TO SEIZE THE INITIATIVE: ASSESSING CONSTITUTIONAL DUE PROCESS CHALLENGES TO THE DEFEND TRADE SECRETS ACT'S EX PARTE SEIZURE PROVISION

STEPHEN D. LEVANDOSKI*

In an effort to protect innovation and increase trade secret enforcement, Congress passed the Defend Trade Secrets Act in 2016. The law contains an ex parte seizure provision that provides for the seizure of property in order to prevent the theft or transmission of a trade secret. This Note is the first to argue that the ex parte seizure provision raises serious constitutional due process concerns. It proceeds by framing the seizure provision within its historical and legislative context, identifying infirmities in the provision through the lens of due process, and addressing larger practical and policy implications. The potentially widespread and lasting effects of the seizure provision on employee mobility, innovation, and competition underscore the importance of eliminating the provision or severely limiting its scope.

 J.D., 2018, New York University School of Law; B.S., 2011, Yale College. I would like to thank everyone who provided advice and feedback on this Note, including Professors Rochelle Dreyfuss, Harry First, Barry Friedman, Jeanne Fromer, and Samuel Issacharoff. I am also grateful for input from participants of the Furman Academic Scholars Program. Special thanks to all the editors of the *New York University Law Review*, especially Benjamin Perotin and Adam Winer, for their thoughtful help and suggestions.

INTRODUCTION

The competitive lifeblood of many firms is their trade secrets.[1] These secrets include advanced genetically engineered seeds,[2] self-driving car technology,[3] and sales lists coveted by former employees and would-be competitors.[4] At any time, any of these secrets may walk out the door, whether in the hands of a disgruntled employee[5] or a foreign operative.[6] After a flight, the person misappropriating the trade secret, for all practical purposes, may have traveled beyond the reach of American law. If a misappropriator's property—thumb drives, computers, equipment, and documents—could be seized without notice, what are the consequences for organizations protecting their innovations and are future innovators potentially subject to unwarranted legal risk?

This very threat to U.S. intellectual property motivated the legislators who approved the Defend Trade Secrets Act of 2016 (DTSA). The DTSA amends the Economic Espionage Act of 1996 (EEA) and provides for a new ex parte seizure[7] provision.[8] In addition to creating

---

[1] Trade secrets must have a business use and confer an economic advantage over competitors. *See, e.g.*, Plea Agreement at 14, United States v. Hailong, No. 4:13-cr-00147 (S.D. Iowa 2016).

[2] *See A Conspiracy to Steal Secrets of U.S. Corn*, N.Y. TIMES (Jan. 28, 2016), http://www.nytimes.com/2016/01/29/business/international/china-us-monsanto-dupont-corn.html; John Eligon & Patrick Zuo, *Designer Seed Thought to Be Latest Target by Chinese*, N.Y. TIMES (Feb. 4, 2014), http://www.nytimes.com/2014/02/05/us/chinese-implicated-in-agricultural-espionage-efforts.html.

[3] *See, e.g.*, Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2017 WL 2123560, at *8–9 (N.D. Cal. May 15, 2017).

[4] *E.g.*, United States v. Nosal, 828 F.3d 865, 881–82 (9th Cir. 2016).

[5] *See* Rochelle Cooper Dreyfuss & Orly Lobel, *Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security*, 20 LEWIS & CLARK L. REV. 419, 461–64 (2016) (describing conditions for employee defection).

[6] *See* FBI, *The Company Man: Protecting America's Secrets*, YOUTUBE (July 23, 2015), https://www.youtube.com/watch?v=Gy_6HwujAtU (depicting tactics used by foreign operatives to steal trade secrets).

[7] Commentators have defined seizures—"the taking possession of property through legal process"—as distinct from forfeitures, which are defined as "the actual divestiture[s] of legal title in property by operation of law." Steven N. Baker & Matthew Lee Fesak, *Who Cares About the Counterfeiters? How the Fight Against Counterfeiting Has Become an In Rem Process*, 83 ST. JOHN'S L. REV. 735, 745 (2009). In the technological context, seizure has meant the taking of electronic devices, including multiple computers. *See* Order Granting *Ex Parte* Civil Seizure at 3, Blue Star Land Servs. v. Coleman, No. CIV-17-931-C

a new federal private cause of action for trade secret theft, the DTSA provides that "[b]ased on an affidavit or verified complaint . . . the court may, upon ex parte application but only in extraordinary circumstances, 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."[9] Without notifying the defendant, a court may authorize federal agents to seize the would-be thief's documents, computer, or thumb drive, seemingly preventing the loss of the trade secret.

This Note proceeds in three parts to argue that the ex parte seizure provision of the DTSA raises serious constitutional due process concerns. Although several contributors to the literature offered *policy*-based critiques and analyses of the DTSA during the legislative process,[10] this Note presents a novel *legal* argument against the validity of the DTSA grounded in constitutional due process.[11] While the DTSA draft language received topical coverage prior to its passage, the scholarly literature following the law's enactment has been devoid of treatment of the seizure provision and the constitutional due process issues it raises.[12] The due process implications of seizure

(W.D. Okla. Dec. 8, 2017) (ordering the seizure of any "computers, computer hard drives, or memory devices" that may contain trade secret information).

[8] *Compare* Economic Espionage Act of 1996, 18 U.S.C. §§ 1831–1839 (2012), *with* Defend Trade Secrets Act of 2016, 18 U.S.C. § 1836 (2012 & Supp. IV 2017). For a critique of the ex parte seizure provision and of its additional procedural mechanisms, see Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 WASH. & LEE L. REV. ONLINE 284, 284, 289 n.21 (2015) (citing *Trade Secrets Protection Act of 2014: Markup Hearing on H.R. 5233 Before the H. Comm. on the Judiciary*, 113th Cong. 27 (2014) (statement of Rep. Bob Goodlatte, Chairman, H. Comm. on the Judiciary)).

[9] 18 U.S.C. § 1836(b)(2)(A)(i) (2012 & Supp. IV 2017).

[10] *See, e.g.*, Zoe Argento, *Killing the Golden Goose: The Dangers of Strengthening Domestic Trade Secret Rights in Response to Cyber-Misappropriation*, 16 YALE J.L. & TECH. 172 (2014) (analyzing policy merits of enhanced trade secrets protection and proposals for a federalized trade secrets law); Goldman, *supra* note 8 (analyzing policy concerns with a 2015 draft of the DTSA's ex parte seizure provision); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015) (raising concerns that the DTSA's provision of a private cause of action will empower trade secret trolls, harming innovation); James Pooley, *The Myth of the Trade Secret Troll: Why the Defend Trade Secrets Act Improves the Protection of Commercial Information*, 23 GEO. MASON L. REV. 1045 (2016) [hereinafter Pooley, *The Myth of the Trade Secret Troll*] (rejecting criticisms of the DTSA and suggesting that fears of trolling behavior from the new private cause of action in the DTSA are unfounded); Joseph Brees, Note, *Trade Secrets Go Federal—Parade to Follow*, 12 J. BUS. & TECH. L. 277 (2017) (reviewing literature on trade secret trolls and anticipating minimal change to litigation behavior because of the DTSA).

[11] *See infra* Part II.

[12] For discussion of the draft legislation, see, for example, Goldman, *supra* note 8, at 285–86; Tony Dutra, *Senate Judiciary Committee OKs Federal Trade Secret Bill*, BNA (Jan. 29, 2016), http://www.bna.com/senate-judiciary-committee-n57982066735/. Goldman's article explicitly excluded constitutional and due process issues from its analytical scope.

provisions in parallel intellectual property (IP) statutes are likely of serious interest to potential litigants, who should rationally seek to gain additional clarity on potential outcomes.[13] In Part I, the Note evaluates the text of the DTSA, explains its passage, and places it in the context of earlier seizure provisions used in IP rights protection. The DTSA does not exist sui generis; it fits within the context of preceding laws and frameworks, including, for example, seizure provisions for copyright and trademark counterfeiting disputes.[14] In Part II, the Note analyzes the ex parte seizure provision in the DTSA through the lens of due process, presenting a motivating hypothetical and weighing the *Mathews v. Eldridge* factors. It assesses the government interest to be modest in comparison to that of the defendants'. Most importantly, the Note demonstrates the high risk of error and defendant harm in a novel and uncertain technological landscape—put simply, physical seizures represent a crude and outmoded response to a twenty-first century challenge. It argues that the ex parte seizure provision is unlikely to survive due process scrutiny. In Part III, the Note turns to practical implications: It extrapolates the provision's potential effects on U.S. innovation and provides recommendations for minimizing its use and effects.

