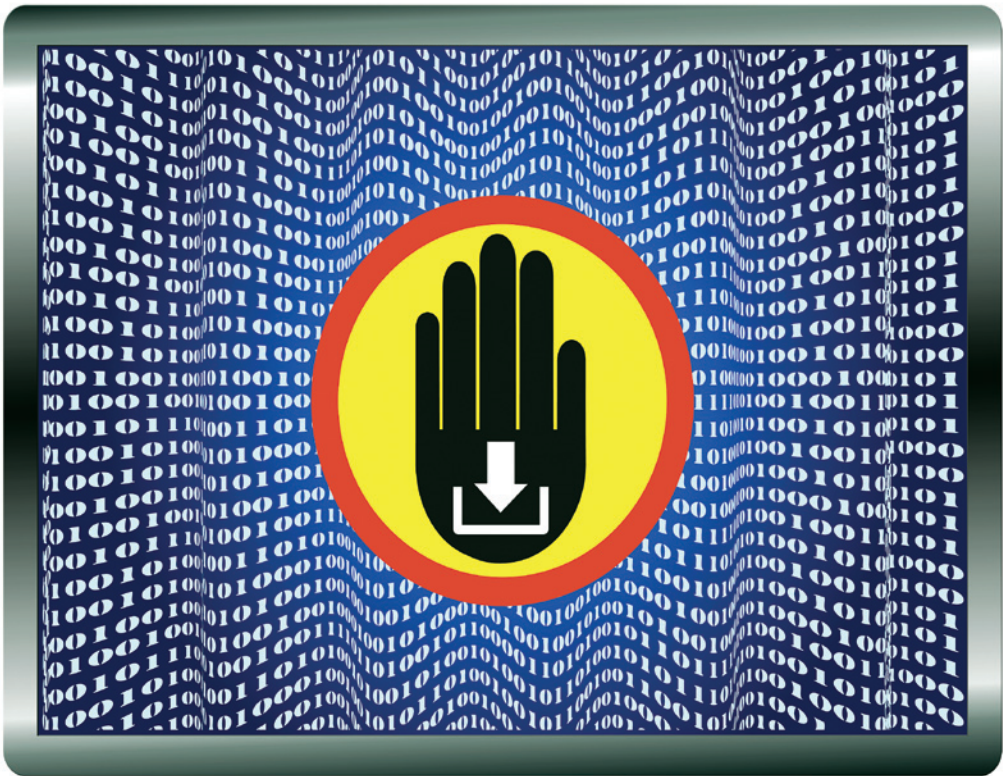
New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
White-Collar Crime
WWW.NYLJ.COM
MONDAY, SEPTEMBER 29, 2014

Cyber Crime And Trade Secret Protection: Strengthening Defenses

BY JONATHAN G. CEDARBAUM AND JANE LOVE



BIGSTOCK

Like almost every other kind of economic activity, theft of intellectual property is increasingly moving to the digital domain. The indictment by the Justice Department this spring of five members of China's military for economic espionage through sophisticated computer hacking threw onto the front pages an issue that has increasingly agitated not only the growing number of corporate victims but also enforcement and regulatory authorities in both the United States and the European Union: how to combat the theft of valuable IP by sophisticated, often government-sponsored, cyber intruders located around the globe.

The 2013 report of the blue ribbon Commission on Theft of American Intellectual Property, chaired by former Director of National Intelligence Admiral Dennis Blair and former U.S. Ambassador to China John Huntsman Report, put the value of stolen U.S. IP at a staggering $300 billion per year. The Obama Administration has responded with a "Strategy on Mitigating Theft of U.S. Trade Secrets," and Congress has responded by strengthening federal laws against trade secret misappropriation and by considering bills to strengthen further both criminal and civil remedies for trade secret theft, particularly by cyber thieves from overseas. In November 2013, the EU took a major step toward addressing the problem as well, with a draft directive on trade secret protection that would both strengthen EU laws against trade secret theft and bring them into closer alignment with U.S. law.

