831 and 1832 for downloading proprietary Motorola files and delivering the files to a Chinese company that developed telecommunications for the Chinese military; convicting defendant under § 1832, but not § 1831 because of insufficient evidence to show an intent to benefit China).

[7] *See, e.g.*, United States v. Agrawal, 726 F.3d 235 (2d Cir. 2013) (affirming a defendant's conviction under § 1832 for stealing computer code from Societe Generale in New York and attempting to sell it to another hedge fund in New York); United States v. Wen Chyu Liu, 716 F.3d 159 (5th Cir. 2013) (concerning a defendant convicted under § 1832 for attempting to sell information about Dow Chemical's manufacturing process to the Chinese); United States v. Williams, 526 F.3d 1312 (11th Cir. 2008) (regarding a disgruntled Coca-Cola employee convicted under § 1832 for attempting to sell trade secrets to Pepsi).

[8] Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. 110-403, 122 Stat. 4255-80 (2008).

[9] Press Release, U.S. Dep't of Justice, Department of Justice Joins in Launch of Administration's Strategic Plan on Intellectual Property Enforcement as Part of Ongoing IP Initiative (June 22, 2010), *available at* http://www.justice.gov/opa/pr/2010/June/10-ag-722.html.

[10] White House, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (February 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[11] White House, *2013 Joint Strategic Plan on Intellectual Property Enforcement* (June 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/2013-us-ipec-joint-strategic-plan.pdf.

[12] Based on the number of 18 U.S.C. §§ 1831, 1832 case opinions (published and unpublished) available in Lexis Advance. A similar method for studying the statistics of trade secret litigation was employed in David S. Almeling, et. al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 Gonz. L. Rev. 291 (2010).

  CARE ISSN 2330-6300

Interested in This Topic?

For further analysis of legal issues pertaining to corporate compliance, see Gregory P. Belanger et al., *Corporate Compliance* , Portfolio 103 in the *Corporate Practice Portfolio Series*, available at Bloomberg BNA. Go to http://www.bna.com/corporate-compliance-building-p17179892453/ for more information.

significant amounts of intellectual property.[13] The U.S. government appears to agree that such attacks were made—in May 2014, it indicted five Chinese military officials for allegedly hacking into U.S. businesses to steal trade secrets.[14] Many prosecutions have resulted in convictions and long prison sentences. For example, in March 2014, a California federal jury convicted a California businessman, his company and a former DuPont engineer of conspiring to steal DuPont's titanium dioxide trade secrets. The court sentenced the businessman to 15 years in prison.[15] In other cases, scientists and engineers have received sentences of five to seven years.[16]

Congress, too, has ramped up its efforts, passing two recent bills to strengthen the EEA. In December 2012, Congress broadened the scope of § 1832 to encompass activities with a looser nexus to interstate or foreign commerce.[17] A few weeks later, Congress enhanced the maximum penalties under § 1831 and required the U.S. Sentencing Commission to review sentencing guidelines for transmitting stolen trade secrets outside of the U.S.[18] The Senate is also considering a bipartisan bill to, among other items, establish a federal private right of action for trade secrets theft.[19]

Additional changes may follow. Even after signing the two EEA amendments near the end of 2012, the White House announced five action items for mitigating the theft of trade secrets—one of which was ''improving domestic legislation.''[20] In addition, the DOJ has proposed amendments to the Federal Rules of Criminal Procedure to relax the requirements to serve a criminal summons on a foreign organization, which have had special relevance in recent trade secrets cases.[21] And in

[13] Nedra Pickler, *White House Announces Anti-Theft Strategy*, BOSTON.COM (Feb. 20, 2013), http://www.bostonglobe.com/news/nation/2013/02/20/white-house-announces-anti-theft-trade-strategy/2YZPAnientoCJPDeKvHxnI/story.html

[14] *See* Indictment, United States v. Dong, et al., No. 2:14-cr-00118-CB, ECF No. 3 (W.D. Penn. May 1, 2014).

[15] Verdict Form, United States v. Liew, 4:11-cr-00573, ECF No. 804 (N.D. Cal. Mar. 5, 2014); Criminal Minute Order, United States v. Liew, ECF No.890 (N.D. Cal. July 10, 2014).