I
The Defend Trade Secrets Act: Trade Secrets and Ex Parte Seizures

The DTSA arose in response to the challenge of trade secret theft, which Section I.A outlines. Section I.B then introduces the legislative background of the DTSA and the specific structure of the ex parte seizure provision. Section I.C describes seizure mechanisms available through copyright law, Federal Rule of Civil Procedure 65 (Rule 65), and the Lanham Act.

Goldman, *supra* note 8, at 298 n.53. Since the DTSA has become law, there is also an important opportunity to connect risks of abuse of the DTSA seizure provision to the narrative in the literature of overzealous trade secrets enforcement harming long-term innovation in the United States. *See, e.g.*, Dreyfuss & Lobel, *supra* note 5, at 451–67.

[13] *See* Mark D. Robins, *Computers and the Discovery of Evidence—A New Dimension to Civil Procedure*, 17 J. Marshall J. Computer & Info. L. 411, 487–500 (1999) (describing constitutional due process issues in ex parte seizure orders, Rule 65, the Trademark Counterfeiting Act of 1984, the Copyright Act, and problems specific to computer-related evidence).

[14] 15 U.S.C. § 1116(d)(7) (2012) (directing courts, pursuant to the Lanham Act, to take into custody any counterfeit materials); 17 U.S.C. § 503(a) (2012) (authorizing courts to "impound[ ]" materials used in violation of copyright holders' exclusive rights under the Copyright Act of 1976); *see also* Goldman, *supra* note 8, at 295–98 (describing and comparing several other ex parte seizure provisions in the IP context); discussion *infra* Section I.C.

A. Trade Secret Theft and the Economic Espionage Act

Trade secret theft, economic espionage, and cyberespionage each have the potential to seriously undermine U.S. national security and economic growth, particularly to the extent that these activities target U.S. science and technological innovations, long held to be strategic competitive assets.[15] Trade secret policy has long required tradeoffs: Proponents of both stricter and more permissive enforcement have claimed that their favored policies promote more innovation. For trade secret hawks, the increasing ease of access to trade secrets and movement of people and information mean that trade secrets are subject to comparatively greater risk of theft. They estimate that the economic damage caused by trade secret theft reaches as high as $300 billion each year.[16] Omnipresent computer technology both enhances the potential profits of information products and increases the risk of unauthorized disclosures.[17] Trade secret doves, on the other hand, have expressed concern over the spread of trade secret enforcement. They note that many trade secrets are contained within the minds of individual employees, and IP protection regimes can strongly influence the diffusion of information and rates of innovation.[18] Overly

---

[15] *See, e.g.*, Christina Parajon Skinner, *An International Law Response to Economic Cyber Espionage*, 46 CONN. L. REV. 1165, 1167–68 (2014) ("[C]yberspace, 'where most business activity and development of new ideas . . . takes place,' allows 'malicious' cyberspies 'to quickly steal and transfer massive quantities of data while remaining anonymous and hard to detect.' . . . [T]he Intelligence Community . . . judges the use of [cyber] tools [as] a larger threat than more traditional espionage methods." (quoting OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, 2009–2011, at i (2011))).

[16] *See* OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., ANNUAL REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE—2002, at 2 (2003); *see also* Adam Cohen, *Securing Trade Secrets in the Information Age: Upgrading the Economic Espionage Act After* United States v. Aleynikov, 30 YALE J. ON REG. 189, 192–93 (2013) (describing the economic impact of trade secret theft on specific industries).

[17] *See* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 858 (2002) ("While . . . the allure of cyberspace expand[s] the potential market for, and the value of, information-based products, the same technology also makes these products vulnerable to illicit use and theft. The market value of an information product can be destroyed in the instant it takes to send digitized information . . . .").

[18] *See* Shubha Ghosh, *Open Borders, Intellectual Property & Federal Criminal Trade Secret Law*, 9 J. MARSHALL REV. INTELL. PROP. L. 24 (2009) (describing how intellectual property, through the EEA, "acts as a type of immigration policy" by "regulat[ing] the movement of people . . . through the movement of ideas"). Innovation and economic growth depend on the full and efficient allocation of human capital, which is now categorized as "cognitive property." *See* Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 835 (2015) ("Stripping individuals of the wealth of knowledge and experience they carry has detrimental effects on innovation, market competition, and economic growth.").

restrictive enforcement of trade secrets would effectively require that capital lie fallow whenever employees leave their current tenures, which are especially short in technology-driven fields.[19]

The EEA attempted to address some of the harms of trade secret theft by imposing criminal sanctions for trade secret misappropriation.[20] Section 1832 addresses trade secret theft.[21] Section 1831, which has been the basis for comparatively fewer federal prosecutions, covers economic espionage, i.e., the misappropriation of trade secrets for the benefit of foreign governments.[22] The EEA's passage represented a significant departure from prior policy, which left trade secrets to the states.[23] Individual states have largely adopted the Uniform Trade Secrets Act,[24] which generally eschews the use of criminal penalties.[25]

Drafting of the EEA focused primarily on the threat of foreign espionage to American businesses, not on domestic thefts.[26] Following the end of the Cold War, foreign industrial espionage superseded military and strategic espionage as the leading threat in policymakers'

---

[19] The information technology industry has the highest employee turnover rate out of all industries recently surveyed. *Tech Companies Have Highest Turnover Rate*, TechRepublic, http://www.techrepublic.com/blog/career-management/tech-companies-have-highest-turnover-rate/ (last visited Aug. 11, 2018).

[20] 18 U.S.C. § 1831 (2012). *See generally* Dreyfuss & Lobel, *supra* note 5, at 427–28 (providing background on the legislative history and statutory construction of the EEA).

[21] 18 U.S.C. § 1832; *see* Peter J. Toren, *A Look at 16 Years of EEA Prosecutions*, Law360 (Sept. 19, 2012, 12:18 PM), http://www.law360.com/articles/378560/a-look-at-16-years-of-eea-prosecutions ("[This] general criminal trade secrets statute . . . applies to anyone who knowingly engages in any act of misappropriation 'with intent to convert a trade secret, . . . to the economic benefit of anyone other than the owner . . . and intending or knowing that the offense will, injure any owner of that trade secret.'" (quoting 18 U.S.C. § 1832(a))).

[22] 18 U.S.C. § 1831; *see* Toren, *supra* note 21 ("The government has brought nine cases under § 1831 as compared to approximately 115 cases under § 1832. The former punishes the misappropriation of trade secrets when knowingly undertaken by anyone 'intending or knowing that the offense will benefit any foreign government, foreign instrumentality or foreign agent.'" (quoting 18 U.S.C. § 1831(a))).

[23] Dreyfuss & Lobel, *supra* note 5, at 423.

[24] Unif. Trade Secrets Act (Unif. Law Comm'n 1985); Dreyfuss & Lobel, *supra* note 5, at 430.

[25] *See* Unif. Trade Secrets Act § 7(b)(3) ("This [Act] does not affect: . . . (3) criminal remedies, whether or not based upon misappropriation of a trade secret."); *see also* Dreyfuss & Lobel, *supra* note 5, at 421, 423–24 ("[V]ery few violations of copyright and trademark law were regulated through the criminal law and no criminal penalties attached to any form of patent infringement.").