This article describes the dimensions of the problem of cyber theft of IP, explains how the problem has gained the attention of policymakers, and reviews the executive and legislative initiatives moving forward in the United States and the EU to combat the problem.

Dimensions of the Problem

In October 2011, the National Counterintelligence Executive—a consortium of U.S. intelligence agencies not known for seeking headlines—put out a report with a blunt title: "Foreign Spies Stealing U.S.

JONATHAN G. CEDARBAUM *is a partner at Wilmer Cutler Pickering Hale and Dorr in Washington, D.C.* JANE M. LOVE *is a partner at the firm's New York office.*

Economic Secrets in Cyberspace." The report declared that "[f]oreign economic collection and industrial espionage against the United States represent significant and growing threats to the nation's prosperity and security." Putting the cost in the billions of dollars, the report was unusual in identifying specific countries as particular sources of danger. "Chinese actors," the report observed, "are the world's most active and persistent perpetrators of economic espionage," while "Russia's intelligence services are conducting a range of activities to collection economic information and technology from U.S. targets."[1]

Since then, a growing number of studies—by government agencies, private commissions, think tanks, and congressional committees—have documented the increasing toll that cyber theft of trade secrets is taking on U.S. and European businesses. Last year, the Defense Security Service put out a special report on the targeting of U.S. defense contractors, noting the particular interest of foreign thieves in advanced microelectronics and aeronautics systems.[2] After an extensive investigation, the security firm Mandiant concluded that Chinese government-sponsored hackers were organized to steal "broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, and emails and contact lists from victim organizations' leadership."[3]

This spring, the Justice Department indicted some members of the groups identified by Mandiant, alleging that they had stolen, at various times, "trade secrets that would have been particularly beneficial to Chinese companies at the time they were stolen" and "sensitive, internal communications that would provide a competitor, or an adversary in litigation, with insight into the strategy and vulnerabilities" of a number of U.S. businesses, including Westinghouse Electric (Westinghouse), U.S. subsidiaries of SolarWorld AG, United States Steel, Allegheny Technologies, the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union and Alcoa.[4]

Limitations on Current Remedies

As that recent indictment indicates, there are federal criminal laws that may be put to use against foreign cyber thieves. State trade-secret misappropriation laws may also provide some degree of relief via civil remedies. And, for imported articles, the International Trade Commission's §337 process may be used to try to exclude goods based on stolen intellectual property. But each of these remedial possibilities has limitations that have led U.S. policymakers to look for ways to strengthen U.S. defenses against cyber theft of trade secrets.

The **International Trade Commission** is authorized to prevent "unfair methods of competition and unfair acts in the importation of articles . . . into the United States" if "the threat or effect" of the importation or sale is "to destroy or substantially injure an industry in the United States."

The most basic limitation of federal criminal laws is the constraint posed by limited investigatory and prosecutorial resources. The Economic Espionage Act (EEA), 18 U.S.C. §§1831-1832, makes it a federal crime to steal trade secrets "for the benefit of foreign entity" or for "pecuniary gain." The National Stolen Property Act (NSPA) prohibits "transport[ing], transmit[ing], transfer[ing] in interstate or foreign commerce any goods, wares, merchandise, securities or money … [k]nowing the same to have been … taken … by fraud." 18 U.S.C. §2314. But federal authorities can go after only a fraction of the growing number of cases of cyber theft of trade secrets, and these statutes do not provide for private rights of action.

Further limitations of the EEA and the NSPA, subsequently remedied in part, were revealed in the *Aleynikov* case involving theft of proprietary software code. Aleynikov, a former Goldman Sachs programmer, was prosecuted in the Southern District of New York for allegedly violating the EEA and NSPA by taking proprietary Goldman trading code with him when he moved to a competing firm. The Second Circuit held that Aleynikov's conviction under the EEA could not stand because the EEA is limited to acts done "with intent to convert a trade secret, that is related to or included in a product that is *produced or placed in interstate or foreign commerce*." The proprietary software code at issue did not qualify, according to the Second Circuit, because it had not been developed to be sold, i.e., "placed in interstate or foreign commerce." The court held Aleynikov's conviction under the NSPA could not stand because intangible property such as software code did not constitute "goods, wares, merchandise, securities or money," the kinds of property covered by the NSPA.[5]

