


2017

Ex Parte Seizures Under the DTSA and the Shift of IP Rights Enforcement

Yvette Joy Liebesman

Follow this and additional works at: <https://scholarship.law.slu.edu/faculty>

 Part of the [Antitrust and Trade Regulation Commons](#), and the [International Trade Law Commons](#)

2017

Ex Parte Seizures Under the DTSA and the Shift of IP Rights Enforcement

Yvette Joy Liebesman

Follow this and additional works at: <https://scholarship.law.missouri.edu/betr>

 Part of the [Intellectual Property Law Commons](#)

Recommended Citation

Yvette J. Liebesman, *Ex Parte Seizures Under the DTSA and the Shift of IP Rights Enforcement*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 390 (2017).

Available at: <https://scholarship.law.missouri.edu/betr/vol1/iss2/4>

This Conference Proceeding is brought to you for free and open access by the Law Journals at University of Missouri School of Law Scholarship Repository. It has been accepted for inclusion in The Business, Entrepreneurship & Tax Law Review by an authorized editor of University of Missouri School of Law Scholarship Repository.

Symposium Article

Ex Parte Seizures Under the DTSA and the Shift of IP Rights Enforcement

Yvette Joy Liebesman*

Abstract

The ex parte seizure provision of the Defend Trade Secrets Act is another step in a long line of legislation that shifts the costs of private enforcement to the public, which already has a toehold in copyright and trademark law. The ex parte provision—which is not incorporated into any state trade secret law—relieves rights owners of two “burdens.” First, it relieves the trade secret owner of the burden of actually having to compete in the marketplace. Second, it relieves the trade secret owner of the burden of the costs associated with the discovery process of a lawsuit. The effect of this cost shifting results in anticompetitive behavior, is ripe for abuse, and offers no added benefit to what is provided via state trade secret causes of action and remedies.

This essay is based on Professor Yvette Joy Liebesman’s presentation at the March 10, 2017 Symposium on “Implementing and Interpreting the Defend Trade Secrets Act of 2016,” hosted by the University of Missouri School of Law’s Center for Intellectual Property and Entrepreneurship and the School’s Business, Entrepreneurship & Tax Law Review.

I. INTRODUCTION

This article will discuss the provision under the federal Defend Trade Secrets Act¹ (“DTSA”) that allows for *ex parte* seizures of goods which are alleged to be produced via the misappropriation of trade secrets and materials that are alleged to contain misappropriated trade secrets—such as laptops, media storage, and paper documents.² Several trade secret scholars have written extensively regarding substantive issues surrounding the *ex parte* seizure provision and its enforcement.³ This article focuses on how the *ex parte* seizure provision follows a trend by which rights owners have steadily sought to shift enforcement of private intellectual property rights from themselves to taxpayers and other entities.

Cost shifting has become so ubiquitous that we do not even realize it is happening. For example, we have all seen these notices: “go green,” “get your bank statement, credit card bill, or W-2 online”, and “save the planet!” However, many of us want that paper copy. So, if I choose to “go green” and have the document sent to me electronically, what is really happening is cost shifting. When a document is sent to consumers through

* Professor of Law, Saint Louis University School of Law. The author wishes to thank Prof. Dennis Crouch and the editors of the Missouri Business, Entrepreneurship & Tax Law Review for organizing the symposium, and for the invitation to participate. She is also grateful for comments and suggestions from David Levine, and for the help of her very capable research assistant, Rachel Jag.

¹ Defend Trade Secrets Act, 18 U.S.C.A. § 1836 (West 2016).

² See, e.g., *Earthbound Corp. v. MiTek USA, Inc.*, 2016 WL 4418013, at *11 (W.D. Wash. Aug. 19, 2016) (ordering Defendants to “immediately deliver to a neutral third-party expert in the greater Seattle area all flash drives, SD cards, cell phones, and other external drives used by the individual defendants . . . that are in Defendants' possession, custody, or control.”).

³ See, e.g., Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 WASH. & LEE L. REV. ONLINE 284 (2015) [hereinafter *Ex Parte Seizures*]; David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015); Eric Goldman et al., *Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326)*, CYBERLAW.STANFORD.EDU 1 (Nov. 17, 2015), <https://cyberlaw.stanford.edu/files/blogs/2015%20Professors%20Letter%20in%20Opposition%20to%20DTSA%20FINAL.pdf> [hereinafter *Professors' Letter*].

the U.S. Postal Service, the institution that created the document pays for the printing and mailing.⁴ Alternatively, if the document is sent electronically, those costs are absorbed by consumers who choose to “go green,” but still want the paper document. Similarly, this cost shifting has been an ongoing theme with intellectual property law enforcement; the latest target is enforcement of trade secrets through the *ex parte* seizure provision under the federal DTSA, a right not provided by any state trade secret statute.⁵

The DTSA’s *ex parte* seizure provision relieves rights owners of two “burdens.” First, it relieves the trade secret owner of the burden of actually having to compete in the marketplace.⁶ Second, it relieves the trade secret owner of the burden of the costs associated with the discovery process of a lawsuit.⁷ Thus, this provision has the strong potential to become an anti-competitive arrow in intellectual property owners’ quivers.

II. THE COST SHIFTING EVOLUTION IN INTELLECTUAL PROPERTY LAW

Before delving into the *ex parte* seizure provision as a new enforcement tool found within the DTSA, this article will first illustrate how this trend of enforcement shifting—and thus, cost shifting—is already present with trademark and copyright rights.⁸

⁴ See generally Jane Porter, *10 Ways to Trim Shipping Costs*, ENTREPRENEUR (Oct. 17, 2012), <https://www.entrepreneur.com/article/224619>.

⁵ *Ex Parte Seizures*, *supra* note 3, at 285.

⁶ Eric Goldman, David S. Levine, & Sharon K. Sandeen, *Federal Trade Secret Bill Re-Introduced—and It’s Still Troublesome*, TECH. & MARKETING L. BLOG (Aug. 4, 2015), <http://blog.ericgoldman.org/archives/2015/08/federal-trade-secret-bill-re-introduced-and-its-still-troublesome-guest-blog-post.htm>.

