Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

Trade Secrets

The authors run down the significant developments in trade secrets law in 2015 and what to watch for in 2016. There is growing concern from the U.S. government and companies about threats to trade secrets.

2015 Trade Secrets Litigation Round-Up



BY JASON C. SCHWARTZ, GRETA B. WILLIAMS, BENJAMIN J. CASSADY AND MIA DONNELLY

Over the past year, there have been a number of significant developments in trade secrets law, amidst growing concern from the U.S. government and U.S. companies about the serious harm caused by trade secret theft at the hands of competitors, former employees and foreign actors.

The Obama administration announced a robust sanctions program that authorizes penalties on foreign individuals who engage in cyberattacks or commercial espionage. The administration also worked with China to protect trade secrets; at the urging of the U.S. government, China arrested a number of hackers who allegedly stole trade secrets from U.S. companies for the benefit of Chinese companies. At the same time, the U.S. Department of Justice continued to prosecute a number of Chinese actors for trade secret theft and cyber-espionage.

Jason C. Schwartz is a litigation partner in the Washington, D.C., office of Gibson, Dunn & Crutcher and a member of the firm's executive committee; his practice includes litigating high-stakes trade secrets, non-compete and employment disputes. Greta B. Williams, Benjamin J. Cassady and Mia Donnelly are litigation associates in the firm's Washington, D.C. office.

In the legislative realm, Congress renewed efforts to grant federal courts jurisdiction over claims of misappropriation of trade secrets used in interstate and foreign commerce. Although similar efforts failed in 2014, sponsors of the legislation are hopeful that this latest effort will prove more successful, pointing to broad bipartisan support.

On the civil side, state and federal courts considered a number of substantive and procedural issues with respect to trade secret claims, including the preemptive effect of the Uniform Trade Secrets Act (UTSA), the types of information that can qualify as a trade secret, and the importance of identifying trade secrets with particularity. 2015 also saw some significant developments in a number of high-profile trade secrets disputes. For instance, Nike reached a settlement with

three former designers it had sued in a trade secrets case that was discussed in last year's *Trade Secrets Litigation Round-Up*.[1] And in a stunning turn of events, Texas-based oil company Moncrief Oil International dropped its billion-dollar trade secrets case against a Russian gas company mid-trial after the defense accused Moncrief of fabricating key evidence.

We discuss these and other developments in trade secrets law in 2015 below.

Legislative & Criminal Law Developments

I. Executive Actions

Over the past year, the Obama administration has shown a willingness and desire to protect trade secrets belonging to American companies, particularly from attacks by those outside of the United States. In January 2015, it announced extensive cybersecurity and privacy initiatives.[2] Then, President Obama signed an executive order on April 1, 2015 declaring a national emergency after finding that ''the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by persons located . . . outside the United States constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.''[3] The executive order established a sanctions program imposing penalties on foreign individuals who engage in cyberattacks or commercial espionage—for example, freezing their financial assets and barring commercial transactions with them.[4] Although the administration has not yet issued sanctions under the new program, it has reportedly considered sanctions against Russia and China.[5]

The Obama administration also worked with other countries to protect trade secrets on an international scale. In September, President Obama and President Xi Jinping of China vowed that neither government would conduct or condone economic espionage in cyberspace, pledging not to ''knowingly support cyber-enabled theft of intellectual property, including trade secrets.''[6] Prior to the visit, the Chinese government, at the urging of the U.S. government, arrested a number of hackers whom U.S. officials identified ''as having stolen commercial secrets from U.S. firms to be sold or passed along to Chinese state-run companies.''[7] Despite this apparent progress, however, reports surfaced in October that Chinese hackers had ''targeted at least seven U.S. companies'' in the three weeks after Xi made his promise.[8] John Carlin, the Obama administration's top national security adviser, later said that the U.S. could consider criminal charges or sanctions against China if the attacks continue.[9] In November, the G20 leaders similarly pledged ''to neither conduct nor support the online theft of intellectual property and trade secrets.''[10]

II. Statutory Developments

Federal Legislation

Last year, as noted in the *2014 Trade Secrets Litigation Round-Up*, both the House of Representatives and Senate introduced bipartisan amendments to the Economic Espionage Act that would create a federal civil cause of action for the misappropriation of trade secrets related to products used in interstate commerce.[11] Although the Senate Judiciary Subcommittee on Crime and Terrorism held a hearing on the Senate bill, and the House Judiciary Committee reported its bill by voice vote, neither bill ultimately passed.[12]

In 2015, however, members of the House and Senate renewed efforts to provide federal jurisdiction for the theft of trade secrets by introducing identical bills known as the Defend Trade Secrets Act of 2015 (''DTSA'').[13] The bills were introduced in July by Sen. Orrin Hatch (R-UT) and Sen. Chris Coons (D-DE), and Rep. Doug Collins (R-GA), respectively.[14] Like the Sen-

---

[1] *See* Jason C. Schwartz, Alexander H. Southwell, Martin A. Hewett, Andrea R. Lucas and Christopher Smith, ''2014 Trade Secrets Litigation Round-Up,'' 89 Bloomberg BNA'a Patent, Trademark & Copyright Journal 627, (89 PTCJ 627, 1/09/2015).

[2] *See* Press Release, White House Office of the Press Secretary, Securing Cyberspace—President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015), https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.

[3] Exec. Order No. 13694, 80 FR 18077, 18077 (2015).

[4] *See id.*; *see also* Ellen Nakashima, *U.S. Establishes Sanctions Program to Combat Cyberattacks, Cyberspying*, WASH. POST (April 2, 2015), https://www.washingtonpost.com/world/national-security/us-to-establish-sanctions-program-to-combat-cyberattacks-cyberspying/2015/03/31/7f563474-d7dc-11e4-ba28-f2a685dc7f89_story.html.

[5] Arshad Mohammed, Matt Spetalnick & Mark Hosenball, *Exclusive: U.S. Weighs Sanctioning Russia As Well As China in Cyber Attacks*, REUTERS (Sept. 1, 2015), http://www.reuters.com/article/us-usa-cybersecurity-russia-exclusive-idUSKCN0R12FE20150901#0w6Poc3gBj8jWPBR.97.

[6] Ellen Nakashima & Steven Mufson, *U.S., China Vow Not to Engage in Economic Cyberespionage*, WASH. POST (Sept. 25, 2015), https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

[7] Ellen Nakashima & Adam Goldman, *In a First, Chinese Hackers are Arrested at the Behest of the U.S. Government*, WASH. POST (Oct. 9, 2015), https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html.

