Cyberespionage and Civil Suits

Law360, New York (July14, 2014, 10:11 AM ET) --

James Dowd

Gregory Lantier

Thomas Sprankling

Five members of the "Comment Crew" — a group of Chinese hackers who operate under pseudonyms like UglyGorilla and KandyGoo — were indicted by a grand jury in May 2014, accused of being employed by the Chinese military to steal trade secrets from U.S. companies.[1] The indictments are the first of their kind, and reportedly just the tip of the iceberg.[2]

Although the media's focus has been on criminal punishment for the hackers, civil remedies are also available to protect firms against cyberespionage. The allegations against the Comment Crew members —for example, that they stole "proprietary and confidential technical and design specifications for pipes, pipe supports, and pipe routing for … nuclear power plants" from the Pennsylvania-based Westinghouse Electric Company's computers while Westinghouse was "negotiating with a Chinese company" to build four plants in China[3] — provide a test case for how a company might pursue private civil litigation against competitors that receive trade secrets from a government actor, both under existing state and federal law, as well as two pieces of legislation pending in Congress — the Defend Trade Secrets Act of 2014 ("DTSA") and the Future of American Innovation and Research Act of 2013 ("FAIR").[4]

Existing Civil Remedies

State Law Remedies

Every state except New York and Massachusetts has adopted some variation of the Uniform Trade Secrets Act,[5] which 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."[6] A "trade secret" is defined as "information … that: (i) derives independent economic value … from not being generally known … [or] readily ascertainable by proper means … and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[7] The UTSA does not list "'[a] complete catalogue'" of what constitutes "improper means," but this term does include "espionage through electronic or other means."[8] Within this framework, the laws implementing the UTSA differ from state-to-state. As a result, the precise elements of a trade secrets claim vary depending on the jurisdiction in which a suit is brought.[9]

If the Comment Crew gave stolen Westinghouse specifications to the company's putative Chinese competitor, who then used them to build a power plant or gain a negotiating advantage, the Chinese company could face civil liability under the UTSA. The specifications should qualify as trade secrets because they are "confidential," stored on protected

Westinghouse computers not accessible by the general public, and derive independent economic value from not being generally known. Among other indicia of value, the cybersecurity breach would allow Westinghouse's "competitor to build a plant … without incurring significant research and development costs."[10] Moreover, the hackers purportedly "gained unauthorized access to Westinghouse's computers" to steal the plans, indicating both that the plans were gathered via improper means, and that the Chinese competitor could not reasonably claim consent. [11] And it would be difficult for a Chinese company that gained access to Westinghouse's specifications while negotiating with Westinghouse to claim that it did not — at least — have "reason to know" the specifications were stolen.

There are challenges to pursuing a state court UTSA claim against state-supported cyber-espionage, however, including the questionable extraterritorial application of state law. To provide a remedy, the state court would either (1) have to apply state trade secret law to acts of a foreign state actor undertaken beyond the U.S. border;[12] or (2) construe the cybersecurity breach of a computer physically located within the state as sufficient to establish jurisdiction over the foreign-company beneficiary of the misappropriation. It is also possible that an overseas company that benefits from trade secrets misappropriated by its government may raise other jurisdictional arguments, such as foreign sovereign immunity.[13] To date, however, trade secret misappropriation claims against state-owned companies have been held to fall within the commercial-activity exception to the foreign sovereign immunity doctrine.[14]

State-law claims also have several inherent disadvantages. It may not be possible to bring a state-law claim in federal court, for example, thereby sacrificing federal court advantages such as broad discovery and having the same judge at every stage of the case.[15] And the absence of a truly uniform trade secrets statute across the states means that a would-be plaintiff might be forced to litigate under a less advantageous statute depending on where the misappropriation occurred.

Federal Law Remedies

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is targeted at individuals and entities who access or use a computer without proper permission.[16] It is the closest, currently existing equivalent to a federal civil cause of action for cyberespionage. Although there are several ways to pursue a CFAA action, the most likely application to the Westinghouse facts would require a demonstration that the Chinese competitor: (1) "conspire[d]" with the Comment Crew; (2) to "intentionally access[] a computer without authorization"; (3) which resulted in obtaining "information"; (4) from a "protected computer" (e.g., a computer "used in or affecting interstate or foreign commerce or communication"); and (5) "causing loss" adding up to at least $5,000 "during any 1-year period."[17] Notably, the CFAA defines "loss" as "any reasonable cost to any victim … and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[18] Some district courts have construed this definition as limited only to (1) "reasonable costs incurred to investigate, remedy, or prevent future occurrences of the unauthorized access; and (2) consequential damages … that arise from 'interruption of service'" due to the unauthorized access.[19]

Westinghouse's Chinese competitor could potentially be liable under the CFAA based upon the allegations set forth above. The Comment Crew clearly did not have authorization to access Westinghouse's computers, and Westinghouse's confidential nuclear power plant specifications certainly constitute "information." Given the importance of the specifications, it is reasonable to conclude that more than $5,000 was spent investigating the theft. Moreover, the computers were presumably connected to the Internet and thus "used in … interstate or foreign commerce."[20]