⁷ See William P. Glenn, Jr., *Ex-Parte Seizure of Intellectual Property Goods*, 9 TEX. INTELL. PROP. L. J. 307, 309 (2001).

⁸ Another area where cost shifting has occurred—with serious constitutional implications—is in the criminal justice system, local governments have shifted the burden of trials and custody from taxpayers to defendants—even when acquitted—to cover court/trial and custodial costs. See, e.g., Joseph Shapiro, *As Court Fees Rise, the Poor Are Paying the Price*, NPR (May 19, 2014), <http://www.npr.org/2014/05/19/312158516/increasing-court-fees-punish-the-poor> (noting that while this is a shift from public to private cost shifting, it shifts the

Trademark and copyright owners have been successful in persuading Congress to legislatively expand and shift enforcement duties to governmental bodies and other entities regarding private intellectual property rights beyond customary importation authority.⁹

1. Stopping the Importation of Counterfeit Goods at the Border via Customs and Border Patrol, and the Importance of Having a Registered Mark

Under both the Lanham Act¹⁰ and the Tariff Act of 1930,¹¹ Customs and Border Protection (“CBP”) has long had the authority to seize counterfeit goods at the border.¹² At ports of entry, CBP personnel regularly

financial burden onto defendants rather than the party instigating the court action, the government).

⁹ See *Protecting Intellectual Property Rights (IPR) Overseas*, U.S. PAT. & TRADEMARK OFF., <https://www.uspto.gov/patents-getting-started/international-protection/protecting-intellectual-property-rights-ipr> (last visited Dec. 8, 2017).

¹⁰ 15 U.S.C. § 1124 (2012) (“[N]o article of imported merchandise which shall copy or simulate the name of any domestic manufacture, or manufacturer, or trader, or of any manufacturer or trader located in any foreign country which, by treaty, convention, or law affords similar privileges to citizens of the United States, or which shall copy or simulate a trademark registered in accordance with the provisions of this chapter . . . shall be admitted to entry at any customhouse of the United States[.]”); 19 C.F.R. § 133.21(b)(1) (2016) (“CBP may detain any article of domestic or foreign manufacture imported into the United States that bears a mark suspected by CBP of being a counterfeit version of a mark that is registered with the U.S. Patent and Trademark Office.”).

¹¹ See 19 U.S.C. § 1526(b) (2012) (“Any such merchandise imported into the United States in violation of the provisions of this section shall be subject to seizure and forfeiture for violation of the customs laws.”); see also *Customs Border Protection Increases Seizure of Counterfeit and Pirated Goods in 2008*, SHIPMAN & GOODWIN LLP (Apr. 3, 2009), <http://www.shipmangoodwin.com/customs-border-protection-increases-seizure-of-counterfeit-and-pirated-goods-in-2008>.

¹² 19 C.F.R. § 133.21(a) (“A ‘counterfeit mark’ is a spurious mark that is identical with, or substantially indistinguishable from, a mark registered on the Principal Register of the U.S. Patent and Trademark Office.”) (emphasis added).

seize counterfeit and otherwise infringing toys, computers, DVD, handbags, apparel, shoes, and consumer electronics.¹³

The reliance on CBP to seize counterfeit goods is a huge benefit to the rights owners. We are probably all familiar with the recent Supreme Court decision of *Matal v. Tam*, where the Court held that the United States Patent and Trademark Office's ("USPTO") ban on registering offensive marks under § 2(a) of the Lanham Act¹⁴ was an unconstitutional viewpoint restriction on speech.¹⁵ What would have happened if the Supreme Court had upheld the Trademark Office's ability to refuse registration of offensive marks? In *Matal v. Tam*, the Supreme Court explained that,

[w]ithout federal registration, a valid trademark may still be used in commerce. And an unregistered trademark can be enforced against would-be infringers in several ways. Most important, even if a trademark is not federally registered, it may still be enforceable under §43(a) of the Lanham Act, which creates a federal cause of action for trademark infringement . . . [u]nregistered trademarks may also be entitled to protection under other federal

¹³ See Reinaldo Rodriguez, *CBP Intellectual Property Rights Seizure Statistics FY 2016*, TAGGART INT'L, LTD. (Jan. 23, 2017), <https://www.taggart-intl.com/cbp-intellectual-property-rights-seizure-statistics-fy-2016/>; see also Thomas C. Frohlich, Alexander E.M. Hess, & Vince Calio, *9 Most Counterfeited Products in the USA*, USA TODAY (Mar. 29, 2014), <https://www.usatoday.com/story/money/business/2014/03/29/24-7-wall-st-counterfeited-products/7023233/>.

¹⁴ 15 U.S.C. § 1052(a) (2012).

¹⁵ *Matal v. Tam*, 137 S.Ct. 1744, 1751 (2017) (holding that the Patent and Trademark Office's denial of a trademark registration "application based on a provision of federal law prohibiting the registration of trademarks that may 'disparage . . . or bring . . . into contemp[t] or disrepute' any 'persons, living or dead' . . . violates the Free Speech Clause of the First Amendment. It offends a bedrock First Amendment principle: Speech may not be banned on the ground that it expresses ideas that offend.") (internal citation omitted).

statutes, such as the Anticybersquatting Consumer Protection Act And an unregistered trademark can be enforced under state common law, or if it has been registered in a State, under that State's registration system.¹⁶

While the Court explicitly stated that it would not decide whether a mark owner “could bring suit under § 43(a) if his application for federal registration had been lawfully denied under the disparagement clause,”¹⁷ this discussion will assume that a ban on registerability under § 2 of the Lanham Act¹⁸ will not render the mark unenforceable as an unregistered mark under § 43(a)(1)(A).¹⁹ Why would Dan Snyder, owner of the Washington, D.C. professional football team,²⁰ or the National Football League care about registration if they can continue to enforce their offensive mark that disparages native Americans as an unregistered mark under § 43(a)(1)(A)? Because, as noted by the Supreme Court, if they want

¹⁶ *Id.* at 1752-53 (internal citations and quotations omitted).