[8] Ellen Nakashima, *China Still Trying to Hack U.S. Firms Despite Xi's Vow to Refrain, Analysts Say*, WASH. POST (Oct. 19, 2015), https://www.washingtonpost.com/world/national-security/china-still-trying-to-hack-us-firms-despite-xis-vow-to-refrain-analysts-say/2015/10/18/d9a923fe-75a8-11e5-b9c1-f03c48c96ac2_story.html.

[9] Tami Abdollah, *Chinese Hackers Could Face U.S. Criminal Charges Says DOJ Official*, PBS NEWSHOUR (Nov. 10, 2015), http://www.pbs.org/newshour/rundown/chinese-hackers-face-u-s-criminal-charges-says-doj-official/.

[10] Katie Bo Williams, *G20 Nations Reach Anti-Hacking Pledge*, THE HILL (Nov. 17, 2015), http://thehill.com/policy/cybersecurity/260414-g20-nations-reach-anti-hacking-pledge.

[11] *See supra* note 1.

[12] *See* 160 CONG. REC. S6125 (daily ed. Nov. 19, 2014) (statement of Sen. Hatch).

[13] Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. (2015).

[14] *Id.*

  PTCJ ISSN 0148-7965

ate bill with the same name introduced in 2014,[15] the Defend Trade Secrets Act of 2015 provides a private civil right of action for misappropriation of trade secrets related to products used in interstate or foreign commerce.[16] The bills also authorize courts to issue a civil seizure order in limited circumstances—a remedy that is not currently provided by any state trade secret law.[17] And, the bills provide remedies for civil actions in the form of injunctions, damages, punitive damages, and attorney's fees.[18]

Although many of the provisions in this year's bills are similar to those in last year's, there are some notable differences. First, the 2015 DTSA civil seizure provision is narrower: it is no longer available for the preservation of evidence; the applicant must show that the information misappropriated is a trade secret; the order must provide for the narrowest seizure necessary; and a hearing must be held if a seizure order is issued.[19] In addition, although the 2015 DTSA still provides for injunctive relief, any injunction would not prevent a person from accepting employment under conditions that avoid actual or threatened misappropriation.[20]

On December 2, 2015, the Senate Judiciary Committee held a hearing on the DTSA. Supporters of the legislation pointed to ''the need for assured, direct access to federal court,'' ''the need to reduce the risk of further trade secret dissemination or the destruction of evidence,''[21] the ineffectiveness of ''the existing patchwork of state laws'' for companies who operate across state and international borders, and the importance of a civil remedy.[22] Opponents of the legislation[23] argued that trade secret litigation will become more expensive under the DTSA, and that it would be particularly expensive for start-up companies and small businesses that are sued for trade secret misappropriation and forced to defend themselves, often when there are no legitimate trade secrets or little or no evidence of misappropriation.''[24] After the hearing, Senator Hatch remarked that the bills have overwhelming bipartisan support and have ''garnered endorsements from a wide-array of industry stakeholders who know firsthand the economic losses caused by trade secret theft.''[25] To date, however, there has been no vote on either the House or Senate version of the DTSA.[26]

State Legislative Developments

All but three states have now adopted the Uniform Trade Secrets Act. In 2015, state legislatures in New York and Massachusetts both introduced legislation to adopt the UTSA.[27] Neither bill has been subject to a vote.[28] If these bills pass, North Carolina will be the only state that has not adopted the Uniform Trade Secrets Act.[29]

III. Criminal Developments

The Obama administration has continued to pursue criminal prosecutions under the Economic Espionage Act. In fiscal year 2015, there were six new prosecutions and eight new convictions under 18 U.S.C. § 1832, which criminalizes the theft of trade secrets, as well as one new conviction under 18 U.S.C. § 1831, which criminalizes economic espionage.[30]

Prosecutions of Foreign Actors

As reported in last year's *Round-Up*, in 2014 the Department of Justice commenced several high-profile indictments of Chinese nationals for the theft of U.S. trade secrets. That trend continued in 2015. In July, the FBI announced a 53 percent increase in economic espionage cases over the prior year, which reportedly cost the U.S. economy hundreds of billions of dollars during

---

[15] Defend Trade Secrets Act of 2014, S. 2267, 113th Cong. (2014).

[16] Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(1) (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(1) (2015).

[17] *See* Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(2)(A)(ii) (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(2)(A)(ii) (2015); *See* Eric Goldman, *Ex Parte Seizure and the Defend Trade Secrets Act*, 72 WASH. LEE L. REV. 284, 285 (2015).

[18] Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(3) (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(3) (2015).

[19] *Compare* Defend Trade Secrets Act of 2015, S. 2267, 113th Cong. § 2(a)(2) (2014), *with* Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(3) (2015), *and* Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(3) (2015).

[20] *Compare* Defend Trade Secrets Act of 2015, S. 2267, 113th Cong. § 2(a)(3)(A) (2014), *with* Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(3)(A)(i)((2015), *and* Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(3)(A)(i) (2015).

[21] *Protecting Trade Secrets: Hearing Before the S. Judiciary Comm.*, 114th Cong. (2015) (statement of Karen Cochran), *transcript available at* http://www.judiciary.senate.gov/imo/media/doc/12-02-15%20Cochran%20Testimony.pdf.

[22] *Protecting Trade Secrets: Hearing Before the S. Judiciary Comm.*, 114th Cong. (2015) (statement of Thomas R. Beall), *transcript available at* http://www.judiciary.senate.gov/imo/media/doc/12-02-15%20Beall%20Testimony.pdf.

[23] The primary opponents of these bills are a group of law professors who argue that ''passage of the DTSA is likely to create new problems that could adversely impact domestic innovation, increase the duration and cost of trade secret litigation, and ultimately negatively affect economic growth.'' Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326) 1 (Nov. 17, 2015), *available at* https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf.

[24] *Protecting Trade Secrets: Hearing Before the S. Judiciary Comm.*, 114th Cong. (2015) (statement of Sharon K. Sandeen), *transcript available at* http://www.judiciary.senate.gov/imo/media/doc/12-02-15%20Sandeen%20Testimony.pdf.

[25] Press Release, Office of Senator Orrin Hatch, Senator Hatch, Coons: Trade Secrets Bill Ready for Markup, Floor Vote (Dec. 2, 2015), http://www.hatch.senate.gov/public/index.cfm/releases?ID=8600afd7-e929-4927-8e19-cf460fb9620a.

[26] *See S. 1890: Defend Trade Secrets Act of 2015*, GOVTRACK.US, https://www.govtrack.us/congress/bills/114/s1890 (last accessed Dec. 7, 2015); *H.R. 3326: Defend Trade Secrets Act of 2015*, GOVTRACK.US, https://www.govtrack.us/congress/bills/114/hr3326 (last accessed Dec. 7, 2015).

