

AN A.S. PRATT PUBLICATION

JUNE 2016

VOL. 2 • NO. 5

PRATT'S
**PRIVACY &
CYBERSECURITY
LAW**
REPORT



EDITOR'S NOTE: LOOKING FORWARD

Steven A. Meyerowitz

**A LOOK FORWARD IN PRIVACY &
CYBERSECURITY**

Rajesh De, Stephen Lilley, and Joshua Silverstein

**FDA RELEASES DRAFT GUIDANCE
ON POSTMARKET MANAGEMENT OF
CYBERSECURITY IN MEDICAL DEVICES**

Vanessa K. Burrows, Jennifer S. Geetter,
Daniel F. Gottlieb, and Michael W. Ryan

**CREDIT CARD DATA BREACHES: PROTECTING
YOUR COMPANY FROM THE HIDDEN
SURPRISES – PART II**

David A. Zetoon and Courtney K. Stout

**CRITICAL ISSUES FOR FOREIGN DEFENDANTS
IN INTERNATIONAL TRADE SECRETS
LITIGATION – PART II**

Jeffrey A. Pade

**RECENT PRIVACY & CYBERSECURITY
DEVELOPMENTS**

Samantha V. Ettari, Alan R. Friedman,
Arielle Warshall Katz, Erica D. Klein,
Daniel Lennard, and Harold Robinson

Pratt's Privacy & Cybersecurity Law Report

VOLUME 2

NUMBER 5

JUNE 2016

Editor's Note: Looking Forward

Steven A. Meyerowitz 151

A Look Forward in Privacy & Cybersecurity

Rajesh De, Stephen Lilley, and Joshua Silverstein 153

**FDA Releases Draft Guidance on Postmarket Management of Cybersecurity
in Medical Devices**

Vanessa K. Burrows, Jennifer S. Geetter, Daniel F. Gottlieb, and Michael W. Ryan 162

**Credit Card Data Breaches: Protecting Your Company from the Hidden
Surprises – Part II**

David A. Zetoony and Courtney K. Stout 167

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

Jeffrey A. Pade 174

Recent Privacy & Cybersecurity Developments

Samantha V. Ettari, Alan R. Friedman, Arielle Warshall Katz, Erica D. Klein,
Daniel Lennard, and Harold Robinson 182

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@lexisnexus.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.lexisnexus.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 [153] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license. A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2016 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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.lexisnexus.com

MATTHEW  BENDER

(2016–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF

STEVEN A. MEYEROWITZ

President, Meyerowitz Communications Inc.

EDITOR

VICTORIA PRUSSEN SPEARS

Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

EMILIO W. CIVIDANES

Partner, Venable LLP

RICHARD COHEN

Special Counsel, Kelley Drye & Warren LLP

CHRISTOPHER G. C WALINA

Partner, Holland & Knight LLP

RICHARD D. HARRIS

Partner, Day Pitney LLP

DAVID C. LASHWAY

Partner, Baker & McKenzie LLP

CRAIG A. NEWMAN

Partner, Patterson Belknap Webb & Tyler LLP

ALAN CHARLES RAUL

Partner, Sidley Austin LLP

AARON P. SIMPSON

Partner, Hunton & Williams LLP

RANDI SINGER

Partner, Weil, Gotshal & Manges LLP

JOHN P. TOMASZEWSKI

Senior Counsel, Seyfarth Shaw LLP

TODD G. VARE

Partner, Barnes & Thornburg LLP

THOMAS F. ZYCH

Partner, Thompson Hine

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. Copyright 2016 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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 II

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. The first part of the article, which appeared in the May 2016 issue of Pratt's Privacy & Cybersecurity Law Report, explored 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. This second part of the article focuses 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.

FEDERAL PROSECUTORS WILL PURSUE CRIMINAL PROSECUTION WHILE CIVIL TRADE SECRETS LITIGATION IS ONGOING OR CONTEMPLATED

The DOJ has had a longstanding policy that federal prosecutors and civil attorneys handling white-collar matters “should timely communicate, coordinate, and cooperate with one another and with agency attorneys to the fullest extent appropriate to the case and permissible by law.”¹ If a foreign company is sued in the U.S. by a U.S. competitor for misappropriation of trade secrets or receives a threatening letter containing a similar allegation, the foreign company should be wary of possible criminal prosecution—even without any formal threat of prosecution from the U.S. government. U.S. plaintiffs strategically seek to involve federal prosecutors in the dispute, because the threat of criminal indictment and prosecution gives U.S. plaintiffs important leverage in civil trade secrets litigation, particularly against foreign defendants that are typically outside the subpoena power of the U.S. government. U.S. plaintiffs may file a complaint with the government describing the foreign company's actions and the U.S. government may quietly cooperate with the U.S. plaintiff, as a victim. Thus, any communication that a foreign company has with a U.S. plaintiff or potential plaintiff may be turned over the U.S. government. If the U.S. government has already gathered evidence of the