¹⁷ *Id.* at 1753.

¹⁸ See 15 U.S.C. § 1052(a) (listing additional grounds for refusal of registration that are still in effect after the Tam decision).

¹⁹ 15 U.S.C. § 1125(a)(1)(A) (2012)

Any person who, on or in connection with any goods or services . . . uses in commerce any word, term, name symbol, or device, or any combination thereof, or any false designation or origin, false or misleading description of fact, or false or misleading representing of fact, which is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities by another person . . . shall be liable in civil action by any person who believes that he or she is *or* is likely to be damaged by such act.

(emphasis in original).

²⁰ *Dan Snyder*, FORBES (Dec. 8, 2017), <https://www.forbes.com/profile/dan-snyder/>.

governmental authorities to stop infringing goods from entering the country, the mark owner must present a valid registration to CBP.²¹

Both § 42 of the Lanham Act²² and § 526 of the Tariff Act of 1930²³ prohibit the importation of merchandise bearing a registered trademark without the mark owner's consent, therefore, no registration of the mark translates to no CBP.²⁴ Without registration of their mark, Dan Snyder and the NFL would still be able to sue infringers and sue for damages and

²¹ See *Matal v. Tam*, 137 S.Ct. 1744, 1753 (2017) (“Registration . . . enables the trademark holder to stop the importation into the United States of articles bearing an infringing mark.”) (internal citation and quotations omitted); see also 19 U.S.C. § 1526(a) (2012)

[I]t shall be unlawful to import into the United States any merchandise of foreign manufacture if such merchandise, or the label, sign, print, package, wrapper, or receptacle, bears a trademark owned by a citizen of, or by a corporation or association created or organized within, the United States, and registered in the Patent and Trademark Office. . . . a copy of the certificate of registration of his trademark . . . shall be kept . . . in the Department of the Treasury. . . and thereupon the Secretary of the Treasury shall cause one or more copies of the same to be transmitted to each collector or other proper officer of customs.

(emphasis added).

²² 15 U.S.C. § 1124.

²³ 19 U.S.C. § 1526.

²⁴ Though because there are situations where it be difficult for CBP agents to determine when goods are, in fact, counterfeit, enforcement is discretionary. See *Olympus Corp. v. U.S.*, 792 F.2d 315, 320 (2d Cir. 1986)

The administrative difficulties inherent in requiring the Customs Service to exclude gray market goods make clear why Customs has long and consistently interpreted section 526 to allow it to refuse to exclude the goods. Absent this bright line for administrative enforcement, the Customs Service would expend resources excluding goods when later private litigation could disclose that the markholder lacked isolable domestic good will and was merely engaging in price discrimination or other behavior questionable as a matter of antitrust law. Regulations that attempted to permit exclusion only of goods the markholders of which possessed discrete domestic good will would . . . place the Customs Service in the position of having to determine at the time of border crossing whether the domestic trademark holder had developed an independent public image in this country.”)

(internal citation and quotations omitted).

forfeiture of the infringing goods via § 43 of the Lanham Act, but at their own expense.²⁵ Thus, owning a registered mark has a major impact on who can enforce the mark owner's rights, and who bears the costs of policing and enforcement.

2. Expansion of Trademark Customs and Border Patrol Through Website Seizures



This domain name has been seized by ICE - Homeland Security Investigations pursuant to a seizure warrant issued by a United States District Court under the authority of Title 18, United States Code, Sections 981 and 2323, and Title 19, Section 1595a.

With enforcement against bulk importers of counterfeit and pirated physical goods safely in the hands of CBP, IP owners had another avenue that they wanted to address. The internet marketplace allowed for small-scale importation that could easily slip through Custom's net.²⁶ Consequently, mark owners needed a new enforcement mechanism to handle these businesses, and thus, found a way to prevent these importations—domain name seizure through civil forfeiture proceedings under provisions in the Prioritizing Resources and Organization for Intellectual Property Act of 2008 ("PRO-IP Act").²⁷ The PRO-IP Act dramatically changed the forfeiture landscape,²⁸

²⁵ 15 U.S.C. § 1125.

²⁶ See Andrew Sellars, *The In Rem Forfeiture of Copyright-Infringing Domain Names*, SSRN 1-2 (May 9, 2011), <https://ssrn.com/abstract=1835604>.

²⁷ 18 U.S.C. § 2323 (2012).

²⁸ Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, § 206(a), 122 Stat. 4256, 4262.

[t]he newly created [s]ection 2323 of Title 18 established that articles, ‘the making or trafficking of which are prohibited’ by a series of IP laws—including criminal copyright infringement, trafficking in counterfeit goods or labels falsely identifying copyrighted works as genuine, and unauthorized recordings of live musical performances or films being shown in theatres—are subject to forfeiture.²⁹

Any property used for these purposes—and this was interpreted to include website domains—was now subject to civil forfeiture.³⁰

One consequence of these new enforcement tools is the increased probability that sites hosting non-infringing works and goods would be seized.³¹ Abuse of the seizure authority would harm online businesses, such as what happened to Rojodirecta.³² Rojodirecta was a target under “Operation In our Sites,” an ICE program that began in 2008 to remove allegedly infringing websites by seizing U.S.-registered domain names believed to be associated with piracy or counterfeiting.³³ Rojodirecta was seized in 2011 during Immigration and Customs Enforcement’s annual “Super Bowl Seizure Spree,” where domain names were seized that were alleged to be infringing on NFL marks or illegally streaming games.³⁴ ICE

²⁹ Sellars, *supra* note 26, at 7-8.

³⁰ *Id.* at 11.

³¹ Nate Anderson, *US Customs Begins Pre-Super Bowl Online Mole-Whack*, ARS TECHNICA (Feb. 1, 2011, 10:13 PM), <https://arstechnica.com/tech-policy/2011/02/us-customs-begins-pre-super-bowl-mole-whacking/>; *Ex Parte Seizures*, *supra* note 3, at 300-02 (describing the damage to Rojadirecta, Dajaz1, and other websites caused by the erroneous seizure of these websites).