[27] Uniform Law Commission, *Trade Secrets Act*, http://www.uniformlaws.org/Act.aspx?title=Trade+Secrets+Act (last accessed Dec. 7, 2015).

[28] *See id.*

[29] *See id.*

[30] Transactional Records Clearinghouse, http://trac.syr.edu/laws/18/18USC01831.html (last accessed Dec. 7, 2015; Transactional Records Clearinghouse, http://trac.syr.edu/laws/18/18USC01832.html (last accessed Dec. 7, 2015).

that time frame.[31] The FBI also stated that the vast majority of perpetrators were based in China and appear to have ties to the Chinese government.[32] As discussed above, however, the administration has simultaneously attempted to combat this issue through diplomacy. Below, we highlight some of the most notable criminal cases of 2015.

United States v. Wei Pang, Hao Zhang, Huisui Zhang, JinPing Chen, Zhao Gang, & Chong Zhou (N.D. Cal.). On April 1, 2015, the United States indicted six Chinese nationals under the Economic Espionage Act for conspiracy to commit the theft of trade secrets. The indictment charged that the defendants ''knowing and intending that the offenses would benefit'' the People's Republic of China (''PRC'') as well as other foreign instrumentalities, conspired to steal, duplicate, and receive stolen trade secrets belonging to two companies headquartered in the United States—Avago Technologies and Skyworks Solutions.[33] The trade secrets at issue are used in wireless devices.[34]

United States v. Xiwen Huang (W.D.N.C.). On October 2, 2015, Chinese businessman, Xiwen Huang, pleaded guilty to one count of theft of trade secrets.[35] The government alleged that from 2006 to 2015, Huang ''engaged in a scheme to steal trade secrets from multiple companies within the United Sates, and intellectual property from the United States government, to further his aspirations of forming and operating his own company in the [PRC].'' Huang allegedly stole a substantial amount of information, including information with research and development costs of (a) $65 million from a chemical company specializing in the development of vehicle and chemical catalyst technology, and (b) $25 million from a company specializing in the development of power plant catalyst technology. [36] In addition, the government alleged that he stole intellectual property from a government research facility, including technology related to military vehicle fuel cells.[37] Huang faces up to ten years in prison and a $250,000 fine.[38]

United States v. Jiaqiang Xu (S.D.N.Y.). In December, federal prosecutors announced the arrest of Jiaqiang Xu, a software engineer who worked in the China branch of IBM, for the theft of trade secrets.[39] After leaving IBM, Xu allegedly stole ''the proprietary source code used for a clustered file system,'' which ''facilitate[d] faster computer performance by coordinating work among multiple servers.''[40] Xu was arrested after he told undercover FBI agents posing as a financial investor and a project manager for a fake data storage technology company that he was ''willing to consider'' giving them the stolen source code.[41] Xu was charged in a criminal complaint in federal court in New York with one count of theft of a trade secret.[42]

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (''CFAA'') provides federal civil and criminal causes of action against any person who, in relevant part, ''intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer,'' or who ''intentionally accesses a protected computer without authorization and as a result of such conduct, causes damage and loss.''[43] Employers who are the victims of trade secret misappropriation by their employees often bring claims for violation of the CFAA because such theft is often committed by accessing the employer's computer. However, to establish a violation of the CFAA in these circumstances, the employee must have (1) lacked authorization to access the computer or (2) ''exceed[ed]'' his or her ''authorized access.''[44]

Federal courts remain deeply split over what qualifies as ''exceed[ing] authorized access.'' This year, the Second Circuit joined the Fourth and Ninth Circuits in holding that an individual who is authorized to access a computer does not exceed his authorized access when he misuses or misappropriates information on that computer (the narrow view).[45] The First, Fifth, Seventh, and Eleventh Circuits hold that this type of misuse or misappropriation of information on a computer to which the individual has legitimate access does exceed authorized access (the broad view).[46]

In the Second Circuit case, *United States v. Valle*, an NYPD officer was charged with improperly accessing a government computer and obtaining information in violation of 18 U.S.C. § 1030(a)(2)(B), when he accessed a computer program that allows officers to search various restricted databases in order to search for a woman as

---

[31] Wendy Bruer, *FBI sees Chinese involvement amid sharp rise in economic espionage cases*, CNN (July 24, 2015), http://www.cnn.com/2015/07/24/politics/fbi-economic-espionage/.

[32] *Id.*

[33] Indictment at ¶¶ 1, 2, 23, *United States v. Wei Pang* (N.D. Cal. Apr. 1, 2015) (CR-15-00106).

[34] *Id.* at ¶¶ 3, 4, 18, 20, 24.

[35] Michael Gordon, Charlotte Scientist Pleads Guilty to Corporate Espionage (Oct. 2, 2015), The Charlotte Observer, http://www.charlotteobserver.com/news/local/crime/article37349634.html..

[36] Bill of Information, at ¶¶ 24, 29, United States v. Huang (W.D.N.C. Oct. 1, 2015) (No. 3:15-CR-00234).

[37] *Id.* at ¶ 16.

[38] Gordon, supra note 35.

[39] Kali Hays, *Feds Arrest Software Developer for Allegedly Stealing Code*, Law360 (Dec. 8, 2015), http://www.law360.com/employment/articles/735713?nl_pk=9dd64945-47c3-4547-bea5-5d2129ec2516&utm_source=newsletter&utm_medium=email&utm_campaign=employment.

[40] *Id.*

[41] *See id.*

[42] Nate Raymond, *Ex-IBM Employee from China Arrested in U.S. for Code Theft*, REUTERS (De. 8. 2015), http://www.reuters.com/article/us-ibm-crime-china-idUSKBN0TR2X820151208.

[43] 18 U.S.C. § § 1030(a)(2)(C), (a)(5)(C).

[44] 18 U.S.C. § 1030(a).

[45] *See United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012) (en banc); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 204 (4th Cir. 2012). Further, and as noted in last year's *Round-Up*, although the Third Circuit appears to be leaning towards accepting the narrow view, based on the 2014 decision in *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014), it has not, however, definitively adopted this view.

[46] *See United States v. John*, 597 F.3d 263, 271-73 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010); *Int'l Airport Ctrs, L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006); *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583 (1st Cir. 2001).