The Computer Fraud and Abuse Act, 18 U.S.C. §1030, a federal statute that prohibits unauthorized access to computers for the purposes of taking information, does authorize private suits in some circumstances. But it requires a $5,000-loss threshold where a number of courts have limited the meaning of "loss" to "reasonable costs incurred to investigate, remedy, or prevent future occurrences of the unauthorized access" and "consequential damages … that arise from 'interruption of service'" due to the unauthorized access, thus excluding the value of the trade secrets that were stolen.[6]

State trade secret misappropriation causes of action also have weaknesses as tools against overseas cyber thieves. The Uniform Trade Secrets Act—adopted in some form by every state except New York and Massachusetts—prohibits "misappropriation" of trade secrets. Among other things, the UTSA proscribes: (1) "use of a trade secret of another"; (2) "without express or implied consent"; (3) "by a person who … at the time of … use, knew or had reason to know that his knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it." "Improper means" include "espionage through electronic or other means."[7]

But there are several challenges to pursuing a UTSA claim against state-supported cyber-espionage. First, relying on these state-law claims may raise difficult questions concerning the extraterritorial reach of state law. Second, state courts offer less broad discovery than federal courts.

The International Trade Commission (ITC) affords another possible forum for victims of foreign cyber thieves. The ITC is authorized to prevent "unfair methods of competition and unfair acts in the importation of articles … into the United States" if "the threat or effect" of the importation or sale is "to destroy or substantially injure an industry in the United States." If these requirements are met, the ITC can "complete[ly] exclu[de]" the offending company's product

from the United States. The ITC's jurisdiction extends to products that incorporate misappropriated trade secrets where the theft took place overseas.[8]

But this remedy also has shortcomings. First, the ITC's remedial power is limited to imported articles. Second, the ITC can only provide the equivalent of forward-looking injunctive relief. It cannot order an award of damages.

U.S. Regulatory and Legislative Responses

Recognizing these limitations in the current regime of legal remedies for victims of trade secret theft, both the Executive Branch and Congress have offered some reform proposals. Last year, the Administration issued a "Strategy on Mitigating Theft of U.S. Trade Secrets" and a "Joint Strategic Plan on IP Enforcement." They call for improving protections against cyber espionage through new trade agreements and through "naming and shaming" countries that don't take action through the issuance of special reports under §301 of the Trade Act. They urge enhanced criminal prosecutions and amendment of the EEA to fix the loophole revealed in *Aleynikov*. That last recommendation was accomplished in January of this year. But the others remain unachieved and of uncertain effectiveness.

Congress has also stepped in, with bipartisan proposals for strengthened criminal and civil remedies. In May, the Senate Judiciary Committee's Subcommittee on Crime and Terrorism held a hearing on "Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?" The subcommittee's chairman, Sen. Sheldon Whitehouse (D-R.I.), and Sen. Lindsey Graham (R-S.C.), used the occasion to float a draft bill that would amend the EEA to make it easier to go after foreign-government-sponsored hackers by clarifying that it covers cyber intrusions from abroad, specify that it encompasses theft of negotiating positions, make violation of the EEA a RICO predicate, and permit intervention by injured private parties.[9]

At nearly the same time, Sens. Carl Levin (D-Mich.), John McCain (R-Ariz.), Jay Rockefeller (D-W. Va.) and Tom Coburn (R-Okla.) re-introduced their Deter Cyber Theft Act (S. 2384). The bill would require the Director of National Intelligence to publish an annual report identifying countries engaging in computer espionage targeting valuable information of U.S. companies; a priority watch list of the foreign countries that are the most egregious offenders; U.S. technologies and information targeted or stolen by foreign cyber espionage; goods and services produced using stolen information; and government actions to combat computer espionage. The bill would also authorize the Treasury Department to freeze the assets of individuals or companies that benefit from theft of U.S. technology or other commercial information.