³² Anderson, *supra* note 31.

³³ Sellars, *supra* note 26, at 11.

³⁴ Nate Anderson, *Government Admits Defeat, Gives Back Seized Rojadirecta Domains*, ARS TECHNICA (Aug. 29, 2012, 3:23 PM), <https://arstechnica.com/tech-policy/2012/08/government-goes-0-2-admits-defeat-in-rojadirecta-domain-forfeit-case/>.

obtained a civil forfeiture order against Rojodirecta, relying on information from the Recording Industry Association of America (“RIAA”).³⁵

After 18 months of stonewalling by the RIAA, however, claiming it had evidence of the direct infringement required under the law, but never producing it—the federal government dropped its seizure claim against the service.³⁶ Rojodirecta was one of only two website domains among 80 seized that challenged its forfeiture order.³⁷ The other site was Dajaz1, a popular hip-hop music blog, was also successful in eventually having its domain name returned, again for lack of evidence.³⁸ The others did not have the resources to challenge the seizure, and there is no way to know how many of them were not infringing, but merely lacked the resources to mount a legal fight.³⁹

Challenging the forfeiture order was an expensive, time-consuming process and both Rojodirecta and Dajaz1 were harmed during the seizure by the shutdown of their websites.⁴⁰ Even though the RIAA and Motion Picture Association of America’s (“MPAA”) lost their proxy-fought court battle, they were also winners because they were able to shut down websites that legitimately competed with RIAA and MPAA members—and the costs were born by the U.S. government and the defendant website owners.⁴¹

A. *Copyright*

Along with stronger customs enforcement at ports of entry and seizures of websites, copyright owners have lobbied Congress to pass legislation that would expand seizure to domestic websites and otherwise shift enforcement of rights.⁴² Most of these attempts have failed, though there have been several successes.

³⁵ *Id.*

³⁶ *Id.*

³⁷ *Id.*

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² John R. Allison et al., *Professors’ Letter in Opposition to “Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011”*

1. Failed Attempts to Shift Civil IP Enforcement to the Department of Justice

The entertainment industry has had several failed efforts to create dubious governmental enforcement mechanisms and relieve itself of the burden of fairly competing in the marketplace.⁴³ One example is the proposed, but never enacted, Combating Online Infringement and Counterfeits Act (“COICA”), which would have allowed *ex parte* governmental seizure of a website's domain name,⁴⁴ if it “ha[d] no demonstrable, commercially significant purpose or use other than” offering or providing access to unauthorized copies of copyrighted works.⁴⁵ This seizure was broadly protested due to the limited due process rights afforded the domain name owner prior to the seizure.⁴⁶ Many of COICA’s questionable anti-competitive provisions were resurrected in the also-failed

(*PROTECT-IP Act of 2011*, S. 968), ELECTRONIC FRONTIER FOUND. (July 5, 2011), <https://www.eff.org/document/law-professors-letter-sopa>.

⁴³ See Combating Online Infringement and Counterfeits Act, S. 3804, 111th Cong. § 2 (2010); Protect IP Act, S. 968, 112th Cong. (2012) (introduced in the House of Representatives as the “Enforcement of Intellectual Property Rights Act.”); Stop Online Piracy Act, H.R. 3261, 112th Cong. (2011).

⁴⁴ S. 3804.

⁴⁵ *Id.* § 2(a)(1)(B).

⁴⁶ See Mark Lemley, David S. Levine, & David G. Post, *DON'T BREAK THE INTERNET*, 64 STAN. L. REV. ONLINE 34 (2011) (arguing that SOPA and PIPA “share an underlying approach and an enforcement philosophy that pose grave constitutional problems and that could have potentially disastrous consequences for the stability and security of the Internet’s addressing system, for the principle of interconnectivity that has helped drive the Internet’s extraordinary growth, and for free expression.”); see also Allison, *supra* note 42.

Protect IP Act (“PIPA”)⁴⁷ and the Stop Online Piracy Act (“SOPA”)⁴⁸ bills.⁴⁹

The PRO-IP Act⁵⁰ originally contained a provision, later removed, which gave the Justice Department the authority to bring civil suits against patent and copyright infringers, and turn over damages to the IP owners.⁵¹ This civil suit provision drew heavy fire not only from online rights’ groups, who blasted it as an “enormous gift” to large content owners, but also from the Justice Department itself.⁵² In a letter to the Chairman and Ranking

⁴⁷ S. 968.

⁴⁸ H.R. 3261; *see also*, Annemarie Bridy, *Notice and Takedown in the Domain Name System: ICANN’s Ambivalent Drift into Online Content Regulation*, 74 WASH. & LEE L. REV. 1343, 1363 (2017) (“In 2010, a bill called COICA, which contained provisions similar to those that later appeared in SOPA, was introduced in the Senate but failed to advance.”).

⁴⁹ *SOPA/PIPA: Internet Blacklist Legislation*, ELECTRONIC FRONTIER FOUND., <https://www EFF.ORG/issues/coica-internet-censorship-and-copyright-bill> (last visited Dec. 8, 2017).

⁵⁰ Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110–403, 122 Stat. 4256.

⁵¹ *See* Enforcement of Intellectual Property Rights Act, S. 3325, 110th Cong. (2008)

TITLE I—Authorization of civil copyright enforcement by attorney general; SEC. 101. Civil penalties for certain violations. (a) In general—Chapter 5 of title 17, United States Code, is amended by inserting after section 506 the following:

SEC. 506a. Civil penalties for violations of section 506. (a) In general—In lieu of a criminal action under section 506, the Attorney General may commence a civil action in the appropriate United States district court against any person who engages in conduct constituting an offense under section 506. Upon proof of such conduct by a preponderance of the evidence, such person shall be subject to a civil penalty under section 504 which shall be in an amount equal to the amount which would be awarded under section 3663(a)(1)(B) of title 18 and restitution to the copyright owner aggrieved by the conduct.