  PTCJ ISSN 0148-7965

part of a kidnapping plan.[47] The prosecution argued that ''Valle 'exceeded authorized access' because his authorization to access [the computer program] was limited to law enforcement purposes and he conducted a search for [the woman] with no such purpose.''[48] Although the court found support for both the broad and narrow view in the language and legislative history of the CFAA, it found that the rule of lenity in interpretation of criminal laws required it to adopt the narrow view.[49] It ''decline[d] to adopt the prosecution's construction, which would criminalize the conduct of millions of ordinary computer users and place [the court] in the position of a legislature.''[50] Accordingly, the court reversed Valle's conviction for violating the CFAA.[51] In dissent, Judge Straub relied on the plain language of the statute and found that '' '[w]here statutory . . . provisions unambiguously cover the defendant's conduct,' as Section 1030(a)(2)(B) clearly proscribes Valle's conduct here, the rule of lenity 'does not come into play.' ''[52]

In addition, the Northern District of California followed the Ninth Circuit's narrow view of the CFAA, rejecting a theory of liability based on agency principles. In *Koninklijke Philips N.V. v. Elec-Tech International Co.*, plaintiff Philips Lumileds, a developer of LED technology, sued 11 defendants, including a China-based competitor, Elec-Tech, alleging that a former Lumileds employee and current Elec-Tech employee, Gangyi Chen, downloaded thousands of files containing Lumileds' trade secrets and confidential information while working at Lumileds, and then disclosed this information to Elec-Tech.[53] Lumileds argue[d] that the defendants '' 'accessed' Lumileds' information through [Chen] as their agent—essentially that [Chen], though himself authorized to access the data, was a conduit by which the [defendants] engaged in their own unauthorized access.''[54] The court rejected these arguments, and dismissed the CFAA claim. The court found that the Ninth Circuit has ''explicitly caution[ed] that the CFAA was designed to target hacking, not misappropriation,'' and therefore ''CFAA violations require a person to engage in the hacking, not merely benefit from its results.''[55] The court also noted that if it accepted the plaintiff's argument, ''it would effectively federalize all trade secret misappropriation cases where parties use a computer to download sensitive or confidential trade secret information—which would be nearly every trade secret case nowadays.''[56]

Although the Third, Sixth, Eight, Tenth and D.C. Circuits have not clearly adopted either the broad or narrow view, 2015 saw numerous district courts within those circuits weighing in, with the majority accepting the narrow view.[57]

Other Notable Cases

United States v. Aleynikov (N.Y.). This year, the New York Supreme Court overturned the conviction of former Goldman Sachs computer programmer Sergey Aleynikov. In 2009, Aleynikov allegedly uploaded computer source code from Goldman's system to a server in Germany, and then downloaded that code from the German server to his personal computer in New Jersey without authorization.[58] This purportedly occurred during Aleynikov's last official week at Goldman—after he had accepted a position at another company—though he remained in possession of the code for several weeks after his employment with Goldman officially ended.[59] In 2012, Aleynikov was charged in New York state court with the ''Unlawful Use of Secret Scientific Material'' and the ''Unlawful Duplication of Computer Related Material.''[60] In May 2015, a jury found Aleynikov guilty, but in July, the New York Supreme Court overturned the verdict, granting the defendant's motion for a trial order of dismissal.[61] It held that ''the prosecution did not prove the defendant made a 'tangible reproduction or representation' of secret scientific material . . . [and] did not demonstrate Aleynikov had the 'intent to appropriate . . . the use of secret scientific material.' ''[62] The court further noted the inapplicability of the 1967 law criminalizing the unlawful use of secret scientific material under which Aleynikov was prosecuted to these modern facts, and stated that ''[t]he demands of the digital age will doubtless require further refinement of our criminal laws.''[63]

United States v. Nosal (9th Cir.). As noted in last year's *Round-Up*, David Nosal was charged in 2008 with eight counts of violating the CFAA and misappropriating trade secrets in connection with a conspiracy to obtain confidential data and trade secrets from his former employer's database.'' [64] In *Nosal I*, the Ninth Circuit, in dismissing five of the eight counts, adopted the narrow view of the CFAA and held that because the defendants had authorized access to the database, they did not exceed their authorized access by misusing or

[47] *United States v. Valle*, —- F.3d —-, 2015 WL 7774548, at *2 (2d Cir. 2015).
[48] *Id.* at *14.
[49] *Id.* at *14–17.
[50] *Id.* at *17.
[51] *Id.* at *18.
[52] *Id.* at *28–30 (Straub, J., dissenting).
[53] *Koninklijke Philips N.V. v. Elec-Tech Int'l Co.*, No. 14–cv–02737–BLF, 2015 WL 1289984, at *2 (N.D. Cal. Mar. 20, 2015).
[54] *Id.* at *4.
[55] *Id.* (internal citation omitted).
[56] *Id.* at *6.
[57] *Compare Experian Marketing Solutions, Inc. v. Lehman*, No. 1:15–CV–476, 2015 WL 5714541, at *5 (W.D. Mich. Sept. 29, 2015) (adopting narrow view), *Giles Constr., LLC v. Tooele Inventory Solution, Inc.*, No. 2:12–cv–37, 2015 WL 3755863, at *3 (D. Utah June 16, 2015) (same), *Allied Portables, LLC v. Youmans*, No. 2:15–cv–294–FtM–38CM, 2015 WL 3720107, at *5 (M.D. Fla. June 15, 2015) (same), *Enhanced Recovery Co., LLC. v. Frady*, No. 3:13–cv–1262–J–34JBT, 2015 WL 1470852, at *5 (M.D. Fla. Mar. 31, 2015) (same), *with* Am. Furukawa, Inc. v. Hossain, No. 14–cv–13633, 2015 WL 2124794, at *11–16 (E.D. Mich. May 6, 2015) (adopting broad view).
[58] *People v. Aleynikov*, 15 N.Y.S.3d 587, 590–91 (N.Y. Sup. Ct. 2015).
[59] *Id.* at 591.
[60] *Id.* at 590.
[61] *See id.* Aleynikov was also convicted in federal court for violating the National Stolen Property Act and the Economic Espionage Act, but these convictions were overturned in 2012. *Id.* at 592.
[62] *Id.*
[63] *See id.* at 628–30; Matthew Goldstein, *Conviction of Former Goldman Sachs Programmer is Overturned*, N.Y. Times (July 6, 2015), http://www.nytimes.com/2015/07/07/business/dealbook/conviction-of-former-goldman-programmer-is-overturned.html.
[64] Indictment at ¶¶ 13–23, *United States v. Nosal* (N.D. Cal. Apr. 10, 2008 (No. CR 08-00237 MHP).

misappropriating the information contained within it.[65] On October 20, 2015, the Ninth Circuit heard oral arguments in *Nosal II*, which concerns the meaning of ''without authorization'' in relation to the charge that Nosal's co-conspirators used the login credentials of Nosal's secretary to access the firm's database.[66] Nosal argued that this ''was not a crime under the CFAA because the secretary had authorization and transferred it consensually.''[67] In addition, the court heard arguments regarding Nosal's conviction under the EEA for theft of trade secrets.[68] The court questioned both sides about whether the source lists obtained by Nosal and his co-conspirators, which contained lists of employment candidates that an executive search firm presented to client companies with respect to particular positions those clients were trying to fill, derived independent economic value by not being generally known to the public.[69]

Civil Developments

In 2015, federal and state courts addressed a wide array of issues involving civil trade secret claims, including whether certain types of information—such as private LinkedIn groups or software program interfaces—qualify for trade secrets protection, and how companies can prevent government entities from disclosing their trade secrets.