[26] *See* Cohen, *supra* note 16, at 191 ("Congress enacted the EEA in 1996 with the primary goal of protecting American business against foreign corporate espionage. The section on domestic theft of trade secrets was hastily added, and in drafting it Congress gave insufficient consideration to striking the right balance between underprotecting and overprotecting intellectual property rights.").

eyes.[27] EEA critics have raised concerns about the use of criminal law to enforce trade secret norms because criminal law can be less effective than civil remedies in this context.[28]

In a globalized economy, in which technology has facilitated ever-faster movements of people and information, the EEA provides for broad extraterritorial effects.[29] This international reach may have the effect of compelling the adoption of increasingly protectionist policies overseas, which may go beyond the uniform minimum standards of intellectual property protection established by the World Trade Organization (WTO) in 1994 Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement.[30] Trade secret policy can potentially chill competitive entry and suppress competitive innovation.[31] Notably, there is considerable variation in the handling of trade secret theft among allied developed nations, which do not uniformly criminalize trade secrets.[32] Although prosecutors have leveraged the statute to charge foreign operatives, including five Chinese People's Liberation Army (PLA) officers,[33] extraterritorial enforcement faces challenging constraints because of difficulties in identifying the perpetrators[34] and barriers to extradition.[35]

---

[27] *See* Jonathan Eric Lewis, *The Economic Espionage Act and the Threat of Chinese Espionage in the United States*, 8 CHI.-KENT J. INTELL. PROP. 189, 190–91 (2009).

[28] *See* Christopher A. Ruhl, Note, *Corporate and Economic Espionage: A Model Penal Approach for Legal Deterrence to Theft of Corporate Trade Secrets and Proprietary Business Information*, 33 VAL. U. L. REV. 763, 786–87 (1999) ("First, criminal statutes do not adequately protect the rights of the victim. Second, prosecutors do not have the expertise to prosecute high-tech crimes. Third, the victim relinquishes control of the case to the government. Fourth, the burden of proof is higher in the criminal context than in civil litigation.").

[29] *See* 18 U.S.C. § 1837 (2012); *see also* Robin J. Effron, Note, *Secrets and Spies: Extraterritorial Application of the Economic Espionage Act and the TRIPS Agreement*, 78 N.Y.U. L. REV. 1475, 1489–92 (2003) (describing the extraterritorial scope of the EEA).

[30] *See* Effron, *supra* note 29, at 1477, 1494–95 ("[E]xtraterritorial application of the EEA might . . . forc[e] countries to adopt more protectionist trade secret laws than the TRIPS minimum standards require.").

[31] *Id.* at 1479 ("[H]ighly protectionist intellectual property laws create barriers to entry and other anti-competitive conditions that . . . tend to suffocate the small and medium-sized firms whose incremental innovations are often the real engines of economic growth.") (internal quotation marks omitted).

[32] *See* Melanie Reid, *A Comparative Approach to Economic Espionage: Is Any Nation Effectively Dealing with This Global Threat?*, 70 U. MIAMI L. REV. 757, 776 (2016) (explaining differences in enforcement levels).

[33] *See* Press Release, U.S. Dep't of Justice, U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage (May 19, 2014), https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor (releasing the indictment and describing the charges filed against the Chinese officials for conducting espionage against U.S. business entities).

[34] For example, while the U.S. government has officially declared the Russian government responsible for the hacking of the Democratic National Committee, then-

B. The Defend Trade Secrets Act

1. Legislative Background, History, and Context

The DTSA, enacted into law on May 11, 2016, amended and expanded the EEA for the first time since 1996. It provides for both ex parte seizures and a new federal private civil cause of action for trade secret theft.[36] The DTSA thus continues the trend of expanding the scope of trade secret enforcement. The DTSA emerged in a political environment increasingly concerned with cyberespionage and digital infiltration of American companies by foreign operatives.[37] One recent example was the disclosure that a specialized PLA unit accessed data from 115 American firms.[38] The volume of DTSA cases has been robust: From the time of the DTSA's passage to 2018, nearly 500 cases were filed.[39] Recently, for example, five complaints have been filed under the DTSA: two in California, two in Florida, and one in Texas.[40] An ex parte seizure has been granted in at least one case

---

presidential candidate Donald Trump expressed skepticism, suggesting that the entity responsible may be "somebody sitting on their bed that weighs 400 pounds." David E. Sanger & Charlie Savage, *U.S. Says Russia Directed Hacks to Influence Elections*, N.Y. TIMES (Oct. 7, 2016), http://www.nytimes.com/2016/10/08/us/politics/us-formally-accuses-russia-of-stealing-dnc-emails.html.

[35] *See* Michael S. Schmidt & David E. Sanger, *5 in China Army Face U.S. Charges of Cyberattacks*, N.Y. TIMES (May 19, 2014), http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html (reporting on the cyberespionage and trade secret misappropriation that led to the indictment of five members of China's People's Liberation Army Unit 61398).

[36] 18 U.S.C. §§ 1836(b)(1)–(2) (2012 & Supp. IV 2017); *see also* Patrick J. Coyne, *What You Should Know About the Defend Trade Secrets Act*, LAW360 (June 27, 2016, 11:10 PM), https://www.law360.com/articles/806201/what-you-should-know-about-the-defend-trade-secrets-act (noting the key features of the DTSA and predicting an increasing level of trade secret theft enforcement).

[37] *See* Dreyfuss & Lobel, *supra* note 5, at 422 (noting an uptick in legislative and executive actions taken in recent years to protect trade secrets and criminalize their misappropriation).

[38] *See* Argento, *supra* note 10, at 173–74 (citing MANDIANT, APT1: EXPOSING ONE OF CHINA'S CYBER ESPIONAGE UNITS 21 (2013), https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf (reporting on the Chinese military cyberunit engaged in the theft of valuable intellectual property from U.S. corporations)).

[39] David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105, 151–56 (2018) (conducting an empirical review of DTSA litigation and finding that the DTSA has been ineffective thus far in addressing foreign cyberespionage threats).

[40] *See* Complaint at 3, ICE Consulting, Inc. v. Jensen, No. 3:16-cv-04349 (N.D. Cal. Aug. 2, 2016) (alleging that a former employee's refusal to return company computer hardware and files amounted to trade secret misappropriation under the DTSA and state law theories); Complaint at 1–2, Shapiro v. Hasbro, Inc., No. 2:16-cv-05750-BRO-AJW (C.D. Cal. Oct. 13, 2016) (asserting that a toy manufacturer misappropriated the trade secrets of and information presented by a doll creator after both sides engaged in negotiations); *see also* Complaint at 5–7, Custom Game Design Software, Inc. v. Katob, No. 2:16-cv-00830-JRG-RSP (E.D. Tex. Aug. 23, 2018) (alleging that the defendant's

under the DTSA.[41]

2. *DTSA Ex Parte Seizure Provision*

The DTSA's ex parte seizure provision has attracted substantial controversy.[42] The law provides that, "[b]ased on an affidavit or verified complaint . . . the court may, upon ex parte application but only in extraordinary circumstances, 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."[43] DTSA supporters have emphasized the severity and scope of the risk of trade secret theft as more information is stored and transported electronically.[44] They also perceive the protections written into the DTSA as sufficient to safeguard both the interests of defendants and third-party entities potentially affected by the ex parte seizures.[45]

There are a number of prerequisites to the granting of a seizure order.[46] A Rule 65-eligible temporary restraining order (TRO)[47] must

---

unlicensed use of the plaintiff's game software constituted trade secret misappropriation under federal and state law).

[41] *See* Seizure Order at 4–5, Mission Capital Advisors LLC v. Romaka, No. 1:16-cv-05878-LLS (S.D.N.Y. Sept. 13, 2016) (ordering the seizure of the plaintiff's customer contact lists from the defendant's computer, pursuant to the DTSA, after the defendant had stopped responding to requests and failed to appear for court); *see also* Jennifer L. Barry, Gabriel S. Gross & Nicholas H. Yu, *5 Lessons Learned as the Defend Trade Secrets Act Turns One*, LATHAM & WATKINS 1 (May 17, 2017), https://www.lw.com/thoughtLeadership/5-lessons-learned-as-defend-trade-secrets-act-turns-one (noting increased levels of misappropriation enforcement post-DTSA, despite the fact that *Mission Capital Advisors* seems to be the "only case with a published *ex parte* seizure order").