But the CFAA also has significant limitations that may make it an inadequate remedy, particularly in jurisdictions that limit recovery under the statute. One challenge in bringing this claim, for example, would be proving the "conspiracy." Using existing discovery devices, one can expect great difficulty in obtaining evidence that a foreign state's agents (here, the Comment Crew) had a pre-existing agreement with Westinghouse's foreign competitor to steal a trade secret (the Westinghouse specifications).[21] Because there is little precedent addressing the CFAA's conspiracy liability provision, it is possible that a court might decline to read the act to apply to co-conspirators who did not personally access Westinghouse's computers — especially if the conspiracy occurred entirely outside the United States.[22] Moreover, a plaintiff may not be fully compensated for its losses "caused by trade secret misappropriation" because courts recently have limited damages to harm "caused by an interruption in [the plaintiff's] computer operations or by loss of its computer files."[23]

Section 337 Trade Secrets Action

The International Trade Commission provides another existing avenue to remedy harm caused by cyberespionage. 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."[24] If this requirement is met, the ITC can "complete[ly] exclu[de]" the offending company's product from the United States.[25] Because the ITC's jurisdiction extends to products that incorporate misappropriated trade secrets where the theft took place overseas,[26] the ITC is a seemingly promising forum.

But this remedy is also limited. Because the ITC's remedial power is limited to imported articles, an ITC exclusion order may provide no relief to a company like Westinghouse — whose specifications were presumably stolen for the purpose of building power plants abroad (or to gain a negotiating advantage), and not to import competing articles. Also, under the ITC's authorizing statute, 19 U.S.C. § 1337, damages are not available.[27] The ITC is limited to granting injunctive relief (an exclusion order), and it is then left to the U.S. Customs Service to catch excluded articles at the border. Finally, demonstrating that an imported article threatens to "substantially injure an industry in the United States" is a fact-intensive question resolved by considering a number of factors that may not be met in every case.[28]

Pending Legislation

There are presently two bills pending in Congress, either of which would overcome many of the shortcomings of existing state and federal state remedies by creating an improved federal cause of action against foreign trade secret thieves. The DTSA appends a civil cause of action onto the existing Economic Espionage Act ("EEA"),[29] which currently imposes

criminal penalties for "economic espionage" and "theft of trade secrets."[30] The DTSA would essentially adopt the UTSA elements and definitions as a federal cause of action, while adding a requirement that the misappropriated trade secret be "related to a product or service used in, or intended for use in, interstate or foreign commerce."[31] This requirement would be readily met in a case like Westinghouse's, or likely by any large company with business extending across state lines. The DTSA also permits "an owner of a trade secret … aggrieved" by a violation of the existing criminal provisions to bring a civil suit.[32]

The FAIR creates a standalone civil cause of action that also largely adopts the UTSA elements and definitions.[33] In contrast to the DTSA, the FAIR's focus is on trade secret theft that is external to the United States: it permits suit to be brought only when the wrongdoer was "located outside" or acting on "behalf of, or for the benefit of, a person located outside" "the territorial jurisdiction of the United States."[34] This requirement would also be easily met by Westinghouse or any other company whose trade secrets are stolen by a foreign government to give to a local competitor.

Both bills would, among other things:

• Create uniformity across the states in terms of the elements required to establish a trade secrets case;

• Capture conduct like the Comment Crew's, overcoming the potential geographical limitations in the various state versions of the UTSA;[35]

• Permit litigants to avoid the difficulty of trying to prove conspiracy under the CFAA and risking that a court may conclude that the CFAA's civil provision does not apply to mere co-conspirators; and

• Permit the injured company to receive damages and thus provide a remedy against trade secret misappropriation that does not result in a product being imported into the United States, unlike a suit filed before the ITC.

Conclusion

Although existing laws support a civil suit against a foreign competitor who misuses trade secrets stolen by its government, each currently available remedy has its own shortcomings. The proposed DTSA and FAIR bills would provide superior remedies. If either becomes law, companies like Westinghouse would have a solid legal tool to address the economic harm caused by government-sponsored theft of their trade secrets.

—By James M. Dowd, Gregory H. Lantier and Thomas G. Sprankling, WilmerHale

James Dowd is a partner in WilmerHale's Los Angeles office. Gregory Lantier is a partner and Thomas Sprankling is an associate in the firm's Washington, D.C., office.

[1] Michael S. Schmidt & David E. Sanger, 5 in China Army Face U.S. Charges of Cyberattacks, N.Y. Times, May 19, 2014, http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html?_r=0.

[2] Press Release, Department of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), available at http://www.justice.gov/opa/pr/2014/May/14-ag-528.html.

[3] Indictment ¶ 2, United States v. Dong, No. 14-118 (W.D. Pa. May 1, 2014), available at http://www.justice.gov/iso/opa/resources/512201451913235846194 9.pdf.