I. Preemptive Effect of the UTSA

Last year's *Round-Up* reported that courts continue to struggle with determining when the UTSA preempts claims that provide remedies for the misappropriation of confidential but non-trade secret information.[70] We noted that the Arizona Supreme Court concluded that Arizona's UTSA does not preempt such claims, contrary to the conclusion of many courts interpreting trade secret statutes around the country that the uniform acts provide an exclusive statutory remedy for the alleged misuse of proprietary information, trade secret or not.[71]

Thus far, the response to the Arizona Supreme Court's approach has been mixed, as many courts continue to hold (with some exceptions) that a plaintiff cannot assert most claims based on the theft of confidential information when the facts underlying those claims also form the basis of the plaintiff's trade secrets claim. For instance, an Arkansas federal court expressly rejected the Arizona Supreme Court's analysis as ''inconsistent'' with Arkansas case-law, holding that Arkansas' UTSA preempts claims for tortious interference and deceptive trade practices where those claims are based on the same acts that support a claim for trade secrets misappropriation.[72] At the same time, the Arkansas court concluded that the Arkansas UTSA does not preempt contract claims at all, regardless of whether the claims are based on misappropriation of trade secrets.[73] Similarly, a federal district court in Washington held that, because the plaintiff would have to rely on the same facts that supported its trade secrets claim to prove tortious interference, the latter claim was preempted by Washington's UTSA.[74]

II. Information Eligible for Trade Secret Protection

Throughout 2015, federal and state courts continued to consider what types of information qualify as a ''trade secret.'' Several cases this year involved the trade secret eligibility of social media data, creative ideas, and software programs. The cases confirm that ''[a]lmost any subject matter may be a trade secret,''[75] but that this general principle has its limits.

Bianco v. Globus Medical, Inc. (Fed. Cir.) .[76] In the final chapter of a case reported in last year's *Round-up*, the Federal Circuit affirmed a jury verdict in favor of a physician who alleged that Globus misappropriated his trade secrets by manufacturing a spinal fusion implant based on his ideas. The physician was awarded $4.3 million in damages for past trade secrets misappropriation and 5% in ongoing royalties for net sales of the implant. In the district court, Globus moved for judgment as a matter of law on the ground that the physician's design was a ''mere idea'' and not a trade secret under Texas law, but the court denied that motion and held that ''[i]deas, whether 'mere' or otherwise, are protected from misappropriation so long as they provide an opportunity to obtain a business advantage over competitors and are maintained in secret.''[77] The Federal Circuit affirmed in an unpublished *per curiam* opinion.[78]

Warehouse Solutions, Inc. v. Integrated Logistics, LLC (11th Cir.).[79] The Eleventh Circuit recently clarified what aspects of proprietary software qualify for trade secret protection. The plaintiff, Warehouse Solutions (WSI), developed a web-based software program called Intelligence Audit that allows companies to track their UPS and FedEx packages and collect refunds for late or missing packages. According to WSI, Defendant Integrated Logistics (ILL) sold Intelligence Audit and

[65] *United States v. Nosal*, 676 F.3d 854, 864 (9th Cir. 2012).
[66] *Watch Recording for Case: USA v. David Nosal, No. 14-10037*, U.S. Courts for the Ninth Circuit, http://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000008351 (last accessed Dec. 18, 2015).
[67] *Id.*
[68] *Id.*
[69] *Id.* The case remained pending before the Ninth Circuit as of the writing of this article.
[70] *See supra* note 1.
[71] *Orca Communications Unlimited LLC v. Noder*, 337 P.3d 545 (Ariz. 2014). For the traditional view from which *Orca* departed, *see, e.g.*, *Firetrace USA, LLC v. Jesclard*, 800 F. Supp. 2d 1042, 1048 (D. Ariz. 2010) (''The majority interpretation appears to be that the UTSA preempts all common law tort claims based on misappropriation of information, whether or not it meets the statutory definition of a trade secret.'').
[72] *3A Composites USA, Inc. v. United Indus., Inc.*, 2015 WL 5437119 (W.D. Ark. Sept. 15, 2015).
[73] *Id.* at *5-6.
[74] *T-Mobile USA v. Huawei Device USA Inc.*, 2015 WL 4308682 (W.D. Wash. July 14, 2015).
[75] Louis Altman and Malla Pollack, 2 *Callmann on Unfair Competition, Trademark & Monopolies* § 14:14 (4th ed. Aug. 2015) (Callmann, *Unfair Competition*).
[76] No. 15-1193, 618 Fed. App'x 1032 (Fed. Cir. 2015), 2015 WL 6124988.
[77] *Bianco v. Globus Medical, Inc.*, 2014 WL 5462388, at *8 (E.D. Texas Oct. 27, 2014).
[78] No. 15-1193, 618 Fed. App'x 1032 (Fed. Cir. 2015), 2015 WL 6124988.
[79] 610 Fed. App'x 881 (11th Cir. 2015).

  PTCJ ISSN 0148-7965

paid WSI a transaction fee on each sale. Because ILL administered the program to end users and actively managed their accounts, WSI claimed that the company had intimate access to the program's features (though not its underlying source code). WSI asserted that ILL then hired another company to develop a web-tracking program similar to Intelligence Audit and allowed that company to log onto the Intelligence Audit program. Once the new program was developed, WSI claimed that ILL cut off its arrangement with WSI and began selling its own tracking software.

