AN A.S. PRATT PUBLICATION
MAY 2016
VOL. 2 • NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2 | NUMBER 4 | MAY 2016

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3000
Fax Number .... (518) 487-3584
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3000

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [121] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2016–Pub. 4939)

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 718.224.2258. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

Critical Issues for Foreign Defendants in International Trade Secrets Litigation – Part I

By Jeffrey A. Pade*

Of the many issues that international businesses face, managing trade secret risks in an increasingly digital age is one of the more daunting challenges. In this two-part article, the author discusses international trade secret misappropriation and litigation. This first part of the article explores civil trade secrets risks facing foreign businesses, the criminal components of trade secrets litigation, and the U.S. government's extraterritorial reach in Economic Espionage Act cases. The second part of the article, which will appear in an upcoming issue of Pratt's Privacy & Cybersecurity Law Report*, will focus on federal prosecutors' pursuit of criminal prosecution while civil trade secrets litigation is ongoing or contemplated, the unique opportunities and risks of parallel civil and criminal trade secrets proceedings, cross-border investigations, and future developments.*

As the business interests of foreign companies continue to expand in the United States, so too do the risks of costly and complex international litigation. Companies operating on an international level have a breadth of legal and regulatory concerns that they must focus on, including protecting proprietary intellectual property while also respecting the intellectual property of others. Of the many issues that international businesses face, managing trade secret risks in an increasingly digital age is one of the more daunting challenges. Corporate financial, business, and technical secrets are easily stored, exchanged, and transmitted in electronic form, making them susceptible to conversion and wrongful theft by others inside and outside the business. Indeed, the losses attributable to trade secret theft are estimated to be one to three percent of the U.S. gross domestic product,[1] amounting to tens or even hundreds of billions of dollars annually in the U.S. alone.[2] International trade secret misappropriation has thus garnered considerable focus from U.S. regulatory and criminal enforcement efforts.

---

* Jeffrey A. Pade is a partner in the Intellectual Property practice of Paul Hastings LLP, practicing all phases of trade secrets and patent law with an emphasis on complex domestic and international intellectual property litigation. He may be reached at jeffpade@paulhastings.com. The author acknowledges the assistance of Tad Richman and Casey L. Miller, also of Paul Hastings LLP.

[1] Ctr. for Responsible Enter. & Trade, PriceWaterhouseCoopers LLP, *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats* (2014), https://www.pwc.com/en_US/us/forensic-services/publications/assets/economic-impact.pdf.

[2] *Economic Espionage and Trade Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 113th Cong. (May 13, 2014) (statement of Randall Coleman, Ass't Dir., Counterterrorism Div., Fed. Bureau of Investigation), http://www.judiciary.senate.gov/imo/media/doc/05-13-14ColemanTestimony.pdf.

CIVIL TRADE SECRETS RISKS FACING FOREIGN BUSINESSES

Forty-eight states and the District of Columbia have enacted trade secret laws adopted from the Uniform Trade Secrets Act ("UTSA"). In the remaining two states—Massachusetts and New York—civil and criminal liability for trade secret violations, extending to both damages and injunctive relief, is based on state-specific statutes and common law, respectively.[3] The UTSA was intended to harmonize disparate trade secret laws among the states, thereby reducing forum shopping and uncertainty among businesses, and the majority view is that the state-enacted UTSA broadly preempts state common law claims.[4] The standard for trade secret liability under the UTSA continues to evolve as more cases test the bounds of what information may constitute a trade secret. Concepts and ideas to solve specific problems may be protectable as trade secrets, even when they have not matured into a specific formula, algorithm, or product.[5] In patent parlance, this means that ideas need not be "reduced to practice" to qualify for trade secret protection. For example, design concepts disclosed during business negotiations may well be protectable as trade secrets, even when those designs are still works-in-progress.[6] For foreign companies, this means that routine business negotiations conducted in the United States have the risk of serving both as a hook for personal jurisdiction and the avenue for disclosure of protectable

---

[3] *See* Mass. Gen. Laws. ch. 93, §§ 42, 42A; ch. 266, § 30.