[16] *See, e.g.*, Judgment, United States v. Huang, No. 1:10-cr-00102, ECF No. 96 (S.D. Ind. Jan. 5, 2012) (Chinese scientist sentenced to 87 months in prison); Judgment, United States v. Yu, No. 2:09-cr-20304, ECF No. 37 (E.D. Mich. Apr. 13, 2011) (Chinese engineer sentenced to 70 months in prison); Judgment, United States v. Liu, No. 3:05-cr-00085, ECF No. 201 (M.D. La. Jan 19, 2012) (research scientist sentenced to 60 months in prison and $600,000 forfeiture).

[17] *See* Theft of Trade Secrets Clarification Act of 2012, Pub. L. 112-236, 126 Stat. 1627 (2012). Under the prior version of the law, § 1832 applied only when the trade secret was ''related to or included in a product that [was] produced for or placed in interstate or foreign commerce.'' In *United States v. Aleynikov*, relying on the then-narrower text of § 1832, the court ruled that Goldman Sachs's high frequency trading system (HFT) was neither ''produced for'' nor ''placed in'' interstate or foreign commerce because it was used internally by the company, and therefore the source code for the HFT was not protected by § 1832. 676 F.3d 71, 82 (2d Cir. 2012). Section 1832 now applies more broadly to any trade secret ''related to a product or service used in or intended for use in interstate or foreign commerce.'' The statute is broader because the product or service relating to the trade secret must only be *used in, or intended for use in*, interstate or foreign commerce, and need not be *produced for or placed in* interstate or foreign commerce.

[18] *See* Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, 126 Stat. 2442, 2443 (2012). The act increases the maximum monetary penalty from $500,000 to $5 million for individuals and for organizations, from $10 million to the higher of $10 million or three times the value of the stolen trade secret to the organization. Subsequently, in 2013, the Sentencing Guidelines were amended to increase the enhancement for a theft of trade secret to benefit a foreign government, instrumentality or agent from two levels to four levels, and to make any another transportation or transmission of a trade secret out of the U.S. a two-level enhancement. U.S. Sentencing Commission, Amendments to the Sentencing Guidelines 1-5 (Apr. 30, 2013), *available at* http://www.ussc.gov/sites/default/files/pdf/amendment-process/reader-friendly-amendments/20130430_RF_Amendments.pdf.

[19] *See* Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-113s2267is/pdf/BILLS-113s2267is.pdf; *see also* Trade Secrets Protection Act of 2014, H.R. 5233, 113th Cong. (2014), *available at* http://holding.house.gov/sites/holding.house.gov/files/documents/TSPA%20-%20HOLDNC_018_xml.pdf.

[20] White House, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* (February 2013), *available at* http://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[21] *See* Advisory Committee on Criminal Rules, Salt Lake City, Utah (Oct. 18, 2013), at 117-156, *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Agenda%20Books/Criminal/CR2013-10.pdf. The current text of the rule reads:

> A summons is served on an organization by delivering a copy to an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process. A copy must also be mailed to the organization's last known address within the district or to its principal place of business elsewhere in the United States.

Fed. R. Crim. P. 4(c)(3)(C). The ''mailing'' requirement arguably excludes from the reach of a federal criminal summons any foreign organization that does not have a presence in the U.S. Indeed, most federal courts that have addressed the issue—including in the trade secrets context—have held that such organizations fall beyond the reach of the rule. *See, e.g.*, United States v. Pangang Grp. Co., Ltd., 879 F. Supp. 2d 1052 (N.D. Cal. 2012) (in trade secrets case, granting motion to quash criminal service on a Chinese corporation); United States v. Alfred L. Wolff GmbH, No. 08-cr-417, 2011 BL 245710 (N.D. Ill. Sept. 26, 2011) (in case outside of trade secrets context, granting motion to quash criminal service on German and Chinese corporations); United States v. Johnson Matthey Plc, No. 2:06-CR-169 DB, 2007 BL 210078 (D. Utah Aug. 2, 2007) (in case outside of trade secrets context, granting motion to quash criminal service on English company). *But cf.* United States v. Kolon Indus., Inc., 926 F. Supp. 2d 794 (E.D. Va. 2013) (finding that mailing requirement need not always be satisfied to exercise jurisdiction over a foreign corporation, then granting in part and denying in part defendant's motion to quash criminal service on a Korean company on other grounds). In another trade secrets case, the question is pend-