* 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 U.S. Attorneys' Manual, *Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings*, Title 1, Chapter 1-12.000 (Nov. 2015), <http://www.justice.gov/usam/usam-1-12000-coordination-parallel-criminal-civil-regulatory-and-administrative-proceedings>.

conduct of the foreign company, the executives of the foreign company who may unwittingly travel to the U.S. could be detained. For example, Chinese businessman and U.S. national, Xiwen Huang, was arrested after returning from China, months before he was formally charged by the U.S. government with one count of theft of trade secrets,² and Chinese national, Hao Zhang, was arrested at the Los Angeles airport upon landing from a flight from China, prior to the U.S. government unsealing his indictment.³ Foreign trade secrets defendants need to be careful, anticipate potential criminal investigations, and not blindly turn over documents or formal discovery to U.S. plaintiffs, even as part of a settlement. It is therefore critically important that foreign companies doing business in the U.S. develop comprehensive strategies to address the risks of potential parallel civil and criminal trade secrets proceedings.

PARALLEL CIVIL AND CRIMINAL TRADE SECRETS PROCEEDINGS CREATE UNIQUE OPPORTUNITIES AND RISKS

Civil discovery rules require careful consideration for foreign defendants embroiled in U.S. trade secrets litigation. Most courts agree that companies threatened with U.S. litigation have a duty to preserve relevant documents. This becomes of primary importance in trade secrets cases for corporate defendants because employees' deletion of relevant documents not only may result in a finding of spoliation in the civil case (and associated sanctions),⁴ but the DOJ can also criminally prosecute companies and individuals who delete documents for obstruction of justice, which is a separate criminal offense from trade secrets misappropriation.⁵ These issues are even more acute for foreign businesses whose local laws often allow only limited or no civil

² 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>.

³ 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>.

⁴ *E.I. du Pont de Nemours and Co. v. Kolon Indus., Inc.*, 803 F. Supp. 2d 469 (E.D. Va. 2011) (awarding the plaintiff attorneys' fees, expenses, costs and an adverse inference jury instruction instead of a default judgment because, notwithstanding the alleged bad faith deletion conduct of employees, Kolon implemented litigation holds and means to preserve files and many deleted items were recoverable because of preserved back-up tapes).

⁵ See 18 U.S.C. §§ 1512(c)(1)–(2) (2008) (“Whoever corruptly—(1) alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object’s integrity or availability for use in an official proceeding; or (2) otherwise obstructs, influences, or impedes any official proceeding, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both.”); *id.* § 1519 (“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States . . . or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.”).

discovery and whose employees might not understand the broad U.S. civil discovery standards and preservation obligations, particularly for electronically stored information.

Foreign businesses subject to civil trade secrets suits should also understand that the documents produced in a civil trade secrets case might be turned over to federal prosecutors and then used against the company and its employees in criminal cases. U.S. prosecutors have few avenues to obtain documents and other evidence located outside of the United States because a federal grand jury subpoena may only be served in the United States or on a United States national or resident in a foreign country.⁶ However, once documents are moved into U.S. jurisdiction, then the DOJ may consider them subject to a grand jury's extensive subpoena power.⁷ Further, some courts consider a foreign document obtainable via grand jury subpoena when a branch of the corporation being subpoenaed "has purposefully availed itself of the privilege of conducting activities within the United States," by having sufficient contacts with the U.S.⁸ These liberal interpretations of a grand jury's reach allow the DOJ to serve a "friendly subpoena" to a civil adversary or related party to obtain documents produced during discovery in a civil trade secrets litigation and then use those documents as evidence in the criminal case against the company and any individuals involved in the wrongdoing. This can occur even when a grand jury's subpoena conflicts with the safeguards of a valid and agreed-upon protective order.⁹

Another aspect of trade secrets litigation that foreign entities often underestimate is the tendency of U.S. federal prosecutors to require self-disclosure and elaborate corporate cooperation while simultaneously pursuing criminal actions against foreign companies' executives and other individuals. It has become increasingly difficult for

⁶ See, e.g., 28 U.S.C. § 1783 (1964) and Fed. R. Crim. P. 17(e)(2); see also *United States v. Moussaoui*, 382 F.3d 453, 462–64 (4th Cir. 2004) (noting the "well established and undisputed principle that the process power of the district court does not extend to foreign nationals abroad"); *United States v. Theresius Filippi*, 918 F.2d 244, 246 n. 2 (1st Cir. 1990) ("The United States has no subpoena power over a foreign national in a foreign country").