[4] *AccuImage Diagnostics Corp. v. Terarecon, Inc.*, 260 F. Supp. 2d 941, 953–54 (N.D. Cal. 2003) (common law misappropriation claim preempted); *Mortgage Specialists, Inc. v. Davey*, 904 A.2d 652, 666 (N.H. 2006) (conversion claim preempted); *Digital Envoy, Inc. v. Google, Inc.*, 370 F. Supp. 2d 1025 (N.D. Cal. 2005), vacated on other grounds, 2006 U.S. Dist. LEXIS 6449 (N.D. Cal. Jan. 25, 2006) (common law and statutory unfair competition and unjust enrichment preempted); *Convolve, Inc. v. Compaq Comput. Corp.*, No. 00CV5141, 2006 U.S. Dist. LEXIS 13848 (S.D.N.Y. Mar. 29, 2006) (claims for tortious interference with contract and prospective business advantage preempted); *Opteum Fin. Servs., LLC v. Spain*, 406 F. Supp. 2d 1378 (N.D. Ga. 2005) (claim for quantum meruit preempted); *Thomas & Betts Corp. v. Panduit Corp.*, 108 F. Supp. 2d 968, 972 (N.D. Ill. 2000) (claim for breach of fiduciary duty preempted); *MicroStrategy, Inc. v. Bus. Objects, S.A.*, 429 F.3d 1344 (Fed. Cir. 2005) (claim for civil conspiracy preempted). In contrast, the minority view suggests that the UTSA preempts only common law actions for trade secret misappropriation. *See, e.g.*, *Burbank Grease Serv., LLC v. Sokolowski*, 717 N.W.2d 781 (Wis. 2006).

[5] *See, e.g.*, *Altavion, Inc. v. Konica Minolta Sys. Lab. Inc.*, 226 Cal. App. 4th 26, 53–57 (2014) (holding that an idea for authenticating documents using barcodes, whether or not separately patentable, may comprise a trade secret and explaining that the "the trade secret is not the idea or fact itself, but *information* tending to communicate (disclose) the idea or fact to another.").

[6] *See, e.g.*, *Bianco v. Globus Med., Inc.*, No. 12-cv-00147, 2014 U.S. Dist. LEXIS 151967, at *26–27 (E.D. Tex. Oct. 27, 2014) (holding that "[i]deas, whether 'mere' or otherwise, are protected from misappropriation as long as they provide an opportunity to obtain a business advantage over competitors and are maintained in secret," and finding that physician's idea for a new design for implants to be used in spinal fusion surgery was identified with sufficient specificity during negotiations to constitute a protectable trade secret).

information. Indeed, a trade secret may consist entirely of information available in the public domain, where the method by which the information is compiled is not generally known. These broad trade secret protections may operate to unwittingly ensnare foreign companies, whose own country's trade secret protections vary dramatically in scope, making routine business activities in the U.S. more susceptible to civil litigation, both domestically and abroad, as is illustrated by the following high-stakes international trade secrets litigations.

In 2009, DuPont filed suit in the Eastern District of Virginia against Korean conglomerate Kolon for misappropriation of trade secrets relating to its Kevlar fiber technology. Personal jurisdiction in the case was predicated primarily on a single meeting between Kolon employees and a former DuPont employee in Virginia, despite the fact that the alleged acts constituting the actual transfer of information took place in Korea. In September 2011, a jury found that Kolon willfully misappropriated 149 DuPont trade secrets in violation of the Virginia UTSA. Kolon was ordered to pay $920 million in damages and the district court entered a sweeping, worldwide shutdown injunction barring Kolon from producing its own fiber that competed with DuPont's Kevlar for an unprecedented twenty year period. Kolon sought, and was granted, a stay of the injunction pending appeal. In April 2014, the U.S. Court of Appeals for the Fourth Circuit reversed the jury verdict and ordered a new trial on the basis that the district court abused its discretion in excluding potentially relevant evidence related to the public disclosure of DuPont's alleged trade secrets in a prior litigation. DuPont entered a civil settlement agreement with Kolon, concurrent with Kolon's guilty plea on related criminal charges for violation of the Economic Espionage Act, before a second trial could take place.