(emphasis added); *see also* Nate Anderson, *New IP Task Force Brings “Stronger and Stricter Enforcement”*, ARS TECHNICA (Feb. 16, 2010), <https://arstechnica.com/tech-policy/2010/02/new-ip-task-force-brings-stronger-and-stricter-enforcement/>.

⁵² Am. Assoc. of Law Libraries et al., *Concerns Regarding S. 3325, The Enforcement of Intellectual Property Rights Act of 2008*, WIRED.COM (Sept. 10, 2008), https://www.wired.com/images_blogs/threatlevel/files/copyrightactletter.pdf

Member of the Senate Committee on the Judiciary, the Department of Justice's Office of Legislative Affairs contended that the proposed law threatened to turn government attorneys into "*pro bono* lawyers for private copyright holders regardless of their resources."⁵³ The language was stripped from the final enacted version of the bill.⁵⁴

2. Successful Copyright Enforcement Shifts

Intellectual Property rights' organizations have also had some legislative success. Two examples are (1) the IP enforcement provisions in the Higher Education Opportunity Act Amendment signed in 2008;⁵⁵ and

Section 101 would be an enormous gift of federal resources to large copyright owners with no demonstration that the copyright owners are having difficulties enforcing their own rights. For example, the recording industry has threatened or filed over 30,000 lawsuits against individual consumers. Movie and television producers, software publishers, music publishers, and print publishers all have their own enforcement programs. There is absolutely no reason for the federal government to assume this private enforcement role.

⁵³ Keith B. Nelson & Lily Fu Claffee, *S. 3325 - Enforcement of Intellectual Property Rights Act*, PUBLICKNOWLEDGE.ORG (Sept. 23, 2008), <https://www.publicknowledge.org/pdf/doj-letter-20080923.pdf> ("Title 1's departure from the settled framework above could result in Department of Justice prosecutors serving as pro bono lawyers for private copyright holders regardless of their resources. In effect, taxpayer-supported Department lawyers would pursue lawsuits for copyright holders, with monetary recovery going to industry.").

⁵⁴ Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403, 122 Stat. 4256.

⁵⁵ Institutional and Financial Assistance Information for Students, 20 U.S.C.A. § 1092(a)(1)(P) (West 2017)

Information dissemination activities. Each eligible institution participating in any program under this subchapter shall carry out information dissemination activities for prospective and enrolled students. The information required by this section shall accurately describe institutional policies and sanctions related to copyright infringement, including—

- (i) an annual disclosure that explicitly informs students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the students to civil and criminal liabilities;
- (ii) a summary of the penalties for violation of Federal copyright laws; and

(2) the enhanced Internet Corporation for Assigned Names and Numbers (“ICANN”) enforcement of intellectual property rights.⁵⁶

In the Higher Education Opportunity Act Amendment of 2008, entertainment industry associations successfully lobbied for legislation that turned universities into its enforcers,⁵⁷ responsible for policing students’ use of the internet for infringing activities.⁵⁸ Through a new provision of the Higher Education Opportunity Act reauthorization of 2008, U.S. colleges and universities had general requirements imposed on them regarding unauthorized file sharing, including: (1) the dissemination of an annual disclosure to students describing copyright law and campus policies relating to infringement of copyright law;⁵⁹ and (2) a plan to “effectively” combat the unauthorized distribution of copyright materials on their networks.⁶⁰ To comply with this latter requirement, many schools enacted policies whereby students faced sanctions including losing access to the school’s internet service and academic suspension.⁶¹ Thus, to receive federal funds, schools

(iii) a description of the institution’s policies with respect to unauthorized peer-to-peer file sharing, including disciplinary actions that are taken against students who engage in unauthorized distribution of copyrighted materials using the institution’s information technology system.

⁵⁶ Dugie Standeford, *ICANN Is Moving Toward Copyright Enforcement, Academic Says*, INTELL. PROP. WATCH (Feb. 28, 2017), <https://www.ip-watch.org/2017/02/28/icann-moving-toward-copyright-enforcement-academic-says/>.

⁵⁷ Specifically, the Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) lobbied for this legislation.

⁵⁸ See William E. Kirwan, *Letter Opposing the Inclusion of the Entertainment Industry Proposal on Illegal File Sharing in the HEA*, EDUCAUSE.EDU (Nov. 7, 2007), <http://net.educause.edu/ir/library/pdf/CSD5226.pdf>.

⁵⁹ 20 U.S.C.A. § 1092(a)(1)(P).

⁶⁰ *Id.*

⁶¹ See, e.g., *Information Technology Services: Copyright FAQs*, ST. LOUIS U., <https://www.slu.edu/its/policies/dmca/copyright-law-faqs> (last visited Dec. 8, 2017)

Q: What happens if the violation notice leads to your computer?

A: When Saint Louis University receives a violation notice, ITSC notifies the network user that they must remove or disable access to the infringing material on their computer. Upon a second notification to a student, network access for their personal computer will be suspended, and the matter will be referred to the Office Student Conduct for *appropriate disciplinary action*.

had to police students' internet use and become copyright enforcers for the rights holders, shifting the burden and the costs associated with it.⁶²

The expansion of ICANN's enforcement of IP rights also shifted costs away from copyright and trademark owners.⁶³ In 1998, under contract with the U.S. Department of Commerce, ICANN was formed as a private-sector non-profit corporation to manage and oversee governance and administration of the internet's underlying address system, the Domain Name System ("DNS").⁶⁴ "ICANN was not created or intended to be an intellectual property enforcer but it was drawn from its inception into disputes over trademark rights in domain names" when, in 1999, "Congress amended the Lanham Act to include the Anti-cybersquatting Consumer Protection Act ("ACPA"), [which created] a [federal] cause of action . . . for bad-faith registration of a domain name containing a protected trademark."⁶⁵ ICANN almost simultaneously adopted the Uniform Domain

Upon a third notification ITSC will terminate network access for anyone who repeatedly infringes on the rights of copyright holders. (emphasis added); *see also Copyright Infringement and Illegal File Sharing*, VILL. U., <http://www1.villanova.edu/villanova/unit/policies/AcceptableUse/copyright.htm> (last visited Dec. 8, 2017)

2.2 Penalties for Copyright Infringement

The unauthorized copying, sharing or distribution of copyrighted material is strictly prohibited. It is a violation of federal law, the Copyright Act, and of the Code of Student Conduct. Students who infringe a copyright are subject to disciplinary action under the Code of Student Conduct, up to and including *expulsion*.