[42] *See* Teague I. Donahey, *Inside the Defend Trade Secrets Act*, LAW360 (Apr. 4, 2016, 7:32 PM), https://www.law360.com/articles/778113/inside-the-defend-trade-secrets-act (attributing controversy over the DTSA to "the fact-intensive nature and overall complexity of trade secret disputes").

[43] 18 U.S.C. § 1836(b)(2)(A)(i) (2012 & Supp. IV 2017).

[44] *See, e.g.*, Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1058; James Pooley, *Guest Post: Why We Need a Seizure Remedy in the Defend Trade Secrets Act*, PATENTLYO (Jan. 18, 2016), http://patentlyo.com/patent/2016/01/seizure-secrets-dtsa.html [hereinafter Pooley, *Why We Need a Seizure Remedy*] ("Trade secrets face far different threats in the digital age, and having federal courts able to intervene immediately in cross-border cases is critical."); James Pooley, *The Inadequacy of Trade Secret Law and Why Congress Should Pass the DTSA*, IPWATCHDOG (Dec. 22, 2015) [hereinafter Pooley, *Inadequacy of Trade Secret Law*], http://www.ipwatchdog.com/2015/12/22/inadequacy-trade-secret-law-congress-dtsa/id=64013/ (arguing that the "narrowly tailored" provisions of the DTSA decrease the likelihood of abuse stemming from parties requesting and courts issuing ex parte seizures).

[45] *See* Pooley, *Inadequacy of Trade Secret Law*, *supra* note 44.

[46] *See* 18 U.S.C. § 1836(b)(2)(A)(ii) (2012 & Supp. IV 2017) (listing eight requirements for issuing an ex parte seizure order).

[47] *See generally* FED. R. CIV. P. 65(b) (describing the requirements necessary for a court to issue a TRO without giving notice to the adverse party); discussion *infra* Section I.C.

be an inadequate remedy for protecting the alleged trade secret from dissemination.[48] There must be a finding that "an immediate and irreparable injury will occur if such seizure is not ordered."[49] The statute requires that "the harm to the applicant of denying the application outweigh[ ] the harm to the legitimate interests of the person against whom seizure would be ordered," in addition to any third-party interests that may be harmed by the seizure.[50] The applicant must be likely to succeed in showing that the information was a trade secret and that the person against whom the seizure would be ordered either misappropriated the trade secret by improper means or conspired to use improper means to misappropriate the trade secret.[51] The applicant must also be likely to succeed in showing that the person has actual possession of the trade secret and any property to be seized.[52] The application must describe the matter and location with "reasonable particularity."[53] The applicant must show that notice would lead to the movement, hiding, or destruction of the matter sought to be seized.[54] The seizure cannot have been requested publicly.[55] The order issued by the court must also require that the applicant provide an adequate security in case of a possible wrongful seizure.[56]

The statute also specifies the means by which seizures will be implemented. Service of the order is carried out by a federal law enforcement officer.[57] Interested parties may make a motion for materials seized to be encrypted to provide for the security of confi-

---

[48] 18 U.S.C. § 1836(b)(2)(A)(ii)(I) (2012 & Supp. IV 2017); *see also* John Caracappa & Jeffrey M. Theodore, *Breaking Down the New Defend Trade Secrets Act*, STEPTOE (May 11, 2016), http://www.steptoe.com/publications-11256.html (discussing the "significant limitations" on courts issuing ex parte seizure orders and noting that a court may not grant the order unless it "clearly appears" from "specific facts" that each of the § 1836 requirements are satisfied).

[49] 18 U.S.C. § 1836(b)(2)(A)(ii)(II) (2012 & Supp. IV 2017).

[50] *Id.* § 1836(b)(2)(A)(ii)(III).

[51] *Id.* § 1836(b)(2)(A)(ii)(IV).

[52] *Id.* § 1836(b)(2)(A)(ii)(V).

[53] *Id.* § 1836(b)(2)(A)(ii)(VI).

[54] *Id.* § 1836(b)(2)(A)(ii)(VII).

[55] *Id.* § 1836(b)(2)(A)(ii)(VIII).

[56] *Id.* § 1836(b)(2)(B)(vi).

[57] *Id.* § 1836(b)(2)(E). This requirement eliminates some of the constitutional difficulties present with the use of private agents for the purpose of seizing materials in earlier IP protection contexts. *See* Warner Bros. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1125–26 (2d Cir. 1989) (articulating the rationale for requiring a public officer to conduct a seizure); *see also* William P. Glenn, Jr., *Ex-Parte Seizure of Intellectual Property Goods*, 9 TEX. INTELL. PROP. L.J. 307, 322 (2001) (discussing some of the constitutional issues that arise when private security firms or attorneys are used to conduct seizures).

dential data during storage and transportation.[58] Measures specifying encryption protocols provide for some measure of data security for the information and devices seized. Following the seizure, a hearing must occur within seven days.[59] Any materials seized are to be taken into the custody of the court.[60]

The seizure provision also attempts to limit the circumstances in which it may be used. On their face, these limitations are not insignificant. The statute calls for the court to issue orders "only in extraordinary circumstances."[61] It requires that the judicial order be the narrowest possible to minimize interruption of business operations to both the person accused of misappropriating trade secrets and third parties.[62] In its text, the statute also offers remedies for those harmed by improvidently granted seizures.[63] Questions arise in practice, however, once a court must adjudicate the limits of these standards at an ex parte hearing, where defendants do not appear and may not present a counternarrative challenging the plaintiff's cogent pleas for urgency.[64]

C. Parallel Seizure Provisions

The DTSA's ex parte seizure provision did not arise ex nihilo but in the legal and policy context of prior IP enforcement statutes in both the copyright and trademark contexts.[65] Copyright law allows the impounding of infringing articles.[66] The copyright regime also provides for protective measures to prevent the improper disclosure of "confidential, private, proprietary, or privileged information con-

---

[58] 18 U.S.C. § 1836(b)(2)(H) (2012 & Supp. IV 2017). One commentator has noted that the encryption requirement is "counter-intuitive" since the material is in the possession of the court and not contained in a networked server. David Levine, *Open Letter to the Sponsors of the Revised Defend Trade Secrets Act*, STAN. L. SCH. CTR. FOR INTERNET & SOC'Y (Aug. 3, 2015), http://cyberlaw.stanford.edu/publications/open-letter-sponsors-revised-defend-trade-secrets-act.

[59] 18 U.S.C. § 1836(b)(2)(F)(i) (2012 & Supp. IV 2017); *see id.* § 1836(b)(2)(B)(v).

[60] *Id.* § 1836(b)(2)(D).

[61] *Id.* § 1836(b)(2)(A)(i). This change tightened the scope of the statute, which previously lacked such limiting language as an earlier bill in the Senate. *See* S. 1890, 114th Cong. § 2(b)(2)(A)(i) (2015); *see also* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1063, 1070 (describing the DTSA as going "well beyond Rule 65(b)" by limiting orders to only "extraordinary circumstances" and only to "prevent the propagation or dissemination of the trade secret").

[62] 18 U.S.C. § 1836(b)(2)(B)(ii).

[63] *Id.* § 1836(b)(2)(G).

[64] *See* discussion *infra* Section II.C.

[65] While outside the scope of this Note, remedies may also be available under state laws to effect ex parte seizures in the IP context. *See, e.g.*, Glenn, *supra* note 57, at 309–13 (discussing attachment, sequestration, garnishment, and seizure remedies for IP violations under Texas state law).

[66] 17 U.S.C. § 503(a)(1)(A)–(C) (2012).

tained in such [impounded] records."[67] Applicant requirements for impounding copyright materials parallel the standards of Rule 65.[68]

Rule 65 provides for issuing ex parte TROs where there is imminent concern that evidence will be removed upon notice of suit.[69] Rule 65 has its foundation in the All Writs Act,[70] which provides a broad grant of authority to the courts and complements the other seizure provisions in the IP space.[71] It requires specific facts in either an affidavit or a verified complaint.[72] The attorney moving for the seizure must certify the reasons that notice should not be required.[73] The issued order must "describe the injury and state why it is irreparable [and] state why the order was issued without notice."[74] The order is not to exceed fourteen days.[75]

The seminal case in the IP context developed out of a campaign by Louis Vuitton to limit competition from sellers of counterfeit merchandise. Here, the court found that Vuitton had sufficiently shown that notice was not required because any notice would defeat later prosecution if merchants subsequently destroyed or hid their illegal wares and little documentation or evidence subsequently remained.[76] Vuitton's argument was not merely hypothetical; the plaintiff's application for a TRO in the case benefited from an extensive factual

---

[67] *Id.* § 503(a)(2).