In April 2012, Nippon Steel & Sumitomo Metal Corp. sued South Korean steel manufacturer Posco in New Jersey for patent infringement, false advertising, and unfair competition related to its steel manufacturing technology. Nippon simultaneously filed a theft of trade secrets case in Japan. Posco brought an action for declaratory judgment in Korea and sought reexamination of Nippon's U.S. patents. The patent issues were litigated in the United States while the trade secret issues were litigated abroad. Notably, Nippon successfully advocated for a modification of the protective order in the New Jersey district court litigation, which allowed Nippon to use confidential information disclosed in the U.S. litigation—through the broad U.S. discovery rules—in the foreign litigation.[7] Although Posco was granted a stay pending

[7] *Nippon Steel & Sumitomo Metal Corp. v. POSCO*, No.12-2429, 2014 U.S. Dist. LEXIS 154227 (D.N.J. Oct. 30, 2014).

appeal two weeks later, it is unclear what documents, if any, had already been transferred abroad.[8] The Federal Circuit ultimately overturned the district court's ruling that the confidential information obtained during the U.S. lawsuit could be used in the foreign litigation, finding that the district court improperly applied certain factors from the U.S. Supreme Court case *Intel Corp. v. Advanced Micro Devices, Inc.*[9] Although Nippon petitioned for *en banc* review, the lawsuit settled in September 2015 when Posco agreed to pay Nippon 30 billion yen ($250 million). This case underscores the risk that plaintiffs, when lacking jurisdiction for a trade secrets action in the U.S., will nonetheless attempt to use discovery obtained from civil, non-trade secrets proceedings in the U.S. to advance trade secrets actions pending in foreign tribunals.

In March 2014, Toshiba and SanDisk filed separate lawsuits against South Korean semiconductor manufacturer SK Hynix. Toshiba brought claims against Hynix in the Tokyo District Court under Japan's Unfair Competition Prevention Act, alleging wrongful acquisition of proprietary Toshiba information pertaining to flash memory. Separately, SanDisk filed suit in California state court alleging trade secret misappropriation under California's UTSA. SanDisk and Toshiba alleged that a former SanDisk engineer shared copies of technical documents that had been jointly developed by Toshiba and SanDisk with Hynix employees. The SanDisk engineer was convicted of criminal unfair competition in Japan for his role in the dispute. In July 2014, the California Superior Court issued a global preliminary injunction barring Hynix from using "any confidential, proprietary, and/or trade secret information."[10] The preliminary injunction did, however, allow Hynix to continue to sell products that were already qualified for commercial sale.[11] In December 2014, Toshiba and Hynix reached a settlement to end the civil litigation in Japan. Hynix reportedly paid $278 million as part of the settlement. In August 2015, SanDisk and Hynix announced a settlement to end the California litigation for an undisclosed payment. The dispute ultimately brought the three companies into a closer working relationship. As part of the SanDisk agreement, Hynix now produces computer memory and disk devices for SanDisk. Toshiba and Hynix have also agreed to collaborate in developing other types of computer memory.

The increasing globalization of trade has created an ever more complex web of rules and regulations governing the enforcement of judgments abroad. A win in the

[8] *Nippon Steel & Sumitomo Metal Corp. v. POSCO*, No. 12-2429, 2014 U.S. Dist. LEXIS 160979 (D.N.J. Nov. 14, 2014).

[9] 542 U.S. 241 (2004). The Court held that the relevant factors pertinent to requests for production of documents for use in foreign proceedings include: (1) whether the person from whom discovery is sought is a participant in the foreign proceeding; (2) the nature of the foreign tribunal, character of proceedings underway abroad, and receptivity of the foreign government or court or agency abroad to assistance from United States federal court; (3) whether production request conceals an attempt to circumvent foreign proof-gathering restrictions or other policies of the foreign country or the United States; and (4) whether the request is otherwise unduly intrusive or burdensome. *In re Posco*, 794 F.3d 1372 (Fed. Cir. 2015).