(emphasis added).

⁶² *See generally* 20 U.S.C. § 1092(a)(1)(P).

⁶³ Professor Annemarie Bridy has written about the substance of ICANN's expansion into copyright enforcement. *See* Bridy, *supra* note 48, at 1346.

⁶⁴ *Id.* at 1349.

⁶⁵ *Id.* at 1353, 1355 (citing 15 U.S.C. § 1125(d)(1)(A)(i)-(ii) (2012) ("A person shall be liable in a civil action by the owner of a mark . . . if, without regard to the goods or services of the parties, that person . . . has a bad faith intent to profit from that mark . . . and registers . . . a domain name that . . . is identical or confusingly similar to that mark.")).

Name Dispute Resolution Policy (“UDRP”) for adjudicating fights over domain names containing trademarked words and phrases.⁶⁶

ICANN has insisted that its sphere of operations and responsibilities do not include copyright enforcement; “ICANN has historically recognized that its role as an online intellectual property enforcer stops at trademarks in domain names and does not extend to copyrights in online content.”⁶⁷ Corporate copyright owners, however, lobbied to shift enforcement responsibilities, and thus the costs, to ICANN,⁶⁸ contending that “all online intermediaries, including those that operate the DNS, should be responsible for enforcing copyrights.”⁶⁹ To accommodate these rights owners, while avoiding direct involvement in copyright enforcement activities, in 2013, ICANN altered its contracts with DNS intermediaries to support “a system of extra-judicial, notice-driven sanctions . . . includ[ing] cancellation of domain names for ‘pirate sites’ about which right holders complain.”⁷⁰ Other ICANN contract modifications facilitated the MPAA’s “trusted notifier” enforcement program that utilized registry operators,⁷¹ thus, shifting this cost of enforcement of IP rights away from the rights owners.

III. ENFORCEMENT SHIFT THROUGH *EX PARTE* SEIZURES UNDER THE DTSA

The shift of enforcement costs from rights owners to others—in this case, the federal government—is again illustrated in the *ex parte* enforcement provision of the DTSA, even though its omission from state trade secret laws has not hindered adequate remedies for trade secret misappropriation.⁷² Its drafters’ claim that this provision seeks to prevent foreign corporate espionage is spurious at best.⁷³

⁶⁶ *Id.* at 1346.

⁶⁷ *Id.* at 1346-47.

⁶⁸ *Id.* at 1347.

⁶⁹ *Id.*

⁷⁰ *Id.*

⁷¹ *Id.* at 1348.

⁷² See 18 U.S.C.A. § 1836 (West 2016).

⁷³ See *Ex Parte Seizures*, *supra* note 3, at 289-90 (noting that the idea of heading to the airport with trade secrets “sounds like the premise of a Hollywood blockbuster movie, but

A. *State Trade Secret laws*

Forty-seven states have adopted, for the most part, the Uniform Trade Secrets Act,⁷⁴ and these state laws have been a satisfactory means of redress.⁷⁵ None of these state trade secret laws have an *ex parte* seizure process similar to the provision in the DTSA.⁷⁶ Businesses are able to obtain relief via the seizure of goods created based on the trade secret misappropriation, as well as the misappropriated trade secrets themselves through traditional injunctive relief available under state trade secret law, as well as under the Lanham Act's unfair competition provisions.⁷⁷ There also does not seem to have been a problem with regard to capturing large monetary awards under state trade secret laws. For example, in 2016, Epic Systems procured a \$940 million judgment against the Tata Consulting Group for misappropriating proprietary computer code.⁷⁸ In 2014, the Minnesota Supreme Court affirmed Seagate Technology's massive

... if someone is truly 'heading to the airport,' the trade secret owner needs a faster mechanism than any court can provide." (quoting *Trade Secrets Protection Act of 2014: Hearing on H.R. 5233 Before the H. Comm. on the Judiciary*, 113th Cong. 413-20, 511-14, 572-73 (2014) (statements of Rep. Goodlatte and Rep. Nadler, who asserted that the *ex parte* seizure provision "will stop thieves planning to flee the country with stolen American property").

⁷⁴ New York, Massachusetts, and North Carolina have not adopted the UTSA, though North Carolina's trade secret law closely resembles the Uniform Trade Secret Act. See *Trade Secrets Act: Enactment Status Map*, UNIFORM L. COMMISSION, <http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act> (last visited Dec. 8, 2017).

⁷⁵ See Rob Shwartz & Cam Phan, *UPDATE: Money, Money, Money: Top 10 Trade Secret Verdicts (With Our Runner-Up Overturned)*, ORRICK (Apr. 7, 2014), <http://blogs.orrick.com/trade-secrets-watch/2014/04/07/update-money-money-money-top-10-trade-secret-verdicts-with-our-runner-up-overturned/>.

⁷⁶ *Ex Parte Seizures*, *supra* note 3, at 285-86.

⁷⁷ 15 U.S.C. § 1125(a) (2012).

⁷⁸ *Epic Systems Wins \$940 Mln U.S. Jury Verdict in Tata Trade Secret Case*, REUTERS (Apr. 16, 2016), <http://www.reuters.com/article/us-tata-epic-verdict-idUSKCN0XD135>.

arbitration award of \$630 million over Western Digital Corporation.⁷⁹ In 2011, St. Jude Medical won a \$2.3 billion judgment against Nervicon,⁸⁰ which was later reduced to \$947 million.⁸¹

But lawsuits and arbitration are expensive. Just in terms of discovery, a plaintiff must request relevant materials, respond to inquiries and objections, store the materials, and review what could be thousands of records.⁸² And unless it is enjoined via a traditional, non-*ex parte* proceeding,⁸³ the defendant business may be able to continue to innovate and compete without being deprived of its resources.