[68] FED. R. CIV. P. 65(f) ("[Rule 65] applies to copyright-impoundment proceedings."); *see* Robins, *supra* note 13, at 496 ("[A]n applicant [must] demonstrate, among other things, a likelihood of success in proving infringement and an imminent danger of being irreparably harmed by the likely disposal of the materials that are subject to statutory impoundment.").

[69] *See* FED. R. CIV. P. 65(b)(1); *see, e.g.*, First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 650 (6th Cir. 1993) (providing for ex parte orders "where notice to the defendant would render fruitless further prosecution of the action" (citing *In re* Vuitton et Fils S.A., 606 F.2d 1, 4–5 (2d Cir. 1979))); Earthbound Corp. v. MiTek USA, Inc., No. C16-1150 RSM, 2016 WL 4418013, at *7 (W.D. Wash. Aug. 19, 2016) (describing conditions for issuing TROs); 13 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE ¶ 65.32 (3d ed. 2018).

[70] 28 U.S.C. § 1651(a) (2012) ("The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law.").

[71] *See, e.g.*, Glenn, *supra* note 57, at 319.

[72] FED. R. CIV. P. 65(b)(1)(A).

[73] FED. R. CIV. P. 65(b)(1)(B).

[74] FED. R. CIV. P. 65(b)(2).

[75] *Id.*

[76] *In re* Vuitton et Fils S.A., 606 F.2d 1, 2, 4–5 (2d Cir. 1979) ("[A counterfeiter] would immediately transfer his inventory to another counterfeit seller . . . . [D]efendants maintain few, if any, records."); *see also* Jules D. Zalon, *Ex Parte Seizure Orders: Don't Kill the Goose That Laid This Golden Egg!*, 23 COLUM.-VLA J.L. & ARTS 181, 181–82 (1999) (describing the context of the *Vuitton* cases).

record that demonstrated the consistent failure of private enforcement actions in the absence of an ex parte seizure.[77]

Even upon granting the TRO, the court required on remand to the district court that the ex parte TRO be sufficiently tailored in scope and duration to protect the rights of the defendants.[78] The seemingly limited additional utility of the DTSA seizure provision in light of the substantial existing seizure framework is one reason for some of the DTSA's criticism in the literature.[79] Courts have overturned ex parte seizure orders where the facts alleged provided insufficient justification for the order.[80] This prior judicial practice suggests that sweeping grants of authority to seize material would be similarly impermissible.

The Lanham Act, governing trademarks, also provides for seizures in cases containing allegations concerning counterfeits.[81] The process for ex parte seizures became a preeminent tool for trademark owners.[82] According to critics of harsh trade secret enforcement, use of the seizure provision far exceeded the levels Congress anticipated.[83] In previous litigation, defendants have successfully raised due process defenses to ex parte seizures and orders under the Lanham and Copyright Acts.[84] Low barriers and perfunctory procedure to

---

[77] *See In re* Vuitton, 606 F.2d at 2.

[78] *Id.* at 3–4 (requiring that the ex parte TRO be "narrow enough and of brief enough duration to protect the interests of the defendants" and stressing "scrupulous[ ]" compliance with the requirements of Rule 65).

[79] *See, e.g.*, Levine & Sandeen, *supra* note 10, at 252–53; *see also infra* Section II.D.

[80] *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1070 (suggesting that a plaintiff's "abstract fear" that the defendant can obtain and remove information is insufficient to obtain a Rule 65 order (citing First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 652 (6th Cir. 1993) (finding that the plaintiff had made an inadequate showing for an ex parte Rule 65 order by citing the easy transportability of computer media))).

[81] 15 U.S.C. § 1116(d)(1)(A) (2012); *e.g.,* Gucci Am., Inc. v. Accents, 955 F. Supp. 279, 281 (S.D.N.Y. 1997) (upholding the seizure of counterfeit Gucci handbags under the Lanham Act). Congress amended the Lanham Act with the Trademark Counterfeiting Act of 1984, adding the seizure provision to ameliorate the law's perceived ineffectiveness. Baker & Fesak, *supra* note 7, at 738–39, 754.

[82] *See* Baker & Fesak, *supra* note 7, at 741 (describing ex parte seizures under the Lanham Act as "the best weapon [for trademark owners] in the fight against counterfeiters" (internal quotation marks omitted)).

[83] *See* S. REP. NO. 98-526, at 6 (1984) (expressing caution over the use of ex parte seizures in civil matters); Baker & Fesak, *supra* note 7, at 741 ("It is fair to say that this seizure and forfeiture procedure has been utilized well beyond the wildest expectations of the enacting Congress . . . .").

[84] *See, e.g.*, Reno Air Racing Ass'n., Inc. v. McCord, 452 F.3d 1126, 1131–32 (9th Cir. 2006) (finding an ex parte TRO improperly issued under the Lanham Act); Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 89–90 (E.D.N.Y. 1993) (denying request from copyright holders for an ex parte seizure order for impoundment of allegedly infringing films). *See generally* 11A CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL

grant seizure orders have led to very little case law.[85] While courts have not completely invalidated the ex parte seizure provisions, they have imposed higher standards.[86] This suggests that litigants are likely to raise due process limitation defenses in connection with DTSA matters. In addition, courts have raised broader concerns about the role of private actors in enforcing sanctions.[87]

II
Constitutional Challenges to the DTSA Ex Parte Seizure Provision: An Analysis

The Constitution requires that any seizure of property by a government actor or court order must be consistent with due process.[88] The mechanism for analyzing seizure orders is a multifactor balancing test, which emerged out of a group of seminal cases.[89] The core approach and legal test for assessing the due process sufficiency of statutes first emerged in *Mathews v. Eldridge*.[90] Applying a *Mathews*-based due process analysis to the issue of DTSA seizures requires balancing the competing interests of the plaintiff and the defendant sub-

---

Practice and Procedure § 2942 (3d ed. 1995) (assessing equitable principles that govern the issuance of injunctive relief).

85 Baker & Fesak, *supra* note 7, at 742 ("[I]ronically, the very ease with which these orders are granted probably explains the dearth of cases upholding the procedures . . . ." (quoting Zalon, *supra* note 76, at 191)). *But see* Gabrielle Levin, *Desperate Times, Desperate Measures? Reconceptualizing Ex Parte Seizure Orders to More Effectively Fight the War on Trademark Counterfeiting*, 14 U. Balt. Intell. Prop. L.J. 171, 196–97 (2006) (arguing that recent case law has the potential to chill worsening trademark counterfeiting and advocating for increased use of ex parte seizures to address the threat).

86 *See, e.g.*, Paramount Pictures Corp., 821 F. Supp. at 87–88 ("Faced with the constitutionally deficient procedure established by the Copyright Rules, courts, exercising their discretion under section 503(a), have held copyright holders to the standards articulated in *Mitchell* [*v. W.T. Grant Co.*, 416 U.S. 600 (1974)] and Rule 65 of the Federal Rules of Civil Procedure.").

87 *See, e.g.*, Young v. United States *ex rel.* Vuitton et Fils S.A., 481 U.S. 787, 814 (1987) (explaining the risks of interested prosecutors and requiring "assurance that those who would wield [prosecutorial] power will be guided solely by their sense of public responsibility for the attainment of justice").

88 U.S. Const. amends. V, XIV. For a general discussion, see, for example, Moore et al., *supra* note 70, ¶ 64.14; Robins, *supra* note 13, at 487–90 (analyzing the history behind the due process limitations for ex parte orders); Zalon, *supra* note 76 (reviewing the history of ex parte seizures in other IP contexts).