[10] *SanDisk Corp. v. SK Hynix, Inc., et.al*, No. 1-14-CV-262078 (Cal. Super. Ct. Jul. 1, 2014) (order granting preliminary injunction).

[11] *See id.*

courtroom no longer means a check in hand. Instead, when enforcing against a company with assets abroad—or a company based entirely abroad—litigators must become versed not just in U.S. enforcement processes, but with the different enforcement requirements in each of the jurisdictions where assets may be found. This process may take years, or even decades, to be completed, with no guarantee that at the end of the day the judgment may be enforced in full.

TRADE SECRETS LITIGATION HAS CRIMINAL COMPONENTS

The current federal statutory framework under the U.S. Economic Espionage Act ("EEA") provides for criminal prosecution and penalties for, among other acts, the knowing theft, duplication, or receipt of trade secrets.[12] Although many foreign companies are familiar with patent litigation in the U.S., which is civil in nature, they are less familiar with the civil and criminal aspects of trade secrets litigation in the U.S. Although the civil liability from a trade secrets suit can have severe consequences, including substantial damages and an injunction, federal criminal liability of a business for misappropriation of trade secrets under the EEA can be even more devastating, resulting in significant criminal fines, forfeiture of ill-gotten profits, and restitution to the aggrieved U.S. company.[13] Federal prosecutors also have the power to use pre-judgment attachment to seize a company's assets, even before trial, although it does not appear that the U.S. government has attempted this in any known EEA cases.[14]

---

[12] 18 U.S.C. § 1832 (2012).

[13] 18 U.S.C. §§ 1834, 2323 (2008).

[14] A conviction under the EEA authorizes, among other things, forfeiture of "[a]ny property used, or intended to be used, in any manner or part to commit or facilitate the commission of an offense" and "[a]ny property constituting or derived from any proceeds obtained directly or indirectly as a result of the commission of an offense." 18 U.S.C. § 2323(a)(1)(B) & (C) (2008); see *id.* § 1834 (applying section 2323 to trade secret offenses). Section 2323 further provides that criminal forfeitures, "including any seizure and disposition of the property and any related judicial or administrative proceeding, shall be governed by the procedures set forth in section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), other than subsection (d) of that section." 18 U.S.C. § 2323(b)(2)(A) (2008). Accordingly, 21 U.S.C. § 853(e) applies to trade secret forfeitures, which authorizes pre-trial protective orders, including restraining orders or performance bonds, at the request of the government. 21 U.S.C. § 853(e) (2009). Section 853 directly provides that such protective orders may include an order to "a defendant to repatriate any property that may be seized and forfeited, and to deposit that property pending trial in the registry of the court, or with the United States Marshals Service or the Secretary of the Treasury, in an interest-bearing account, if appropriate." *Id.* § 853(e)(4)(A). The government may also request a warrant to seize the property, which the court "shall issue" if a protective order under section 853(e) would not suffice to ensure the availability of the property for forfeiture. *Id.* § 853(f). The statute also permits the court to order forfeiture of "substitute property," if the defendant has transferred or commingled the forfeitable property with other property, up to the value of the transferred or commingled property. *Id.* § 853(p). Title to the forfeitable property is deemed as a matter of law to vest in the United States immediately upon the commission of the crime: "all right, title, and interest in property described [in the forfeiture statute] vests in the United States upon the commission of the act giving rise to forfeiture." *Id.* § 853(c).