[4] See S. 2267, 113th Cong. (2014), available at http://coons.senate.gov/download/defend-trade-secrets-act (DTSA); S. 1770, 113th Cong. (2013), available at http://www.gpo.gov/fdsys/pkg/BILLS-113s1770is/pdf/BILLS-113s1770is.pdf (FAIR).

[5] David W. Quinto & Stuart H. Singer, Trade Secrets: Law & Practice § 1.01 (2014). Massachusetts prohibits trade secret misappropriation via a statute not modeled after the UTSA; New York has developed anti-misappropriation common law. Id. § 1.01 & n.6.

[6] 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).

[7] Id. § 1(4).

[8] Id. § 1(1) & cmt.

[9] See Quinto & Singer, Trade Secrets § 2.03 (comparing elements required by various states). See generally id. app. A ("Overview of Trade Secret Laws of Selected States").

[10] Dong Indictment ¶ 21.

[11] Id.

[12] Cf. Global Reinsurance Corp. U.S. Branch v. Equitas Ltd., 969 N.E.2d 187, 194-196 (N.Y. 2012).

[13] See 28 U.S.C. § 1604.

[14] E.g., BP Chemicals Ltd. v. Jiangsu SOPO Corp., 420 F.3d 810, 818 (8th Cir. 2005); Gould, Inc. v. Mitsui Mining & Smelting Co., 947 F.2d 218, 223 (6th Cir. 1991); see also 28 U.S.C. § 1605(a)(2) (no immunity when "the action is based," inter alia, "upon an act outside the territory of the United States in connection with a commercial activity of the foreign state elsewhere and that act causes a direct effect in the United States").

[15] See Bill Donahue, Federal Trade Secrets Law Earns High Marks From Attys, Law360, May 1, 2014, http://www.law360.com/articles/533792/federal-trade-secrets-law-earns-high-marks-from-attys (discussing advantages of federalizing trade secret law); see also Quinto & Singer, Trade Secrets §2.04[1] (discussing basic advantages of proceeding in federal court, such as "higher caliber" judges who "are frequently more willing to grant summary judgment than their state counterparts").

[16] See 18 U.S.C. § 1030(a)-(b); see also id. § 1030(g) (providing civil cause of action). The CFAA probably applies extraterritorially, although apparently only one reported decision has squarely considered the issue. See United States v. Ivanov, 175 F. Supp. 2d 367, 374-375 (D. Conn 2001).

[17] 18 U.S.C. § 1030(a)(2)(C), (b), (g); see also id. § 1030(c)(4)(a)(i)(I).

[18] Id. § 1030(e)(11).

[19] 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").

[20] See id. ¶ 3.05[2][B] (noting that the term "protected computer" "essentially includes any computer connected to the Internet").

[21] See generally Charles Doyle, Cong. Research Serv., R41223, Federal Conspiracy Law: A Brief Overview (2010), available at http://www.fas.org/sgp/crs/misc/R41223.pdf.

[22] Cf. Trademotion, LLC v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1293 (M.D. Fla. 2012). But see Flynn v. Liner Grode Stein Yankelevitz Sunshine Regenstreif & Taylor LLP, 2011 WL 2847712, at *3 (D. Nev. July 15, 2011) (noting in context of a civil suit that the CFAA's "plain language sets forth who is liable under § 1030: a primary violator, a person who attempts a primary violation, and a co-conspirator of a primary violator").

[23] See Quinto & Singer, Trade Secrets § 2.04[3][b] & n.184.

[24] See 19 U.S.C. § 337(a)(1)(A).

[25] See Quinto & Singer, Trade Secrets § 2.04[4]; see also 19 U.S.C. § 1337(d).

[26] TianRui Grp. Co. v. ITC, 661 F.3d 1322, 1337 (Fed. Cir. 2011).

[27] See Quinto & Singer, Trade Secrets § 2.04[4].

[28] See id. (listing factors and noting "there is no bright-line test").

[29] See generally 18 U.S.C. §§ 1831-1839.

[30] Id. §§ 1831-1832.

[31] S. 2667, § 2.

[32] See id. While section 1832(a) in particular may provide an alternate vehicle for a civil suit under these circumstances, it requires the plaintiff to show a higher level of awareness by the defendant company that the trade secret was stolen or otherwise misappropriated than is required by the UTSA language (knowledge and "intent", rather than "reason to know"), which could pose difficult evidentiary issues at trial.

[33] See S. 1770 § 2. Most notably, FAIR does not adopt the UTSA provision imposing liability on a person (1) who discloses or uses a trade secret of another, (2) "without express or implied consent," and (3) "before a material change of his [or her] position," (4) "knew or had reason to know that [i] it was a trade secret and [ii] that knowledge of it had been acquired by accident or mistake." See UTSA § 1(2)(ii)(C).

[34] S. 1770, § 3(a).

[35] The FAIR expressly states that it does. See id. § 3(c). Given the DTSA's text and structure, it seems likely to apply extraterritorially as well.