89 A landmark example of this analysis is *Fuentes v. Shevin*, 407 U.S. 67 (1972), which concerned the constitutionality of prejudgment replevin statutes. *See also* Robins, *supra* note 13, at 487–90 (describing the development of due process limitations on ex parte seizures); *cf.* Paul S. Owens, *Impoundment Procedures Under the Copyright Act: The Constitutional Infirmities*, 14 Hofstra L. Rev. 211, 233–34 (1985) (evaluating due process requirements in the copyright impoundment context).

90 424 U.S. 319 (1976); *see* Robins, *supra* note 13, 487–88 (citing factors).

ject to seizure, the risk of error, and the potential benefits of enhanced process.[91]

Since *Mathews*, a progression of Supreme Court cases has gradually restricted the use of ex parte prejudgment remedies and applied the test more broadly.[92] In *Connecticut v. Doehr*, the Court applied the *Mathews* framework, taking it out of its original administrative law context and applying it to the use of prejudgment attachments.[93] The *Doehr* court required:

> [F]irst, consideration of the private interest that will be affected by the prejudgment measure; second, an examination of the risk of erroneous deprivation through the procedures under attack and the probable value of additional or alternative safeguards; and third, in contrast to *Mathews*, principal attention to the interest of the party seeking the prejudgment remedy, with, nonetheless, due regard for any ancillary interest the government may have in providing the procedure or forgoing the added burden of providing greater protections.[94]

This point of departure from *Mathews* stems from the fact that, outside of the administrative context, the government no longer has a direct interest in effecting the seizure or deprivation of property. The underlying policy thrust of these cases, particularly in moving away from the administrative law arena, was to mediate the extent to which state power should be brought to bear on private parties in the service of private interests.[95] In this way, due process creates an interesting parallel with both questions of private enforcement[96] and the complementary roles of publicly and privately directed sanctions against harms.[97]

---

[91] *See Mathews*, 424 U.S. at 335.

[92] *See, e.g.*, Connecticut v. Doehr, 501 U.S. 1, 11 (1991) (applying *Mathews*'s balancing standard to prejudgment attachment); N. Ga. Finishing, Inc. v. Di-Chem, Inc., 419 U.S. 601, 606–07 (1975) (defining due process requirements for garnishment); Fuentes v. Shevin, 407 U.S. 67, 96–97 (1972) (analyzing due process concerns in the replevin context). *But see* Mitchell v. W.T. Grant Co., 416 U.S. 600, 619–20 (1974) (holding that Louisiana's issuance of an ex parte writ of sequestration did not deprive the plaintiff of procedural due process).

[93] *Mathews*, 424 U.S. at 335; *Doehr*, 501 U.S. at 11.

[94] *Doehr*, 501 U.S. at 11 (citing *Mathews*, 424 U.S. at 335).

[95] *See* Young v. United States *ex rel.* Vuitton et Fils S.A., 481 U.S. 787, 810 (1987) ("It is a fundamental premise of our society that the state wield its formidable criminal enforcement powers in a rigorously disinterested fashion . . . .").

[96] *See id.* at 811 ("If a prosecutor uses the expansive prosecutorial powers to gather information for private purposes, the prosecution function has been seriously abused . . . ."); *id.* at 814 ("Between the private life of the citizen and the public glare of criminal accusation stands the prosecutor.").

[97] Beyond due process considerations, other constitutionally-based arguments based on the Fourth Amendment may be available and are valuable to note in passing, but they are outside the scope of this Note. For a discussion regarding the Fourth Amendment

Courts later extended this methodology for due process analysis to the IP seizure and civil contexts.[98] In *Gucci America, Inc. v. Accents*,[99] the defendants argued that the plaintiffs had not satisfied the "numerous preliminary requirements" mandated by the Trademark Counterfeiting Act of 1984, while the plaintiffs questioned whether a challenge was even proper outside of the specific statutory provision[100] providing for damages in the case of a wrongful seizure.[101] The court rejected the argument, however, that the statutory remedy was the only means by which the defendants could challenge an ex parte seizure.[102] As a result, defendants subject to the DTSA's ex parte seizure provision may look beyond its statutorily defined remedies and to constitutional arguments in order to oppose the seizures.[103] The framework of the constitutional argument incorporates nonlegal, practical considerations. The analysis that emerges is fundamentally legal but is also confirmed by useful observations distilled from the policy literature.[104] For example, in *Doehr*, the Court combined an analysis of the historical and legal foundation of prejudgment attachments with a practical examination of the facts, which included the lack of any indication that the house in question would be sold and the relative indeterminacy of the tort allegations supporting the attachment.[105]

Supporters of the DTSA have highlighted aspects of the seizure provision that appear to sufficiently circumscribe its use.[106] Nevertheless, a full examination of the relevant case law and a weighing of the individual interests implicated by the ex parte seizure provision suggest multiple due process concerns. Since there are not yet any cases to guide the application of the new DTSA ex parte seizure provision, a hypothetical example may help to clarify some of the potential procedural dangers of the new law.

---

considerations raised by IP seizures and impoundments, see Owens, *supra* note 89, at 239–43.

98 *See supra* Section I.C (discussing more broadly seizures in the trademark and copyright context).

99 955 F. Supp. 279, 281 (S.D.N.Y. 1997).

100 15 U.S.C. § 1116(d)(11) (2012); Robins, *supra* note 13, at 490.

101 *Gucci Am.*, 955 F. Supp. at 281.

102 *Id.* ("The Court is not prepared to hold that this statutory remedy is the sole remedy available to a defendant whose property is the subject of an improperly-issued seizure order." (citing Soldal v. Cook Cty., 506 U.S. 56, 60–62 (1992) for the proposition that Fourth Amendment scrutiny can provide a non-statutory remedy for aggrieved defendants)).

103 *See id.*; Goldman, *supra* note 8, at 298–99 n.53.

104 *See* sources cited *supra* note 10; discussion *infra* Part III.

105 Connecticut v. Doehr, 501 U.S. 1, 16–18 (1991).

106 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1063 ("The provisions covering ex parte seizure of property are extensive and tightly drawn.").

In this hypothetical, a valuable employee may leave an established firm to join an emerging start-up competitor. The former employer may seek an ex parte seizure application against its new competitor, specifying that any devices containing information related to its trade secrets, both located on its own business premises and stored at third-party vendor locations, should be seized. The specified information may in fact be stored at a third-party data center, perhaps by a cloud-based storage provider such as Dropbox or a cloud computing and software provider such as Salesforce.com or HubSpot. The data may be distributed across dozens of servers, each of which contains many terabytes of information belonging to fourth-party customers completely unrelated to the target start-up, only happening to use the same vendor.

The adjudicating court, reviewing the application ex parte, cannot know these facts. The federal officers, sent to either the competitor's data storage facility or a third-party facility to execute the seizure of storage media, cannot meaningfully isolate the targeted information from the haystacks of innocuous data.[107] All the agents see are servers and devices, any of which may contain the information in question. This scenario is further complicated by the possibility that the employee *did* in fact remove information from her former employer, but only information that should not have received trade secret protection, either because it was widely known or not sufficiently protected in the firm.[108] Disruption and revenue loss may ensue long after a hearing finally restores hardware such as computer servers, storage media, and data to the third-party firm.

A. Interest of the Government

The first factor considered in the *Mathews* constitutional due process analysis is the interest of the plaintiff, which here stands in for the interest of the government in effecting the seizure.[109] Importantly, the weight of the interest ascribed to the implementation of the ex parte seizure provision may be significant but is complicated and potentially uncertain. In formal terms, the plaintiff does not have a preexisting property interest in the physical data storage media, provided that the specific and tangible thumb drives, personal computers, servers, or

---

[107] *See* Andrew McAfee, *What Every CEO Needs to Know About the Cloud*, HARV. BUS. REV. (Nov. 2011), https://hbr.org/2011/11/what-every-ceo-needs-to-know-about-the-cloud (discussing the significance of cloud computing and the difficulty in pinpointing data location).

[108] *See* Goldman, *supra* note 8, at 304.