The EEA was initiated in 1996 and clarified in December 2012 pursuant to the Theft of Trade Secrets Clarification Act (the "Clarification Act"). In light of the U.S. Court of Appeals for the Second Circuit's decision in *United States v. Aleynikov*,[15] the Clarification Act expanded the scope of Section 1832 of the EEA ("Theft of trade secrets") to include products or processes that may be used, or intended for use, in interstate or foreign commerce. Thus, the definition of trade secrets broadened under the EEA such that nearly any confidential and proprietary information of value, whether financial, business, technical, or other nature, can be viewed as a trade secret by federal prosecutors.[16]

Moreover, even if the subject information is not a trade secret, federal prosecutors can still pursue indictments if a conspiracy existed to obtain what the company or its employees thought were trade secrets.[17] Because the Economic Espionage Act carries a five-year statute of limitations[18] that begins to run from the date upon which the offense is "committed,"[19] federal prosecutors may attempt to pursue cases involving older wrongful acts based on conspiracy theories, for which the limitations period begins to run on the date of the last "overt act" committed in furtherance of the conspiracy.[20]

The Obama administration made "stamping out" intellectual property theft a "top priority" and has accordingly escalated federal administrative efforts to enforce the EEA.[21] In just two years (from 2010 to 2013), the number of trade secret theft

---

[15] 676 F.3d 71 (2d Cir. 2012).

[16] "[T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, the public." 18 U.S.C. § 1839 (1996).

[17] 18 U.S.C. § 1832 (a)(5) (2012).

[18] *See id.* § 1832(a), 18 U.S.C. § 3282(a) (2003).

[19] *See id.*

[20] Both the U.S. Department of Justice and courts have recognized as much. *See U.S. Dep't of Justice Criminal Resource Manual* § 652, http://www.justice.gov/usam/criminal-resource-manual-652-statute-limitations-conspiracy (acknowledging that for conspiracy statutes that contain an overt act requirement, the "statute of limitations begins to run on the date of the last overt act") (citations omitted); *United States v. Case*, No. 3:06-cr-210, 2008 U.S. Dist. LEXIS 34367, at *22–25 (S.D. Miss. Apr. 25, 2008) (applying five-year limitations period under 18 U.S.C. § 3282 to indictment alleging conspiracy under 18 U.S.C. § 1832(a)(5)), *aff'd in relevant part*, 309 F. App'x 883 (5th Cir. 2009); *see also United States v. Hsu*, 155 F.3d 189, 204 n.21 (3d Cir. 1998) (acknowledging that Section 1832(a)(5) contains an "overt act" requirement).

[21] *See, e.g.*, Press Release, U.S. Dep't of Justice, *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets* (Jun. 27, 2013), http://www.justice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets.

investigations performed by the Federal Bureau of Investigation (the agency primarily responsible for investigating domestic offenses under the EEA) increased 29 percent.[22] Between 2008 and 2013, the number of economic espionage arrests doubled, indictments increased five-fold, and convictions rose eight-fold.[23] The administration has also supported legislative efforts in Congress to heighten enforcement of the Economic Espionage Act.[24] In 2012, two relevant bills were passed.[25] The first, the Clarification Act, closed a loophole regarding computer source code.[26] The second, The Foreign and Economic Espionage Penalty Enhancement Act, strengthened criminal penalties for economic espionage and directed the sentencing commission to consider increasing offense levels for trade secret crimes.[27]

As of 2012, approximately 115 cases had been brought under Section 1832 of the EEA, as opposed to only nine cases under Section 1831.[28] Section 1831 violations require intent or knowledge that the misappropriation will "benefit any foreign government, foreign instrumentality or foreign agent."[29] Thus, according to these statistics, greater than ninety percent of EEA prosecutions include allegations of theft of trade secrets by individuals or organizations, many of which concern highly-sensitive technologies.

In the first federal jury conviction under the EEA, Walter Lian-Heen Liew, his company USA Performance Technology Inc., and Robert Maegerle were convicted of conspiracy to steal titanium dioxide production trade secrets from DuPont and selling those secrets for large sums of money to state-owned companies of the People's Republic of China ("PRC") to help those companies develop large-scale production

[22] Executive Office of the President, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* at 7 (Feb. 2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[23] Press Release, U.S. Dep't of Justice, *Sinovel Corporation and Three Individuals Charged in Wisconsin with Theft of AMSC Trade Secrets* (Jun. 27, 2013), http://www.justice.gov/opa/pr/sinovel-corporation-and-three-individuals-charged-wisconsin-theft-amsc-trade-secrets.