⁷ *In re Grand Jury Subpoena*, 646 F.3d 159, 166 (4th Cir. 2011); *In re Grand Jury Subpoenas*, 627 F.3d 1143, 1144 (9th Cir. 2010) cert. denied, 131 S. Ct. 3061, 180 L. Ed. 2d 903 (U.S. 2011) and cert. denied, 131 S. Ct. 3062, 180 L. Ed. 2d 903 (U.S. 2011) ("[b]y a chance of litigation, the documents have been moved from outside the grasp of the grand jury to within its grasp. No authority forbids the government from closing its grip on what lies within the jurisdiction of the grand jury.").

⁸ *In re Grand Jury* 81-2, 550 F. Supp. 24, 27 (W.D. Mich. 1982); see also *Ghandi v. Police Dept. of City of Detroit*, 74 F.R.D. 115, 121 (E.D. Mich. 1977) ("[a] foreign corporation doing business in a district is subject to all process, including subpoena, in the district, and if the documents are required in response to a subpoena, the court has the power to order their production even though they are physically located outside of the jurisdiction.").

⁹ *In re Grand Jury Subpoena*, 646 F.3d at 168 ("There is a per se rule in the Fourth Circuit favoring the 'enforcement of a grand jury subpoena despite the existence of an otherwise valid protective order.');" see also *In re Grand Jury Subpoenas*, 627 F.3d at 1144 ("grand jury subpoena takes precedence over a civil protective order").

companies to resolve incidents of economic espionage without revealing the names of the individuals involved in the corporate misconduct. In September 2015, the Deputy Attorney General issued a broad and expansive policy (the “Yates memorandum”) that reinforces and expands on EEA policy imperatives.¹⁰ In the Yates memorandum, the DOJ made clear that if a company attempting to settle with the DOJ desires credit¹¹ for cooperating with the DOJ, the only way that it can get that credit is by conducting a thorough internal investigation of the wrongful activities, agreeing to share the results of that investigation, and also divulging the names of all individuals that participated in the alleged wrongdoing.¹² In this manner, the DOJ can use cooperation credit to obtain overseas evidence from foreign businesses that the U.S. government might not normally be able to access (as it is outside the scope of a federal grand jury subpoena). Thus, to obtain some leniency and reduced corporate penalties, foreign companies are encouraged to voluntarily turn over information that is typically outside the reach of federal prosecutors and to assist in the identification and prosecution of their own employees. Of course, this barter can make it extremely difficult for foreign companies to remain loyal to employees, as there is a strong possibility that the interests of the business may become adverse to those of a particular individual, which may also conflict with local culture, habits, and social expectations. Companies and individuals should therefore make early decisions about the need for separate counsel for employees at all levels when misconduct is identified.

Once the DOJ identifies and pursues employees involved in the alleged wrongdoing, it then becomes arduous for foreign companies to extricate the company from the potential criminal exposure without having to separately resolve a criminal case against the individuals. This is primarily because the DOJ is reluctant to allow an indicted company to resolve an issue of economic espionage globally without a plan to resolve related individual criminal cases as well, including separately speaking with independent counsel for any indicted employees of the company. In the Yates memorandum, the DOJ emphasized that the U.S. government should not settle with a company without also attempting to settle with any indicted employees: “absent extraordinary circumstances . . . Department lawyers should not agree to a corporate resolution that includes an agreement to dismiss charges against, or provide immunity for, individual officers or employees.”¹³ Likewise, the DOJ is similarly reluctant to “release claims

¹⁰ Memorandum from Deputy Att’y Gen. Sally Q. Yates to the Ass’t Att’y Gen., Antitrust Div., et al., *Individual Accountability for Corporate Wrongdoing* (Sep. 9, 2015), <http://www.justice.gov/dag/file/769036/download> (“Yates memorandum”).