[109] *See Doehr*, 501 U.S. at 11 (refocusing interest inquiry from the government to the party seeking the seizure).

other media were not directly stolen. Admittedly, the plaintiff may have much at stake in ensuring the integrity of its trade secrets.[110] Courts have also recognized this interest in other litigation contexts, such as the codification of a trade secret privilege in evidentiary rules.[111] Importantly, however, because of the fact-driven nature of trade secret inquiries establishing trade secrets and defenses such as reverse engineering and inadequate safeguards, presumptions of the plaintiff's interest in the integrity of the alleged trade secret should not be accepted uncritically.[112] As a result, the plaintiff's interest, though potentially compelling, does not on balance outweigh the other relevant factors.

B. Interest of the Defendant

The second prong of the *Mathews* constitutional due process analysis is the interest of the defendant whose property is subject to the seizure in question.[113] On its face, the DTSA, similar to the Lanham Act, does require the weighing of defendants' interests, so the DTSA seems unlikely to create a due process problem for want of a requirement to consider that interest alone. Rather, important differences in technology fundamentally alter the character of these effects. As a result, the stakes become significantly higher, so any procedural failure to properly quantify that interest will magnify the volume and scope of bad outcomes.

Timing is a critical factor in the due process calculus. The length of time between the seizure and the subsequent hearing may be relatively brief, at seven days, but every day matters for technology companies.[114] After all, the justification for the DTSA depends, supporters concede,[115] on the particular harms that technology and its high capacity for data storage and transmission enables. Just as technology may heighten the risk of harm caused by trade secret theft, technology has also served to amplify the pace of business and to mag-

---

110 *See* discussion *supra* Section I.A.

111 *See, e.g.*, Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1378–81, 1388–95 (2018) (describing the evolution of the trade secret privilege codification by courts and citing cases).

112 *See infra* Section II.C and text accompanying note 130.

113 Mathews v. Eldridge, 424 U.S. 319, 334 (1976).

114 *See* 18 U.S.C. § 1836(b)(2)(B)(v) (2012 & Supp. IV 2017) (providing that the ex parte order must "set a date for a hearing . . . at the earliest possible time, and not later than 7 days after the order was issued").

115 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1066–67 ("With the arrival of ubiquitous digital devices with massive storage and robust wireless communications, the risk profile of holding trade secrets has been profoundly and irretrievably altered. Never have information assets been so vulnerable to loss. And never have they been so valuable.").

nify the impact of even a relatively brief disruption. Businesses dependent on always-on connectivity, such as communications, cloud computing, data storage, and "software as a service" firms, are responsible not only for their own data and technology but for clients' as well.[116] Financial firms also face the disruption of high-speed trading or of unbalanced hedges, whose costs could be immense.[117] The recent distributed denial-of-service attack launched against Dyn, a provider of network and internet infrastructure services, on October 21, 2016, also illustrates the extraordinary costs and ripple effects of service outages for technology firms.[118] Certain internet companies can lose tens of thousands of dollars *per minute* if their web and computer infrastructure is compromised.[119]

In addition, even firms without high connectivity are vulnerable to disruption; many technology start-ups have very precarious operations and funding.[120] The early development of many start-ups further complicates damage calculations. If a temporary seizure disables a promising enterprise, was a fledgling unicorn, i.e., a company with a billion dollar valuation,[121] lost?[122] The risks are exacerbated to the

---

116 *See Trade Secrets: Promoting and Protecting American Innovation, Competiveness and Market Access in Foreign Markets: Hearing Before the H. Subcomm. on Courts, Intellectual Prop., & the Internet of the H. Comm. on the Judiciary*, 113th Cong. 21–22 (2014) [hereinafter *Hearing*] (statement of David M. Simon, Senior Vice President for Intellectual Property, Salesforce.com, Inc.).

117 This example is not entirely hypothetical. In *United States v. Aleynikov*, although the competitor firm to which the defendant moved had not yet developed a functional high-frequency trading system, actively running software may have generated "many millions of dollars in annual profits." 676 F.3d 71, 80–82 (2d Cir. 2012) (reversing conviction for stealing high-frequency trading code and holding that source code is not a trade secret because it is not a "product produced for [or] placed in interstate or foreign commerce"); *see also* People v. Aleynikov, 15 N.Y.S.3d 587, 590 (Sup. Ct. 2015) (dismissing state law misappropriation claims for failure to satisfy theft element under the New York penal code).

118 *See* Drew FitzGerald, *Dyn Says Cyberattack Has Ended, Investigation Continues*, WALL ST. J. (Oct. 24, 2016), http://www.wsj.com/articles/dyn-says-cyberattack-has-ended-investigation-continues-1477178773 ("[U]sers from California to Malaysia had trouble accessing 1200 web domains . . . . Among the most popular sites affected were Twitter, Netflix and PayPal.").

119 *See* Adriene LaFrance, *How Much Will Today's Internet Outage Cost?*, ATLANTIC (Oct. 21, 2016), http://www.theatlantic.com/technology/archive/2016/10/a-lot/505025 ("One 2012 study . . . found the average company's cost for every *minute* of downtime during [an ongoing distributed denial-of-service] attack was $22,000.").

120 *See generally* DAN LYONS, DISRUPTED: MY MISADVENTURE IN THE START-UP BUBBLE 11–14 (2016) (providing a personal narrative describing the precarious state of many start-ups, which can quickly run out of money or lose the confidence of their investors).

121 *See* Ben Zimmer, *How 'Unicorns' Became Silicon Valley Companies*, WALL ST. J. (Mar. 20, 2015), http://www.wsj.com/articles/how-unicorns-became-silicon-valley-companies-1426861606 ("Data scientists aren't as rare as unicorns, and neither are those billion-dollar startups. . . . [T]he 'unicorn' label is imperfect. 'Unicorns apparently don't

extent that new companies often depend on high-stakes fundraising rounds, which adverse procedures could negatively disrupt.[123] The danger to young firms is particularly acute, because, according to one venture analytics group, lack of cash was the second-most common reason that start-ups fail, leading to twenty-nine percent of all bad start-up outcomes.[124]

The claimed narrowness of the DTSA's enforcement ambit is no cause for relief. Commentators arguing for the sufficiency of the DTSA ex parte seizure provision have argued that limitations such as to property "necessary to prevent the propagation or dissemination of the trade secret" adequately address due process concerns.[125] Because of the nature of file sharing and copying in modern technology, however, line drawing is no longer as easy as it was in a paper-based era, or during a time in which copying required specific, perhaps unique instrumentalities, such as custom plates or pattern templates, to achieve. Today, any network-connected device is capable of storing, copying, and transmitting information, and the distribution often occurs automatically. The increasing capabilities of modern internet-enabled devices have also created new vulnerabilities and liabilities.[126] In addition, the limitation of seizures to "extraordinary" circumstances should not be a cause for comfort, even if it has the potential to limit the risk of misapplication of the statute.[127] Absent proper

exist, and these companies do . . . but we like the term because to us, it means something extremely rare, and magical.'" (quoting Aileen Lee, *Welcome to the Unicorn Club: Learning from Billion-Dollar Startups*, TECHCRUNCH (Nov. 2, 2013), https://techcrunch.com/2013/11/02/welcome-to-the-unicorn-club/?mod=article_inline)).

122 *See* Goldman, *supra* note 8, at 293–94 (noting the difficulties in calculating damages).

123 *See* Timothy B. Lee, *No One Knows What Will Happen if the Silicon Valley Boom Ends*, VOX (Oct. 27, 2015, 8:30 AM), http://www.vox.com/2015/10/27/9617996/silicon-valley-boom-fragile ("[A] 'down round' [of fundraising] . . . can be devastating. Not only is a declining value bad for previous investors, but it can shake the confidence of employees . . . and customers, who might wonder if the company will still be around in a couple of years.").

124 *See* Jurica Dujmovic, *20 Biggest Reasons Why Startup Companies Fail*, MARKETWATCH (June 16, 2015), http://www.marketwatch.com/story/20-biggest-reasons-why-startup-companies-fail-2015-06-16.