B. *Ex Parte Seizures under the Defend Trade Secrets Act*

Despite adequate remedies at the state level, there was a push for a federal cause of action, and what was legislated closely resembled the Uniform Trade Secret Act with one big exception—the *ex parte* procedure provision.⁸⁴ As noted in the introduction, this provision is the major difference between the state and federal laws,⁸⁵ and the *ex parte* provision under the DTSA relieves the plaintiff trade secret owner of two burdens: (1)

⁷⁹ Seagate Tech., LLC v. W. Dig. Corp., 854 N.W.2d 750, 754 (Minn. 2014) (affirming the decision of the Minnesota Court of Appeals to reinstate the arbitration award in full).

⁸⁰ Pacesetter Inc. v. Nervicon Co. Ltd., No. BC424443, 2011 WL 2714864 (Cal. Super. Ct. Apr. 22, 2011) (verdict and settlement summary).

⁸¹ Shwartz & Phan, *supra* note 75.

⁸² *How Courts Work*, AM. BAR ASS'N, https://www.americanbar.org/groups/public_education/resources/law_related_education_network/how_courts_work/discovery.html (last visited Dec. 8, 2017).

⁸³ See, e.g., Epic Sys. Corp. v. Tata Consultancy Servs. Ltd., No. 14-cv-748-wmc, 2016 WL 1696912, at *2 (W.D. Wis. Apr. 27, 2016) (whereby after winning a jury verdict of trade secret misappropriation, the court granted the plaintiffs request for permanent injunction).

⁸⁴ 18 U.S.C.A. § 1836 (West 2016).

⁸⁵ See *Ex Parte Seizure*, *supra* note 3, at 285. “Doctrinally, the Seizure Provision would represent unprecedented innovation. No state trade secret law has a trade secret-specific *ex parte* seizure process similar to the Seizure Provision” (citing *The Trade Secrets Protection Act of 2014: Hearing on H.R. 5233 Before the H. Comm. on the Judiciary*, 113th Cong. 413-20 (2014) (statement of Rep. Lofgren).

the burden of actually having to compete in the marketplace; and (2) the burden of the costs associated with the discovery process of a lawsuit.⁸⁶

Under the DTSA, if a company believes its trade secrets have been stolen, it can seek a court order to seize the trade secrets—and take possession of the computers, flash drives, cell phones, and any other device in which the trade secrets allegedly reside,⁸⁷ without providing notice to the defendant.⁸⁸ Federal Marshals can show up at the alleged offender’s door and confiscate computers, cell phones, flash drives, and other documents.⁸⁹ A special master appointed by the court must then review all the materials to identify any misappropriated content, preserve it, and remove it from the defendant’s computers, if necessary.⁹⁰ The court may also employ technical experts to assist in these tasks.⁹¹ These tasks consume time, labor, and skill mainly at the expense of the courts, not the plaintiff.⁹²

⁸⁶ See *Ex Parte Seizure*, *supra* note 3, at 285-88.

⁸⁷ *Magnesita Refractories Co. v. Mishra*, No. 2:16-CV-524-PPS-JEM, 2017 WL 365619, at *4 (D. Ind. Jan. 25, 2017) (internal citations omitted).

⁸⁸ 18 U.S.C.A. § 1836(b)(2)(A)(ii) (“ . . . the court may, upon ex parte application . . . issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.”).

⁸⁹ *Id.* § (b)(2)(B)(iv) (“If an order is issued . . . it shall . . . provide guidance to the law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials.”); *Ex Parte Seizures*, *supra* note 3, at 290 (noting that “[T]he Seizure Provision . . . allows seizure of every . . . copy of allegedly stolen information, which could include every computer that contains one or more stolen files, along with any hard copy files containing printouts. Read literally, every storage medium of a departing employee’s new employer potentially would be subject to seizure. A thorough seizure in a departing employee situation could easily shut down the new employer until the hearing.”).

⁹⁰ § 1836(b)(2)(D)(iv) (“The court may appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized.”).

⁹¹ *Id.* § (b)(2)(E) (“At the request of law enforcement officials, the court may allow a technical expert who is unaffiliated with the applicant and who is bound by a court-approved non-disclosure agreement to participate in the seizure if the court determines that the participation of the expert will aid the efficient execution of and minimize the burden of the seizure.”).

⁹² *Id.*

The plaintiff business is supposedly prohibited from directly accessing these seized materials.⁹³ In the meantime, however, the court has appropriated the tools necessary for the defendant business to function, beyond the supposed trade secret.⁹⁴ “A seizure could massively disrupt a targeted business, temporarily shut it down,” or even kill it.⁹⁵ The plaintiff company has effectively eliminated its competition without any litigation. There is no need to compete in the marketplace through innovation or by producing higher quality products when one can use the government to shut down the competition. This legislation has created an extreme remedy whereby the trade secret plaintiffs can claim any basis to argue that things have to happen quickly, and without notice, in order to preserve their trade secret from misappropriation.⁹⁶

This expansion of rights can easily lead to anti-competitive abuse.⁹⁷ Start-up companies would be especially vulnerable when faced with the sudden seizure of their computers, documents, and other items that may contain unrelated material, including their own trade secrets, with no recourse until they are released at another hearing or at the end of adjudication.⁹⁸ And again, we see a cost shifting to taxpayers—for a mere

⁹³ *Id.* § (b)(2)(B).

⁹⁴ *Id.* § 1 (b)(2)(A)-(B).

⁹⁵ *Ex Parte Seizures*, *supra* note 3, at 293.

⁹⁶ § 1836(b)(2)(A)(ii).