WSI sued ILL for trade secrets misappropriation, among other claims. The district court granted summary judgment to ILL on all of WSI's claims, notably finding that the Intelligence Audit program was not a ''trade secret.'' The court reasoned that ILL had access only to the program's screen displays, which are not secret but are ''readily apparent to users of the software.''[80] While the underlying source code of a software program (written in programming language and not visible to users) may be a trade secret, a program's obvious functions and appearance cannot be.[81] The Eleventh Circuit affirmed, reasoning that ''[h]ow Intelligence Audit looked and worked was readily apparent to authorized users with an ID and password.''[82]

CDM Media USA v. Simms (N.D. Ill.). [83] A federal court this year considered whether a LinkedIn contact group can qualify as a trade secret, yet refused to resolve the issue in the defense's favor on a motion to dismiss. Defendant Robert Simms was allegedly a member of the senior management team for plaintiff CDM Media USA. According to CDM, Simms managed a CDM LinkedIn group called the CIO Speaker Bureau, a private group of almost 700 chief information officers and executives who were interested in speaking at or participating in CDM events.[84] When Simms left CDM to work for one of its customers, he allegedly refused to relinquish control of the LinkedIn Group or return the Bureau's membership list and communications to CDM, and instead was asserted to have used them to solicit customers in violation of his non-compete agreement with CDM. CDM sued Simms in Illinois state court for breach of contract, violation of the Illinois Trade Secrets Act, and common law misappropriation.[85] After Simms removed the case to federal court, he moved to dismiss. While the court granted the motion in part, it refused to dismiss CDM's trade secrets claim.[86] CDM, the court noted, alleged that the LinkedIn group contained names of potential customers that would be valuable to CDM's competition; that it took significant time and effort to compile the list; and that access to the group was restricted by its privacy settings.[87] In light of this, the court held that ''too little is known about the contents, configuration, and function of the LinkedIn group at this time, to conclude as a matter of law that its list of members did not constitute a trade secret.''[88]

III. Cases against Government Entities

At least two federal cases this year involved companies filing suit against government entities to prevent disclosure of confidential business information and trade secrets. Private companies are sometimes obligated to disclose such information to the government—for instance, to procure or carry out a government contract or to obtain agency approval of a proposed merger. But disclosing proprietary information to government entities poses risks to companies, because, for example, public entities are often required to allow the public to view certain documents during the notice-and-comment phase of agency proceedings or pursuant to public access statutes such as the Freedom of Information Act (FOIA), which raises the concern that a company's valuable proprietary information will be disclosed to competitors. The cases below demonstrate several companies' attempts to protect themselves from government disclosure of trade secrets.

Batelle Memorial Institute v. U.S. Department of the Army (S.D. Ohio).[89] Batelle Memorial Institute, a logistics-support contractor, reached a settlement with the U.S. Army in a suit alleging that the Army improperly disclosed the company's trade secrets in response to a FOIA request without notifying Batelle in advance so that the company could object.[90] The Army allegedly released Batelle's detailed financial information, costs, profits and rates, workforce data, selling prices and purchase activity, pricing strategy, and subcontractor information—information that allegedly would allow competitors to adjust and improve their future bids against Batelle—which was then published on a third-party website.[91] Batelle sought relief under several theories, including (1) FOIA Exemption 4, which protects ''trade secrets and commercial or financial information'' submitted by a company to the government from disclosure,[92] and (2) the Trade Secrets Act (TSA), which prohibits federal officials from unlawfully disclosing a company's trade secrets and other confidential business information.[93] The complaint sought declaratory and injunctive relief and contractual damages of over $4 million. The parties entered into a confidential settlement agreement in summer 2015.[94]

CBS Corporation v. Federal Communications Commission (D.C. Cir.).[95] In this case, the FCC considered the respective mergers of AT&T with DirecTV, and Comcast with Time Warner and Charter Communications. As part of the review process, the FCC required the applicants to submit ''video programming confidential information'' (VCPI), including contracts and negotiating documents related to the applicants' deals with content providers such as CBS, Viacom, and Disney.[96] These content providers argued that the FCC should not permit disclosure of such sensitive proprietary informa-

[80] *Id*. at 884.
[81] *Id*.
[82] *Id*. at 885.
[83] No. 14-cv-9111 (N.D. Ill. March 25, 2015), 2015 WL 1399050.
[84] *Id*. at *2.
[85] *Id*. at *2.
[86] *Id*. at *4-*5.
[87] *Id*. at *4-*5.
[88] *Id*. at *4.
[89] No. 2:14-cv-445 (S.D. Ohio May 14, 2014).
[90] Complaint at ¶¶ 1, 17-39, No. 2:14-cv-445 (S.D. Ohio May 14, 2014).
[91] *Id*. at ¶¶ 59-60.
[92] 5 U.S.C. § 552(b)(4).
[93] 18 U.S.C. § 1905.
[94] Stipulated Dismissal with Prejudice, No. 2:14-cv-445 (N.D. Ohio Aug. 6, 2015).
[95] 785 F.3d 699 (D.C. Cir. 2015).
[96] 785 F.3d at 701-02.

tion to competitors during the review process, but ultimately, the FCC determined that VCPI must be provided to all potential commenters subject to a protective order.

The D.C. Circuit vacated the FCC's decision to disclose the VCPI. Relying on the TSA and the FCC's own regulations, the court held that the FCC must apply a ''presumption against disclosure of confidential information'' to third parties in the merger review context.[97] That presumption can be overcome only if the FCC shows that the confidential business information itself is ''necessary to the evaluation process'' and thus must be disclosed to outsiders if the FCC is to fulfill its statutory obligation to review the merger properly.[98]

IV. Alleging and Proving Misappropriation

Several recent federal and state decisions underscore the importance of identifying trade secrets with particularity, and the doctrines companies may rely on to obtain injunctive relief against suspected misappropriation.

Top Agent Network, Inc. v. Zillow, Inc. (N.D. Cal.).[99] In April 2015, a federal district court in California dismissed 12 of Top Agent Network's (TAN's) 13 claims against Zillow, including a trade secrets claim that was later resuscitated. TAN is an online community that allows participating real estate agents to exchange valuable information about upcoming or about-to-be listed properties. TAN claims that Zillow feigned interest in investing in TAN in order to gain access to its confidential proprietary information and business model.[100] According to TAN, Zillow then informed TAN that it was not going to make an investment and, a month later, launched a copycat product that incorporated confidential and proprietary information obtained from TAN to offer Zillow users access to listings not yet on the market.[101] The court dismissed the trade secrets claim because TAN failed to adequately specify how anything Zillow allegedly may have taken qualified as a trade secret.[102] TAN alleged only that it had shared information with Zillow through conversations and by granting it access to its password-protected webpages, but did not specify ''what pieces of information shared through each could constitute trade secrets.''[103] TAN later provided more specific details, and the court allowed the trade secrets claim to proceed.[104]