¹¹ See Memorandum from Deputy Att’y Gen. Mark Filip to Heads of Dep’t Components, United States Att’ys, *Principles of Federal Prosecution of Business Organizations* (Aug. 28, 2008), <http://www.justice.gov/sites/default/files/dag/legacy/2008/11/03/dag-memo-08282008.pdf> (the “Filip memorandum”). The Filip memorandum, which has been set forth in the United States Attorney’s Manual at § 9-28.000 et seq., is binding on federal prosecutors within the DOJ.

¹² Yates memorandum at 3.

¹³ *Id.* at 5.

related to the liability of individuals based on corporate settlement releases.”¹⁴ Foreign companies trying to resolve corporate EEA indictments should therefore anticipate the DOJ simultaneously seeking accountability of culpable individuals, whose potential cooperation could impact both civil and criminal litigation strategies. If faced with a government indictment, possible culpable employees may wish to minimize their personal liability and divulge any involvement in funneling trade secrets to their employer, in exchange for leniency from the government.

CROSS-BORDER INVESTIGATIONS AND FUTURE DEVELOPMENTS

Foreign corporate defendants should also be mindful that a U.S. civil action can spawn multiple criminal investigations across different jurisdictions. U.S. trade secrets plaintiffs have ample incentive to help initiate foreign investigations of defendants to help advance U.S. criminal prosecutions of the business entity and any culpable individuals. These efforts to initiate foreign investigations may include filing formal complaints with regulators that might include evidence produced during U.S. civil discovery. When many aspects of the alleged wrongdoing occurred overseas, foreign defendants risk that they may have also violated foreign laws, truly creating a global dispute. Cooperation between foreign law enforcement agencies in intellectual property investigations is expected to increase in coming years, resulting in governments willingly and increasingly sharing information and participating in investigations and prosecutions across multiple jurisdictions, particularly where cross-border investigations yield hefty corporate penalties. Defendants should keep in mind, however, that in the right situation, they too can initiate such an investigation and can use that foreign governmental investigation as leverage against the plaintiff.

The United States Department of State, in cooperation with the DOJ, has negotiated and entered into mutual legal assistance treaties (“MLATs”) with over 50 countries that generally allow for the exchange of evidence and information in criminal investigations.¹⁵ In 2010, the United States entered into 27 additional instruments, agreements, and/or protocols that supplement or create MLATs between the United States and every member of the European Union.¹⁶ In 2000, the United States entered into a Mutual Legal Assistance Agreement (“MLAA”) with China, providing for cooperation in international investigation of criminal matters.¹⁷ Under both the China MLAA and the MLATs, the country from whom assistance is

¹⁴ *Id.*

¹⁵ See U.S. Dep’t of State, *2012 International Narcotics Control Strategy Report (INCSR)* (Mar. 7, 2012), <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>.

¹⁶ See *id.*

¹⁷ U.S. Dep’t of Commerce, *U.S. Fact Sheet: 26th U.S.-China Joint Commission on Commerce and Trade* (Nov. 23, 2015), <https://www.commerce.gov/news/fact-sheets/2015/11/us-fact-sheet-26th-us-china-joint-commission-commerce-and-trade>.

being requested may typically deny assistance if the conduct being investigated does not constitute an offense in that country.¹⁸ In the context of criminal narcotics investigation, the US government has sought to entice cooperation of foreign governments in joint investigations by sharing forfeited assets. Between 1989 and 2011, the DOJ, through its international asset sharing program, shared over \$230MM of forfeited assets with foreign governments that cooperated and assisted with criminal investigations.¹⁹ It would not be surprising to see the DOJ offer similar asset sharing incentives in the context of international EEA investigations, particularly where it is inappropriate or impossible to pass the forfeited assets to an injured party.

Just this November, the United States and China held the Joint Commission for Commerce and Trade (“JCCT”) in Guangzhou, China.²⁰ Among other initiatives, preventing and coordinating the prosecution of trade secret theft is a key component of the JCCT’s mission. China informed the United States that it is in the process of amending its Anti-Unfair Competition Law and is taking other measures to bolster trade secret protection in its country.²¹ The United States and China also agreed “to jointly share experiences and practices in the areas of protecting trade secrets from disclosure during investigations and in court proceedings, and identify practices that companies may undertake to protect trade secrets from misappropriation in accordance with respective laws.”²²

Nearly every nation provides some legal protection for trade secrets. For example, the Agreement on Trade Related Aspects of Intellectual Property Rights (“TRIPS”), an international agreement administered by the World Trade Organization (“WTO”), establishes minimum standards for intellectual property protection by WTO members. With respect to trade secrets, TRIPS requires member nations to provide a means for protecting the disclosure, acquisition, or use by third parties without consent of information that is secret (*i.e.*, not generally known or readily ascertainable), has commercial value because it is secret, and has been subject to reasonable efforts to retain secrecy.²³ Note that TRIPS does not define the term “information,” giving

¹⁸ See, e.g., *id.* at Article 3(1)(a).