These bills rely principally on government action to go after cyber thieves. Two other bills would give affected companies the ability to go to federal court themselves. Sen. Jeff Flake's (R-Ariz.) Future of American Innovation and Research (FAIR) Act (S. 1770) would create a federal civil cause of action for trade secret misappropriation against defendants located outside the territorial jurisdiction of the United States or acting on behalf of, or for the benefit of, a person outside the territorial jurisdiction of the United States, that is, a foreign government or corporation. The bill expressly provides that actions may arise from extraterritorial conduct "if the conduct, either by itself or in combination with conduct within the territorial jurisdiction of the U.S., causes or is reasonably anticipated to cause, an injury" either within U.S. territorial jurisdiction or to a U.S. person. And the bill provides a process for promptly seeking an order of seizure against goods used in or gained through the cyber theft.

Sens. Chris Coons (D-Del.) and Orin Hatch (R-Ut.) have introduced a similar bill (S. 2267). Building on the criminal prohibitions in the EEA, it would authorize federal civil suits on largely the same grounds. Like the FAIR Act, the Coons/Hatch bill would also authorize seizure orders and would have extraterritorial reach, though somewhat more limited, circumstances.

Despite the bipartisan backing for many of these legislative proposals, their prospects remain uncertain in a Congress that seems unable to move forward on nearly any legislative business of substance.

Developments in the European Union

The United States is not alone in recognizing cyber espionage and trade secret theft as growing economic threats. Last November, the European Commission put out a draft directive designed to strengthen EU laws against trade secret misappropriation. The draft directive notes that "[i]nnovative businesses are increasingly exposed to dishonest practices aiming at misappropriating trade secrets, such as theft, unauthorised copying, economic espionage, breach of confidentiality requirements, whether from within or from outside of the Union." The draft directive also expressed concern about lack of adequate legal protection for trade secrets and variation in trade secret laws among member states discouraging cross-border research and development.[10]

If approved, the directive would work a major change in trade secret protection in Europe. By providing a uniform definition of trade secrets and trade secret misappropriation, it would bring European law much more closely into alignment with U.S. law. It would authorize damages and prompt injunctive relief, thus making Europe's trade secret laws much more effective tools for victims of cyber espionage.

Time for Action

As cyber thieves become more sophisticated, the problem of cyber theft of trade secrets and other IP is likely to grow. Policymakers on both sides of the Atlantic have recognized the problem, but more needs to be done to turn proposals into effective tools in the hands of victims and supportive governments.

•••••••••••••●●•••••••••••••

1. Office of the National Counterintelligence Executive, Foreign Spies Stealing US Economic Secrets in Cyberspace 1 (1991).
2. Defense Security Service, Targeting U.S. Technologies, A Trend Analysis of Reporting From Defense Industry (2012).
3. Mandiant, Exposing One of China's Cyber Espionage Units 3 (2013).
4. Press Release, DOJ, Office of Public Affairs, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014).
5. *United States v. Aleynikov*, 676 F.3d 71 (2d Cir. Apr. 11, 2012).
6. 18 U.S.C. §1030(a)(2)(C), (b), (g); see also id. §1030(c)(4)(a)(i)(I).
7. National Conference of Commissioners on Uniform State Laws, Uniform Trade Secrets Act with 1985 Amendments §1(2)(ii)(B)(I) (1985), available at http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf; see also id. §§2-3 (injunctive relief and damages provisions).
8. See 19 U.S.C. §337(a)(1)(A); see Raymond T. Nimmer & Holly K. Towle, The Law of Electronic Commercial Transactions ¶ 3.05[2][A] (rev. 2013) (noting several courts have expressly held the term does not encompass "revenue loss due to a competitor's use of … trade secrets").
9. The draft bill and explanatory materials are available at http://www.whitehouse.senate.gov/news/release/whitehouse-and-graham-working-to-crack-down-on-economic-espionage.
10. The draft directive is available at http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/131128_proposal_en.pdf.