InnoSys, Inc. v. Mercer (Utah Supreme Court).[105] The Utah Supreme Court held that once a company has shown its trade secrets were misappropriated, it need not prove how it was or stands to be harmed by the misappropriation in order to obtain injunctive relief. InnoSys, a technology company in the defense industry, alleged that its former engineer, Amanda Mercer, violated a non-disclosure agreement and engaged in misappropriation of trade secrets when she e-mailed company information and a confidential company business plan to her personal email account, downloaded it onto a personal thumb drive, and used the information in an administrative unemployment hearing following her dismissal from InnoSys. The trial court granted summary judgment to Mercer on all claims, finding that InnoSys had produced no evidence of actual or threatened harm posed to the company by any of her alleged misdeeds.[106]

The Utah Supreme Court reversed. The majority reasoned that there must be a presumption of harm whenever a plaintiff makes a *prima facie* case of trade secrets misappropriation.[107] InnoSys established that the materials Mercer took included trade secrets, and also introduced evidence that Mercer committed misappropriation by disclosing and acquiring those secrets unlawfully.[108] Under such circumstances, ''the law presumes that the infringement of a property right is harmful, and sustains the remedy of an injunction to vindicate that right and prevent future harm.''[109] While that presumption may be rebutted, Mercer could not do so here: The only guarantee she could offer InnoSys that it would not be harmed in the future was her ''self-serving assertions'' that she had deleted any InnoSys materials in her possession.[110]

V. Developments in High-Stakes Trade Secrets Cases in 2015

Nike, Inc. v. Dekovic (Cir. Ct. Multnomah Co., Or.).[111] As reported in last year's *Round-up*, Nike sued three former designers in Oregon state court seeking injunctive relief and $10 million in damages based on allegations that the designers misappropriated Nike's trade secrets, developed plans to create a competing studio while still employed by Nike, and destroyed or deleted evidence of their misconduct. In June 2015, the parties reached a confidential settlement following entry of a preliminary injunction in favor of Nike.[112]

Moncrief Oil International v. OAO Gazprom (17th Jud. Dist. Tarant Cty., Tex.).[113] Texas-based oil company Moncrief Oil International abruptly dropped its billion-dollar trade secrets case against a Russian gas company mid-trial after the defense accused Moncrief of fabricating a key piece of evidence. Moncrief filed the suit against Gazprom in 2008, alleging that Gazprom stole Moncrief's trade secrets and excluded the Texas company from a deal to develop a lucrative Russian gas field.[114] Moncrief produced a financial model to the defense that it claimed constituted a de-

[97] *Id*. at 707.
[98] *Id*. at 707-08.
[99] No. 3:14-cv-04769 (N.D. Cal. Oct. 27, 2014).
[100] Complaint at ¶ 3, No. 3:14-cv-04769 (N.D. Cal. Oct. 27, 2014).
[101] *Id*. at ¶ 4.
[102] Order Granting Motion to Dismiss and Denying Request for Judicial notice, No. 14-cv-04769 (N.D. Cal. April 13, 2015).
[103] *Id*. at 8.
[104] Order Granting in Part and Denying in Part Motion to Dismiss with Partial Leave to Amend, No. 14-cv-04769 (N.D. Cal. Aug. 6, 2015).
[105] No. 20110261, 2015 WL 5090452 (Utah August 28, 2015).
[106] *Id*. at *5.
[107] *Id*. at *7-*8.
[108] *Id*. at *5-*6.
[109] *Id*. at *7.
[110] *Id*. at *9.
[111] No. 14 Cv. 18876 (Cir. Ct. Multnomah Co. Dec. 8, 2014).
[112] Gibson Dunn represented Nike in the lawsuit.
[113] No. 017-229664-08 (April 3, 2008).
[114] Complaint, No. 017-229664-08 (17th Jud. Dist. Tarant Cty., Tex. April 3, 2008).

  PTCJ ISSN 0148-7965

tailed financial business plan that Gazprom stole.[115] Moncrief's former CFO testified at trial that he created the document in 2004, but his testimony was contradicted on cross-examination when the defense revealed that one of the images in the document did not exist until 2012.[116] Shortly afterward, Gazprom moved for sanctions, prompting Moncrief to file a motion to dismiss the entire case with prejudice, which the trial court granted.[117] Moncrief's attorney said he was unaware of the flawed document until it was discovered by the defense at trial[118].

Alcoa, Inc. v. Universal Alloy Corp. (N.D. Ga.).[119] Steel products manufacturer Alcoa filed a trade secret lawsuit in Georgia federal court against rival manufacturer Universal Alloy in 2015, alleging that Universal Alloy lured away its employees and used their knowledge of Alcoa's trade secrets to obtain a supply contract with an aircraft manufacturer for aircraft wing parts. According to Alcoa, Universal Alloy hired Alcoa employees and consultants who disclosed their ex-employer's secrets, giving Universal Alloy unfair access to a manufacturing technique that Alcoa claims is ''a mixture of art and science [developed through a] painstaking, trial-and-error process, which took place over the course of many years.''[120] Alcoa asserted that after Universal Alloy convinced the aircraft manufacturer that it could supply the same parts as Alcoa at a lower cost, the aircraft manufacturer retained Universal Alloy to manufacture the wing parts during the next contractual cycle.[121] Because Alcoa is no longer the aircraft manufacturer's exclusive supplier, it projects losses of ''more than $200 million in sales over the life of the ten-year contract.''[122]

Jawbone v. Fitbit. Two wearable fitness-device manufacturers are engaged in a fierce legal battle before the International Trade Commission (ITC) and federal and state courts around the country. It began in May 2015, when Jawbone filed a trade secrets lawsuit in California state court against Fitbit and several ex-Jawbone employees now at Fitbit.[123] That suit alleges that Fitbit poached Jawbone's employees and misappropriated its trade secrets to develop wearable fitness trackers. In June, just before Fitbit's initial public offering, Jawbone filed a patent infringement suit in California federal court, claiming that Fitbit's line of fitness-tracking devices infringes Jawbone's patents.[124] And in July, Jawbone filed an ITC complaint initiating an import investigation into whether Fitbit unlawfully imported patent-infringing devices into the United States.[125] For its part, Fitbit has filed patent infringement suits against Jawbone in California and Delaware federal court and submitted a complaint of its own to the ITC regarding Jawbone's alleged importation of devices that infringe Fitbit's patents.[126] [127]