¹⁹ See U.S. Dep’t of State, *2012 International Narcotics Control Strategy Report (INCSR)* (Mar. 7, 2012), <http://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm>.

²⁰ U.S. Dep’t of Commerce, *U.S. Fact Sheet: 26th U.S.-China Joint Commission on Commerce and Trade* (Nov. 23, 2015), <https://www.commerce.gov/news/fact-sheets/2015/11/us-fact-sheet-26th-us-china-joint-commission-commerce-and-trade>.

²¹ *Id.*

²² *Id.*

²³ World Trade Organization, *Agreement on Trade-Related Aspects of Intellectual Property Rights*, https://www.wto.org/english/tratop_e/trips_e/t_agm3d_e.htm#7.

WTO members some latitude to broadly or narrowly interpret the term as they see fit. The United States routinely encourages signatories to free trade agreements to provide intellectual property protections that exceed those specified in TRIPS (often referred to as “TRIPS-Plus” provisions).²⁴

Although the Economic Espionage Act criminalizes the theft of trade secrets and conspiracies or attempts to steal trade secrets, it does not currently provide a private civil action for aggrieved parties. Although the UTSA intended to codify and harmonize trade secrets misappropriation standards, the current differences between state trade secrets laws and their judicial interpretations continue to raise complaints of forum-shopping. Legislators and commentators have therefore recommended that Congress consider amending the EEA to provide a federal civil cause of action for the misappropriation of trade secrets, thereby streamlining a medley of federal criminal laws and state civil statutes. One House version of the new bill would “create a civil cause of action and allow companies to enforce their rights in federal court.”²⁵ The bill also adopts the protections of the UTSA, including making unlawful the acquisition, disclosure, or use of trade secrets, along with remedies of injunctive relief, damages, and attorneys’ fees. The bill further creates *ex parte* seizure rights, meaning litigants may pursue an order seizing property to preserve evidence or to prevent the dissemination of trade secrets at issue in the action. If the bill eventually becomes law, it would supplement the EEA by creating a uniform standard for trade secret misappropriation cases in federal courts, which is expected to increase U.S. district court trade secrets filings and make court-supervised cooperation between federal prosecutors and civil litigants even more commonplace.

CONCLUSION

Although the Economic Espionage Act criminalizes the theft of trade secrets and conspiracies or attempts to steal trade secrets, it does not currently provide a private civil action for aggrieved parties. The UTSA intended to codify and harmonize trade secrets misappropriation standards, but the current differences between state trade secrets laws and their judicial interpretations continue to raise complaints of forum-shopping. Legislators and commentators, therefore, recommended that Congress consider amending the EEA to provide a federal civil cause of action for the misappropriation of trade secrets, thereby streamlining a medley of federal criminal laws and state civil statutes.

On April 27, 2016 the U.S. House of Representatives passed the Defend Trade Secrets, which creates a civil cause of action and allows companies to enforce their trade

²⁴ See Alexander W. Koff, et al., *Study on the Economic Impact of “TRIPS-Plus” Free Trade Agreements* (Aug. 10, 2011), <http://iipi.org/wp-content/uploads/2011/09/IIPi-USPTO-TRIPS-Plus-Study-10-Aug-2011.pdf>.

²⁵ Statement by Ranking Member John Conyers (D-MI), dated July 29, 2014.

secrets rights in federal court.²⁶ The Defend Trade Secrets Act also adopts the protections of the UTSA, including making unlawful the acquisition, disclosure, or use of trade secrets, along with remedies of injunctive relief, damages, and attorneys' fees. The act further creates *ex parte* seizure rights, meaning litigants may pursue an order seizing property to preserve evidence or to prevent the dissemination of trade secrets at issue in the action.

When the act eventually becomes law, it will supplement the EEA by creating a uniform standard for trade secret misappropriation cases in federal courts, which is expected to increase U.S. District Court trade secrets filings and make court-supervised cooperation between federal prosecutors and civil litigants even more commonplace.

²⁶ House Judiciary Committee Transcript at 5:68-72, dated Sep. 17, 2014 (Statement by House Judiciary Committee Chairman Bob Goodlatte (R-VA)).