[24] Executive Office of the President, *Administration Strategy on Mitigating the Theft of U.S. Trade Secrets* at 11 (Feb. 2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] Peter J. Toren, *A Look at 16 Years of EEA Prosecutions*, Law360 (Sept. 19, 2012), http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions.

[29] 18 U.S.C. § 1831 (2013).

capabilities, including a planned 100,000-ton titanium dioxide factory. Liew was sentenced on June 10, 2014 to serve 15 years in prison, forfeit $27.8 million in illegal profits, and pay $511,667.82 in restitution.[30]

In April 2015, Kolon Industries Inc. entered a criminal plea agreement and agreed to pay $85 million in criminal fines and $275 million in restitution on charges of conspiracy to steal trade secrets concerning Kevlar. Two former DuPont employees who consulted for Kolon, Edward Schulz and Michael Mitchell, entered guilty pleas for their roles in the conspiracy. In 2010, Mitchell was sentenced to two concurrent 18 month prison terms and ordered to pay DuPont $188,000 in restitution for theft of trade secrets and obstruction of justice. In 2015, Schulz was sentenced to two years' probation, community service, and fined $75,000 for conspiracy to misappropriate trade secrets.

In May 2015, Tianjin University Professor Hao Zhang was arrested when he returned to the U.S. from China. Zhang and five others were indicted for stealing trade secrets from two U.S. companies concerning film bulk acoustic resonator ("FBAR") technologies, which have applications in consumer electronics and military communications technologies. As set forth in the indictment, Zhang and his co-conspirators are alleged to have stolen and shared with Tianjin University recipes, source code, specifications, presentations, design layouts and other trade secrets. Tianjin University in turn constructed a state-of-the-art FBAR fabrication facility in China and formed a joint venture to obtain contracts for providing FBARs to commercial and military entities.[31]

Also in May 2015, Chinese businessman, Xiwen Huang of Charlotte, N.C., was similarly arrested when he returned from a trip to China. Huang is alleged to have stolen trade secrets from a U.S. Government Research Facility and two U.S. companies, including trade secrets concerning military vehicle fuel cells, which he took with him to China to further his business interests. In October 2015, Huang agreed to plead guilty to stealing trade secrets.[32]

---

[30] Press Release, U.S. Dep't of Justice, *U.S. and Chinese Defendants Charged with Economic Espionage and Theft of Trade Secrets in Connection with Conspiracy to Sell Trade Secrets to Chinese Companies* (Feb. 8, 2012), http://www.justice.gov/opa/pr/us-and-chinese-defendants-charged-economic-espionage-and-theft-trade-secrets-connection.

[31] Press Release, U.S. Dep't of Justice, *Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People's Republic of China* (May 19, 2015), http://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets.

[32] Press Release, U.S. Dep't of Justice, *Chinese Businessman Charged with Theft of Trade Secrets* (Oct. 1, 2015), http://www.justice.gov/usao-wdnc/pr/chinese-businessman-charged-theft-trade-secrets.

THE U.S. GOVERNMENT EMBRACES ITS EXTRATERRITORIAL REACH IN EEA CASES

The U.S. government considers itself to have jurisdiction to prosecute a company or individual for violations of the EEA as long a one act in furtherance of the offense takes place on U.S. soil.[33] This could be something seemingly insignificant like conducting an interview of a potential lateral employee, a contractor, or a consultant to the company, or even directing email communications at the forum state. Activities like these, which have only the slightest nexus to the U.S., are now viewed by the U.S. Department of Justice ("DOJ") as sufficient to support jurisdiction over economic espionage conspiracy claims, even if all of the remaining wrongful activities occurred entirely outside the U.S. For example, in *U.S. v. Kolon Industries Inc.*, a single meeting between Kolon employees and a former DuPont employee in the United States, along with email communications, formed the primary basis for civil and criminal jurisdiction. Thus, the actions of one foreign employee while travelling to U.S. have the potential to subject the foreign employer to both civil and criminal trade secrets liability in the U.S.