February 2014, the nominee to head the DOJ's Criminal Division stated in confirmation hearings that she would take a ''very aggressive'' stance against intellectual property theft.[22]

II. Crimes by Agents: How Companies Can Be on the Hook

When considering its potential liability for trade secret theft, a company must consider the conduct of its agents, whether employees or independent contractors.[23] Under foundational principles of corporate criminal liability, a corporation can be criminally liable for illegal agent conduct when the agent acted (i) within the scope of the agent's employment and (ii) with intent to benefit the company.[24]

The scope of corporate criminal liability, under this standard, has been interpreted by some courts to be quite broad. Although courts sometimes use phrases from the civil context like ''actual or apparent authority'' to define the ''scope of employment,'' in the criminal context many courts have found it sufficient that the conduct falls within the agent's general line of work or relates to the agent's job responsibilities.[25] As the U.S. Court of Appeals for the Sixth Circuit explained in *Continental Baking Co. v. United States*, a corporation cannot insulate itself from liability by arguing that an agent was ''only 'authorized' to act legally.''[26]

The case law repeatedly illustrates this principle. In *United States v. Ionia Management. S.A.*, for example, a company's tanker crew, under the direction of lead engineers, unlawfully dumped into the ocean oily waste water and falsified records to conceal those acts. The U.S. Court of Appeals for the Second Circuit held that the crew acted within the scope of their employment in part because they had ''authority to maintain the engine room, discharge waste, and record relevant information.''[27]

Agents have been held to act within the scope of their employment even when they violate express company policies and supervisor instructions. For example, in *United States v. Hilton Hotels Corp.*,[28] the U.S. Court of Appeals for the Ninth Circuit upheld a hotel company's conviction under the Sherman Act. Hilton Hotels's purchasing agent, along with other hotels and businesses in a trade association, had threatened to boycott certain suppliers who did not make voluntary payments to the association. The court held Hilton responsible, even though such conduct was contrary to corporate policy and the hotel had twice told the agent not to engage in the conduct.

Similarly, two U.S. Court of Appeals for the Fourth Circuit decisions upheld corporate convictions for agent conduct that violated express company policies and express instructions. In one case, employee bid rigging in violation of the Sherman Act contravened employer antitrust policies.[29] In another, an employee violated corporate policies when he falsified logbooks to conceal unlawful conduct from the Food and Drug Administration.[30] Consistent with these cases, the RESTATEMENT (SECOND) OF AGENCY provides a hypothetical: say that ''[an employer] directs [a] salesman in selling guns, never to insert a cartridge while exhibiting a gun. [The] salesman[] does so. This act is within the scope of employment.''[31]

In dicta, however, courts have offered at least qualified hope for companies: A comprehensive, rigorously enforced compliance policy may cabin an agent's scope of employment.[32] For example, in *Ionia Management*,

---

ing before the court. United States v. Sinovel Wind Grp. Co. Ltd., No. 3:13-cr-84 (W.D. Wisc. filed Feb. 22, 2012).

[22] Kelly Knaub, *DOJ Criminal Division Pick Lays out Prosecution Priorities*, LAW360 (Feb. 11, 2014), http://www.law360.com/corporate/articles/509257?nl_pk=08ce3216-138a-4a73-8656-cafd3efc62f5&utm_source=newsletter&utm_medium=email&utm_campaign=corporate.

[23] An ''agent'' is anyone ''who is authorized to act for or in place of another.'' BLACK'S LAW DICTIONARY 15(c) (9th ed. 2009). A principal's right to control the agent is a critical factor in assessing whether an agency relationship exists. *See, e.g.*, First Am. Title Ins. Co. v. First Alliance Title. Inc., 718 F. Supp.2d 669, 681 (E.D. Va. 2010). ''Agents'' for whose conduct companies can be criminally liable can potentially include employees and independent contractors. *See, e.g.*, United States v. Parfait Powder Puff. Co., 163 F.2d 1008, 1009-10 (7th Cir. 1947) (upholding company conviction for acts of independent contractor); United States v. Singh, 518 F.3d 236, 251 n.20 (4th Cir. 2008) (stating in dicta that court finds compelling the argument for imputing corporate criminal liability not just for employees, but for independent contractors).