E.I. du Pont de Nemours and Co. v. Kolon Industries, Inc. et al. (E.D. Va.).[128] A long-running trade secrets case with both criminal and civil elements ended this year as Korean company Kolon Industries pled guilty and agreed to pay $360 million in fines and criminal restitution to DuPont for conspiring with ex-DuPont employees to steal trade secrets related to DuPont's signature Kevlar bulletproof vests. DuPont originally won a $920 million jury verdict against Kolon that was overturned by the Fourth Circuit.[129] The parties reached a settlement in the civil case as well. Five South Korean Kolon employees still face federal criminal charges.[130]

Miller UK Ltd et al. v. Caterpillar, Inc. (N.D. Ill.).[131] An Illinois federal jury awarded a U.K. earth-moving equipment supplier nearly $74 million in a trade secrets lawsuit against a U.S. company that was once its largest customer.[132] The jury verdict followed an eight-week trial in which Plaintiff Miller UK Ltd. (Miller) accused Caterpillar of using a supply contract to gain access to Miller's trade secrets for products that Miller manufactures, including couplers used in excavations.[133] Miller filed a lawsuit against Caterpillar in 2010 for trade secret misappropriation and other claims, alleging that Caterpillar exploited its access to Miller's trade secrets so that Caterpillar could produce its own products without having to engineer them from scratch.[134] The case also drew attention from commentators because Miller (a small company compared to its

---

[115] Margaret Cronin Fisk and Tom Korosec, *Perry Mason Moment Halts Moncrief $1.37 Billion Gazprom Suit*. Bloomberg Business (February 2, 2015, 10:21 AM EST), http://www.bloomberg.com/news/articles/2015-02-02/moncrief-drops-1-37-billion-gazprom-suit-after-sanction-request. *See also* Defendants' Second Motion for Sanctions at 1, No. 017-229664-08 (17th Jud. Dist. Tarant Cty., Tex., Jan. 29, 2015).

[116] *See id.*

[117] Order of Dismissal with Prejudice, No. 017-229664-08 (17th Jud. Dist. Tarant Cty, Tex. Feb. 2, 2015).

[118] Fisk and Korosec, supra note 115.

[119] Complaint, No. 1:15-cv-01466 (N.D. Ga. April 30, 2015).

[120] *Id*. ¶¶ 4-5, 27.

[121] *Id*. ¶¶ 6-7.

[122] *Id*. ¶ 37.

[123] *AliphCom, Inc. d/b/a Jawbone v. Fitbit, et al.*, No. CGC-15-546004 (S.F. Sup. Ct. May 27, 2015).

[124] *AliphCom and BodyMedia, Inc. v. Fitbit, Inc.*, No. 3:15-cv-2579 (N.D. Cal. June 10, 2015).

[125] International Trade Commission, *Certain Activity Tracking Devices, Systems, and Components Thereof; Institution of Investigation*, Investigation No. 337-TA-963 (August 18, 2015), *available at* https://www.federalregister.gov/articles/2015/08/21/2015-20730/certain-activity-tracking-devices-systems-and components-thereof-institution-of-investigation.

[126] *Fitbit, Inc. v. AliphCom d/b/a Jawbone and BodyMedia, Inc.*, No. 1:15-cv-00775 (September 3, 2015); *Fitbit, Inc. v. Aliphcom d/b/a Jawbone & BodyMedia, Inc.*, No. 5:15-cv-04073 (N.D. Cal. Sept. 8, 2015); *Fitbit, Inc. v. AliphCom d/b/a Jawbone and BodyMedia, Inc.*, No. 1:15-cv-00990 (Dist. Delaware October 29, 2015); *Verified Complaint of Fitbit Under Section 337 of the Tariff Act of 1930, As Amended* (ITC Oct. 28, 2015), *available at* http://www.itcblog.com/images/fitbitcomplaint.pdf.

[127] Gibson Dunn represents Fitbit in the dueling patent infringement suits and in Fitbit's ITC complaint.

[128] The criminal case is *USA v. Kolon Indus., Inc. et al.*, No. 3:12-cr-00137 (E.D. Va.), and the civil case is *E.I. du Pont de Nemours & Co. v. Kolon Indus. Inc.*, et al., No. 3:09-cv-00058 (E.D. Va.).

[129] *E.I. DuPont De Nemours & Co. v. Kolon Indus., Inc.*, 564 Fed. App'x 710 (4th Cir. 2014) (unpublished).

[130] Indictment, No. 3:12-cr-00137 (E.D. Va. August 21, 2012).

[131] No. 1:10-cv-03770 (June 17, 2010).

[132] James R. Hagerty, *Supplier Wins $74 Million Verdict Against Caterpillar*, Wall Street Journal (Dec. 21, 2015 12:46 PM EST), http://www.wsj.com/articles/supplier-wins-74-million-verdict-against-caterpillar-1450700414.

[133] *Id*.

[134] Complaint, No. 1:10-cv-03770 (N.D. Ill. June 17, 2010).

Fortune 50 adversary) relied on third-party investors to fund the litigation.[135]

Conclusion

Developments in 2015 demonstrate that U.S. companies, and the U.S. government itself , remain vulnerable to trade secret theft and misappropriation from domestic and foreign actors. 2015 saw a number of high-profile cases across a wide variety of industries involving trade secret theft and misappropriation by former employees and competitors, making it increasingly important that all companies take steps—and continually reevaluate those steps—to safeguard their trade secrets and other valuable intellectual property, and to mitigate the risk that they may be accused of misappropriating another company's secrets when hiring employees from competitors.

While the Obama administration took a number of notable steps in 2015 to protect U.S. trade secrets, including the creation of a sanctions program and diplomatic efforts aimed at curbing hacking by perpetrators in China, it will be interesting to see if these efforts prove effective in reducing cyber espionage and trade secret theft in 2016, particularly at the hands of foreign actors. It will also be important in 2016 for U.S. companies to monitor legislative developments, such as the potential passage of the DTSA, which would create a federal civil cause of action for misappropriation of trade secrets related to products used in interstate or foreign commerce.[136]

---

[135] Mattathias Schwartz, *Should You Be Allowed to Invest in a Lawsuit?*, New York Times Magazine (Oct. 22, 2015), http://www.nytimes.com/2015/10/25/magazine/should-you-be-allowed-to-invest-in-a-lawsuit.html?_r=0. *See also* Memorandum Op. at 3, No. 1:10-cv-03770 (N.D. Ill. Jan. 6, 2014).

[136] Defend Trade Secrets Act of 2015, S. 1890, 114th Cong. § 2(b)(1) (2015); Defend Trade Secrets Act of 2015, H.R. 3326, 114th Cong. § 2(b)(1) (2015).

  PTCJ ISSN 0148-7965