Historically, foreign companies have attempted to avoid service of criminal indictments by not establishing a physical presence in the United States (if a foreign company has a U.S.-based affiliate, the DOJ will often attempt to serve process on the US-based affiliate of the foreign company pursuant to a civil alter ego theory). Foreign corporate defendants with no U.S. presence argue that under Criminal Rule 4(c)(3)(C), which addresses the manner of service of a criminal summons upon an organization, the U.S. government must both (1) deliver the summons to "an officer, to a managing or general agent, or to another agent appointed or legally authorized to receive service of process," and (2) mail the summons to the "organization's last known address within the district or to [the organization's] principal place of business elsewhere in the United States."[34] That is, under the plain language of Criminal Rule 4, a summons cannot be served outside the United States; it may only be served within the jurisdiction of the United States, making Rule 4 attempts of service ineffective against corporations with enterprises entirely outside of the United States.[35] However, the DOJ has asked the Advisory Committee on Criminal Rules to amend Criminal Rule 4

---

[33] *See* 18 U.S.C. § 1837(2) (1996).

[34] Fed. R. Crim. P. 4(c)(3)(C); *see also United States v. Pangang Grp. Co.*, 879 F. Supp. 2d 1052, 1064 65 (N.D. Cal. 2012).

[35] *See, e.g.*, *Pangang*, 879 F. Supp. 2d at 1057 58 (affirming that service under Rule 4 requires both mailing and delivery); *United States v. Chitron Elecs. Co.*, 668 F. Supp. 2d 298, 304 (D. Mass. 2009) (recognizing that both the Delivery and Mailing Requirements "are essential prerequisites to effective service"); *United States v. Johnson Matthey PLC*, No. 2:06-CR-169 DB, 2007 U.S. Dist. LEXIS 56510, at *2 (D. Utah. Aug. 2, 2007) ("Rule 4 has two requirements," *i.e.*, the Delivery and Mailing Requirements); *contra United States v. Kolon Indus., Inc.*, 926 F. Supp. 2d 794 (E.D. Va. 2013).

to "permit the effective service of a summons on a foreign organizational defendant" with no presence in the United States.[36] In particular, the DOJ requested removal of Criminal Rule 4(c)(3)(C)'s mailing requirement and an expansion of Criminal Rule 4(c)(2) to authorize service "at a place not within a judicial district of the United States."[37] The Advisory Committee, in turn, recognized that the current Rules "pose[] an obstacle to the prosecution of foreign corporations . . . that cannot be served because they have no last known address or principal place of business in the United States."[38] The amendment to Criminal Rule 4 is in its penultimate stage, having been submitted for approval to the Supreme Court in early October 2015.[39]

With federal prosecutors pushing the limits on their extraterritorial jurisdiction, the trend of foreign entities involved in both civil and criminal trade secrets litigation is expected to increase in the coming years, even where the vast majority of the wrongful conduct is overseas, the evidence is overseas, the actors are overseas, the business is overseas, and all the sales are overseas.

***

The second part of this article will appear in an upcoming issue of *Pratt's Privacy & Cybersecurity Law Report*.

[36] Letter from Lanny A. Breuer, then Ass't Att'y Gen., to the Hon. Reena Raggi, Chair of the Advisory Comm. on the Criminal Rules (Oct. 25, 2012), http://www.uscourts.gov/file/15532/download.

[37] *Id.*

[38] *Advisory Comm. on Criminal Rules, Durham, N.C* (Apr. 25–26, 2013), http://www.uscourts.gov/file/15532/download.

[39] U.S. Courts, *Pending Rules Amendments*, http://www.uscourts.gov/rules-policies/pending-rules-amendments.