[24] *See* N.Y. Cent. & Hudson River R.R. Co. v. United States, 212 U.S. 481, 493-494 (1909) (''A corporation is held responsible for acts not within the agent's corporate powers strictly construed, but which the agent has assumed to perform for the corporation when employing the corporate powers actually authorized, and in such cases there need be no written authority under seal or vote of the corporation in order to constitute the agency or to authorize the act.''); *see also, e.g.*, United States v. Singh, 518 F.3d 236, 250 (4th Cir. 2008) (''[A] corporation is liable for the criminal acts of its employees and agents done within the scope of their employment with the intent to benefit the corporation.''); Memorandum from the Dep't of Justice, Paul J. McNulty, Deputy Att'y Gen., Principles of Federal Prosecution of Business Organizations (2006) (''To hold a corporation liable for [the illegal acts of its directors, officers, employees, and agents], the government must establish that the corporate agent's actions [i] were within the scope of his duties and [ii] were intended, at least in part, to benefit the corporation.''); *see generally* Joel M. Androphy, et al., *General Corporate Criminal Liability*, 60 TEX. B. J. 121, 122 (1997).

[25] See, e.g., *Singh*, 518 F.3d at 249 (''The appropriate ''scope of employment'' of such an employee or agent has been defined to include all those acts falling within the employee's or agent's general line of work, when they are motivated-at least in part-by an intent to benefit the corporate employer.''); United States v. Hilton Hotels Corp., 467 F.2d 1000, 1004 (9th Cir. 1972) (noting that district court instructed jury—and defendants did not challenge on appeal—that ''scope of employment'' means ''[on] the corporation's behalf in performance of the agent's general line of work,'' including ''not only that which has been authorized by the corporation, but also that which outsiders could reasonably assume the agent would have authority to do'').

[26] 281 F.2d 137, 150 (6th Cir. 1960).

[27] *See* United States v. Ionia Mgmt. S.A., 555 F.3d 303, 309 (2nd Cir. 2009).

[28] 467 F.2d 1000, 1007 (9th Cir. 1972).

[29] *See* United States v. Basic Constr. Co., 711 F.2d 570, 573 (4th Cir. 1983) (upholding company Sherman Act conviction).

[30] *See* United States v. Automated Med. Labs. (''*AML*''), 770 F.2d 399, 406 (4th Cir. 1985) (upholding company convictions for conspiracy and making and using false documents within the jurisdiction of a federal agency).

[31] United States v. Potter, 463 F.3d 9, 26 n.10 (1st Cir. 2006) (quoting RESTATEMENT (SECOND) OF AGENCY § 230, illus. 1 (1958)).

[32] Although courts have not yet addressed this question in the theft of trade secrets context, general principles of corpo-

  CARE ISSN 2330-6300

even though the Second Circuit rejected an argument that the government must prove in its case-in-chief that the company lacked sufficient policies to deter and detect misconduct, it approvingly noted the district court's jury instruction that ''a corporate compliance program may be relevant to whether an employee was acting in the scope of his employment.''[33]

Similarly, in *United States v. Potter*, the U.S. Court of Appeals for the First Circuit noted the potential relevance of corporate policies. In that case, a high-ranking employee had attempted to bribe the Speaker of the Rhode Island state House of Representatives. The court rejected the company's arguments that its president had instructed the high-ranking employee not to make the unlawful payments, noting that ''[e]ven a specific directive to an agent or employee or honest efforts to police such rules do not automatically free the company for the wrongful acts of agents.'' The court did, however, admit that this is a ''gray area,'' and that corporate policies, ''although not mechanically exculpatory of corporate liability, may well bear upon what is or is not within the scope of the agent's duties.''[34]

Likewise, the Ninth Circuit—which in *Hilton Hotels* upheld the corporate conviction even though the purchasing agent contravened corporate policies and instructions—offered helpful dicta in *United States v. Beusch*. The court upheld the conviction of a foreign currency exchange dealer for a corporate officer's violations of the Bank Secrecy Act. The dealer challenged a jury instruction stating that ''[a] corporation may be responsible for the acts of its agents done or made within the scope of its authority, even though the agent's conduct may be contrary to the corporation's actual instruction or contrary to the corporation's stated policies.'' The court held that this instruction did not improperly impose strict liability on the dealer for its agent's acts. In so holding, however, the court allowed for the possibility that rigorously *enforced* compliance programs could be relevant to corporate criminal liability, remarking:

> Merely stating or publishing [express] instructions and policies without diligently *enforcing* them is not enough to place the acts of an employee who violates them outside the scope of his employment . . . . It is a question of fact whether measures taken to enforce corporate policy in this area will adequately insulate the corporation against such acts, and we see no reason to disturb the jury's finding in this regard.[35]

III. Building Defenses With Stronger Controls

Courts have not yet analyzed vicarious corporate liability in a prosecution for corporate theft of trade secrets. Yet the potential implications are clear. Suppose, for instance, that one company employee on a research and development team unlawfully obtained a competitor's trade secret, in an effort to improve the company's own product. Or suppose that a company engaged a competitor's former employee as a consultant to the company's product development team and the consultant provided confidential information about the competitor. In either case, the government could argue that the agent's general line of work was to help the company develop a product and that any theft of trade secrets in furtherance of that goal was sufficiently related to those responsibilities to criminally bind the company. The government may reason that such an employee is no different than the employee in *Basic Construction Co.,* whose job was to submit bids and who criminally bound the company when he rigged those bids; or from the tanker crew in *Ionia Management,* who had authority to dump waste from the ship, and who criminally bound the company when it did so in an illegal way.

Companies concerned about potential criminal liability for trade secrets theft should therefore ask how they can mitigate their risk through internal policies and controls. Such policies may help prevent misconduct in the first instance, render any actual misconduct outside the ''scope of employment'' and favorably influence regulator charging decisions.

In the best-case scenario, sound policies and procedures can prevent misconduct altogether. A company might achieve this goal if it implements a detailed compliance policy that unequivocally prohibits misappropriation of third-party trade secrets, regularly trains its employees on policy requirements, rigorously monitors employee conduct for compliance with the policy and imposes meaningful penalties for violation (including termination of employment).

If misconduct occurs, courts appear open to the possibility that sufficiently strong policies can provide a back-end defense against company liability by narrowing the agent's scope of employment. This defense comports with the underlying justification for vicarious corporate liability, which, as the Court of Appeals for the District of Columbia explained, is intended to ''increase incentives for corporations to monitor and prevent illegal employee conduct.''[36] Companies that implement sufficiently strong controls seem properly incentivized and would not seem appropriate targets for prosecution on an agency theory.

Even if a strong compliance policy were completely unavailing in an actual trade secrets prosecution, it might still be highly relevant to regulator charging decisions. The U.S. Attorneys' Manual encourages prosecutors to consider ''the existence and effectiveness of the corporation's pre-existing compliance program.''[37] As a

rate criminal liability expressed in other criminal cases are instructive.

[33] 555 F.3d at 310 (2nd Cir. 2009).

[34] 463 F.3d 9, 25-26 (1st Cir. 2006).

[35] 596 F.2d 871, 877-78 (9th Cir. 1979) (emphasis added).

[36] *See* United States v. Sun-Diamond Growers of Calif., 138 F.3d 961, 971 (D.C. Cir. 1998). The Fourth Circuit offered what could be interpreted as an alternative justification in *United States v. Singh*: namely, that the ''rule prevents corporations from avoiding liability by simply contracting-out the more risky elements of their business.'' 518 F.3d 236, 251 n.20 (4th Cir. 2008). But even that justification is potentially consistent with, on one hand, punishing corporations who take a ''head in the sand'' approach to risky agent conduct, *cf.* United States v. Kozeny, 667 F.3d 122 (2d Cir. 2011) (upholding a defendant's conviction for violating FCPA under conscious avoidance charge when, knowing about pervasiveness of corruption in Azerbaijan and agent's bad reputation, defendant took steps to insulate himself from learning about bribery); and, on the other, permitting companies which take compliance seriously to assert that their compliance efforts cabin the scope of an agent's employment.