⁹⁷ See generally Levine & Sandeen, *supra* note 3, at 244-45; Professors’ Letter, *supra* note 3, at 3-4 (describing how the DTSA’s *ex parte* seizure provision could be abused to harm competition by small businesses and start-ups); Brook K. Baker et al., Professors’ Letter in Opposition to the “Defend Trade Secrets Act of 2014” (S.2267) and the “Trade Secret Protection Act of 2014” (H.R. 5233), SSRN 4-5 (Aug. 26, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699735 (describing how the DTSA’s *ex parte* seizure provision could be used for anti-competitive purposes).

⁹⁸ *Ex Parte Seizures*, *supra* note 3, at 294

For well-established businesses with predictable revenues and costs, it may be possible to non-speculatively estimate the costs and foregone revenues from a wrongful seizure. In contrast, thinly resourced start-up enterprises could suffer less clear consequences from a wrongful seizure. As we are increasingly seeing small start-ups blossom into Unicorns and Decacorns, a disrupted start-up may lose billions of dollars of market cap potential.³⁶ Judges will be reluctant to award large and seemingly speculative

\$2,000 fee,⁹⁹ seizure necessary for the preservation of evidence is performed by officers of the court.¹⁰⁰ Thus, *ex parte* seizure is an unprecedented remedy that can be used to effectively shut down legitimate competition.

Take for example, Surendra Mishra, who was accused of misappropriation of trade secrets by his employer, Magnesita Refractories.¹⁰¹ Mishra's laptop was seized, and he no longer had access to anything on it because his employer thought he might be conspiring to misappropriate trade secrets.¹⁰² In this instance, the court gave Mishra's computers to his employer, who asked for access to the laptop for 48 hours so it could be imaged and returned, despite the prohibition of this action under the DTSA.¹⁰³ Magnesita had possession of Mishra's own independently created confidential material.¹⁰⁴ Magnesita was able to stifle its competitor without having to actually compete. Magnesita did this at little cost to itself.¹⁰⁵ A preservation order could have served the same

compensating damages to an unproven start-up, even if a seizure permanently diminishes or destroys its business.

⁹⁹ See, e.g., *Mission Capital Advisors, LLC v. Romaka*, No. 1:16-cv-05878-LLS, at *5 (S.D.N.Y. July 29, 2016) (Santa Clara Law Digital Commons) (ordering the plaintiff to “pay a non-refundable fee of \$2,000 to the U.S. Marshal to cover the cost of effectuating the seizure”).

¹⁰⁰ Jeanne M. Gills, *What's Reasonable?—Protecting and Enforcing Trade Secrets in the Digital Age*, FOLEY, <https://www.foley.com/files/uploads/AIPLA%20Article%20on%20DTSA%20and%20Reasonable%20Efforts%20to%20Protect%20Trade%20Secrets%2048.pdf> (last visited Dec. 8, 2017) (Section “1836(b) authorizes a federal court to issue an order in extraordinary circumstances and upon an *ex parte* application (based on a sworn declaration or verified complaint) to provide for seizure of property where necessary to preserve evidence or prevent dissemination of the trade secret.”); 18 U.S.C.A. § 1836(b)(2)(A)(ii)(VII) (“[T]he person against whom seizure would be ordered, or persons acting in concert with such person, would destroy, move, hide, or otherwise make such matter inaccessible to the court, if the applicant were to proceed on notice to such person.”).

¹⁰¹ *Magnesita Refractories Co. v. Mishra*, No. 2:16-CV-524-PPS-JEM, 2017 WL 365619, at *1 (N.D. Ind. Jan. 25, 2017).

¹⁰² *Id.*

¹⁰³ *Id.* at *2.

¹⁰⁴ *Id.* at *1.

¹⁰⁵ *Id.* at *2.

purpose, and was already available under existing laws and court procedures, without these benefits to Magnesita.

As for the shifting of costs associated with the discovery process of a lawsuit, the trade secret owner can use the government seizure and review of materials as a substitute for the discovery process that would normally be at the plaintiff's expense.¹⁰⁶ The task of identifying the relevant evidence for collection, preservation, and destruction is transformed into an all-encompassing sweep-up by U.S. Marshals of documents, computers, and anything else that "may" contain the allegedly stolen trade secret.¹⁰⁷ The court stores these materials.¹⁰⁸ The appointed special master, who can hire technical experts to assist in the task, reviews the materials for relevancy.¹⁰⁹ The special master examines, isolates trade secret information, and facilitates the return of unrelated property.¹¹⁰ This information is then passed on to the presiding judge.¹¹¹ The *ex parte* procedure provision is a boon to the bottom line of trade secret owners, with little risk other than a \$2,000 Marshal's fee and \$1,000 bond.¹¹²

IV. CONCLUSION

The DTSA's *ex parte* provision is part of the overall trend to shift costs associated with enforcement of IP rights and is a new avenue to stifle competition. By relieving plaintiffs of many of the early costs associated with trade secret misappropriation litigation, as well as the ability to remove the necessary resources that its competitor needs to operate its business, the

¹⁰⁶ 18 U.S.C.A. § 1836(b)(2)(E) (West 2016).

¹⁰⁷ *Id.* § (b)(2)(B).

¹⁰⁸ *Id.* § (b)(2)(D).

¹⁰⁹ At the court's discretion, the Plaintiff can be ordered to pay the technical expert's fee. *See, e.g.,* Mission Capital Advisors, LLC v. Romaka, No. 1:16-cv-05878-LLS, at *5 (S.D.N.Y. July 29, 2016) (Santa Clara Law Digital Commons) (ordering Mission Capital to "(b) recommend a neutral technical expert for the Court to appoint, upon the request of the U.S. Marshal, to assist in the seizure; [and] (c) pay the fee of the neutral technical expert.").

¹¹⁰ 18 U.S.C.A. § 1836(b)(2)(D)(iv).

¹¹¹ *Id.*

¹¹² *Mission Capital Advisors*, at *5 (Santa Clara Law Digital Commons).

provision has the strong potential to become an anti-competitive arrow in IP owners' quivers. Only time will tell how this plays out.