[37] *See* U.S. DEP'T OF JUSTICE, United States Attorney's Manual § 9-28.300 (1997); see also *id.* § 9-28.800 (noting that prosecutors should ''attempt to determine whether a corporation's compliance program is merely a 'paper program' or whether it was designed, implemented, reviewed, and revised,

result, in the trade secrets and other arenas, the U.S. enforcement landscape is replete with Deferred Prosecution Agreements,[38] Non-Prosecution Agreements[39] and even declinations (regulator ''walk-aways'')[40] that explicitly credit effective company compliance programs as an important contributing factor to the resolution.

Finally, a strong compliance program can also be relevant to sentencing, as the U.S. Sentencing Guidelines provide for a reduction in an organization's culpability score (and thus ultimate potential sentence) if the organization has a sufficiently rigorous compliance and ethics program and meets certain additional prerequisites.[41]

IV. The Time to Act Is Now

An international company with a mobile workforce must manage multiple risks. The trick is to assess compliance risk prospectively—to analyze today where enforcement authorities will likely come calling tomorrow. Where such risk exists, companies should assess where controls could be implemented or strengthened. Because of the ongoing perception that U.S. intellectual property is under assault both at home and abroad, trade secret theft prosecutions have risen quickly, and will almost certainly continue to increase. Companies should consider implementing controls now—and not be caught flat-footed when authorities knock at the door.

---

as appropriate, in an effective manner[;] . . . whether the corporation has provided for a staff sufficient to audit, document, analyze, and utilize the results of the corporation's compliance efforts[;] . . . [and] whether the corporation's employees are adequately informed about the compliance program and are convinced of the corporation's commitment to it'').

[38] *See, e.g.*, Press Release, U.S. Dep't of Justice, Johnson & Johnson Agrees to Pay $21.4 Million Criminal Penalty to Resolve Foreign Corrupt Practices Act and Oil for Food Investigations (Apr. 8, 2011), *available at* http://www.justice.gov/opa/pr/2011/April/11-crm-446.html (''Due to J&J's pre-existing compliance and ethics programs, extensive remediation, and improvement of its compliance systems and internal controls, as well as the enhanced compliance undertakings included in the agreement, J&J was not required to retain a corporate monitor . . . .'').

[39] *See, e.g.*, The Boeing Company Global Settlement Agreement: Hearing Before the S. Comm. on Armed Services, 109th Cong. 16 (2006) (statement of Paul McNulty, Deputy Attorney General), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-109shrg36090/pdf/CHRG-109shrg36090.pdf (in discussing non-prosecution agreement resolving allegations, among others, that Boeing obtained competitor's proprietary information, stating decision not to seek criminal charges was based partially on ''policies and procedures in place at the time of the conduct''); Letter from John M. Bales, U.S. Attorney for the Eastern District of Texas, to James T. Jacks, counsel for ADA-ES, Inc. and ADA Environmental Solutions LLC, Non-Prosecution Agreement (Sept. 9, 2013), *available at* http://www.sec.gov/Archives/edgar/data/1515156/000119312513365275/d596938dex991.htm (justifying non-prosecution agreement after investigation into alleged § 1832 and other offenses by company in part because ''prior to being notified of this investigation, ADA has employed general counsel, trained all of its employees in the appropriate use and protection of confidential information, provided yearly training to its employees, and provides compliance checks designed to ensure that proper safeguards are in place to protect confidential information'').

[40] *See, e.g.*, Press Release, U.S. Dep't of Justice, Former Morgan Stanley Director Pleads Guilty for Role in Evading Internal Controls Required by FCPA (Apr. 25, 2012), *available at* http://www.justice.gov/opa/pr/2012/April/12-crm-534.html (''After considering all the available facts and circumstances, including that Morgan Stanley constructed and maintained a system of internal controls, which provided reasonable assurances that its employees were not bribing government officials, the Department of Justice declined to bring any enforcement action against Morgan Stanley related to Peterson's conduct.'').

[41] *See* U.S. Sentencing Guidelines § 8C2.5(f) (providing for three-point reduction in culpability score if the organization had in place at the time of the offense a compliance and ethics program meeting the standards of § 8B2.1, so long as the organization did not unreasonably delay reporting the offense to the government and no high-level personnel within the organization participated in, condoned or were willfully ignorant of the offense).

   ISSN 2330-6300