125 18 U.S.C. § 1836(b)(2)(A)(i) (2012 & Supp. IV 2017); *see* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1056 (discussing admissions by critics of the DTSA legislation that legislative draft amendments mitigated some earlier concerns).

126 *See* David E. Sanger & Nicole Perlroth, *A New Era of Internet Attacks Powered by Everyday Devices*, N.Y. TIMES (Oct. 23, 2016), http://www.nytimes.com/2016/10/23/us/politics/a-new-era-of-internet-attacks-powered-by-everyday-devices.html ("[T]he problem is quickly expanding: Cisco estimates that the number of such [internet-enabled] devices could reach 50 billion by 2020, from 15 billion today.").

127 *See* Goldman, *supra* note 8, at 296 (arguing that because the seizure provision "does not expressly tell judges that seizure orders should be extraordinary[ ] . . . judges may treat the Seizure Provision as relatively routine."). Trademark law may represent a cautionary example. *See* discussion *supra* notes 76–80 and accompanying text.

application and vigilance of the courts, an ex parte seizure application may be issued as a matter of course upon the perfunctory box checking of the DTSA's statutory requirements.[128] Without a counternarrative, the dubious conclusions may appear obvious, and "extraordinary" remedies may become widespread and issued as a matter of course.

C. Risk of Error

The third prong of the *Mathews* constitutional due process analysis concerns the risk of error that the seizure procedures create in the absence of additional safeguards.[129] While all ex parte hearings have a risk of error, seizures under the DTSA are particularly susceptible given the lack of physical evidence in trade secret theft, the technological difficulties surrounding isolating the offending trade secrets, and the challenge of quantifying the impact of such seizures, particularly on third parties. Despite references to the demanding level of specific factual proof required in order to secure an ex parte seizure order, supporters' arguments do not dispel concerns about the risk of error.[130] For example, while one observer suggests that the "plaintiff's abstract fear" of harm resulting from the defendant's misappropriation of trade secrets is insufficient, the cited examples of "clear evidence of relevant behavior" are hardly more concrete and reassuring.[131] At a certain level, an activity such as file downloading will exceed a threshold of suspicious activity, but at lower levels, they constitute normal behavior. Even within a larger context, it is not clear that a court is well equipped to draw demarcating boundaries in the absence of a contrasting narrative.[132]

---

[128] *See* Caracappa & Theodore, *supra* note 48 ("[I]t is possible to characterize many cases as 'extraordinary.' . . . [C]ourts may find that extraordinary circumstances exist whenever a plaintiff has made a showing that satisfies the DTSA's list of specific prerequisites for a seizure order. If so, ex parte seizure orders may become . . . distressingly common . . . ."); *cf*. Baker & Fesak, *supra* note 7, at 741, 788.

[129] Mathews v. Eldridge, 424 U.S. 319, 335 (1976).

[130] This assumes that seizure orders will be limited by the safeguards put in place. However, this has not been the practice with seizure orders issued under the Lanham Act. *See* Baker & Fesak, *supra* note 7, at 789 ("The seizure order . . . has long since left many of these limitations behind. Applications for lengthy seizures meet only the very broadest definitions of particularity, if at all. . . . Incredibly, courts seem all too willing to ignore the express limitations of Congress . . . .").

[131] *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1070 ("[E]xcessive downloading followed by reformatting of the company laptop, revenge-tainted threats, missing files, attempted, improper access to data, and the like, . . . when considered in context convinces the court that the secrets are in immediate peril.").

[132] *Cf.* MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT 145–50 (2014) (describing an alternative narrative for seemingly suspicious behavior).

The absence of physical evidence in contemporary trade secret theft, highlighted by supporters as a cause for the new measures, equally calls into question the adequacy of the safeguards. Older methods of theft were more time consuming and left less ephemeral physical traces.[133] This justification fails, however, to the extent that the statutory requirements demanding sufficient demonstration of possession of the trade secret must either be ineffectual or must preclude enforcement in cases where digital theft truly occurs without a clear trace or by means of an obscured path. The absence of clear boundaries has also increased the risk that a physical seizure of computer equipment could lead to unrestrained access to and searching of data.[134] The incorporeal nature of trade secrets further complicates enforcement of requirements in the ex parte seizure provision that require particularity in specifying the location and nature of the material to be seized. Unlike physical objects, trade secrets, as information and ideas, do not necessarily manifest themselves in physical locations.

Moreover, the ability to instantaneously copy and transmit data, sometimes unknowingly, complicates claims that seizure provisions can lower the risk of trade secret theft by returning the information to the company from which they were allegedly misappropriated. In the days of physical theft of paper documents, this approach might have made sense: An employee who stole ten boxes of secret paper documents but who later returned them or lost them in a seizure may not be said to possess the trade secrets contained within them in any meaningful sense. On the other hand, seizing 100 computers, servers, or devices would be wholly ineffectual, no matter how disruptive, if even a single copy remained on an unaccounted-for phone or thumb drive. In the context of the hypothetical servers, what constitutes adequate relief? Put within the legal framework of the third *Mathews* factor, technological progress in copying and transmitting data has ironically diminished the precision with which data can be seized and controlled, compounding the risk of error in ex parte seizures. While this brave new world of information diffusion is unlikely to put companies at ease, no rational firm should take solace in the promise that

---

133 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1066 ("In the 1970s and 80s, taking trade secrets from a business typically was slow and tedious work, involving standing at a photocopier at night and making hundreds or thousands of copies. . . . [U]sually there was physical evidence (or a security camera) pointing to the perpetrator.").

134 *Cf.* Clark D. Cunningham, *No Sexting, No Emails: In Getting "New" Clinton Emails, Did the FBI Violate the Constitution?*, SLATE (Oct. 30, 2016, 6:05 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2016/10/in_getting_new_clinton_emails_did_the_fbi_violate_the_constitution.html (discussing the discovery of emails allegedly linked to Hillary Clinton on a computer in the course of a separate investigation).

ex parte seizures will contain or restore the protected state of information once it has been spilled into the world.

While supporters of the ex parte seizure provisions look to the experience of the federal judiciary with "complex cross-border litigation" to correctly adjudicate the ex parte hearings,[135] our hypothetical judge, accustomed to the adversary system, must complete a fact-intensive inquiry with presentations from only a single party.[136] The Supreme Court has long recognized that the procedural barriers to ex parte remedies are premised on a judicial system that generally assumes notice to each party to the dispute.[137] Trade secrets present a difficult challenge for the courts, which must adjudicate both whether reasonable measures are in place to protect the trade secrets and whether the information had independent economic value because of its secrecy.[138] In addition, because a trade secret can be lawfully reverse engineered, a company may be in legitimate possession of another company's secret, but without a preseizure hearing, the lawfulness of that possession may be difficult to ascertain.[139]

The difficulty courts face in adjudicating fact-intensive inquiries also diminishes the protective value of the statute's security-posting requirement.[140] Without any representation by the defendant, it may be extremely difficult for the court to value potential wrongful seizure claims. Valuation is particularly difficult for either difficult-to-understand technology-extensive interdependencies or start-up firms with uncertain prospects but nonzero probabilities of multibillion dollar valuations.[141] As a result, the very ex parte process of setting the value

---

135 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1069 ("[A]s a result of their extensive experience with complex cross-border litigation involving intellectual property, they will be able to resolve ex parte matters fairly and jurisdictional issues quickly and efficiently.").

136 *See* Goldman, *supra* note 8, at 299 (describing the limitations of ex parte proceedings in an adjudicatory regime "built for adversary proceedings").

137 *See, e.g.*, Granny Goose Foods, Inc. v. Brotherhood of Teamsters, Local No. 70, 415 U.S. 423, 438–39 (1974) ("The stringent restrictions imposed by . . . Rule 65 . . . on the availability of ex parte temporary restraining orders reflect the fact that our entire jurisprudence runs counter to the notion of court action taken before reasonable notice and an opportunity to be heard has been granted both sides of a dispute.").

138 *See* Goldman, *supra* note 8, at 303–04 (citing 18 U.S.C. § 1839(3) (2012) for the definition of "trade secret").

139 *See id.* at 299–300, 304–05 (noting the fact-intensive inquiry of reverse engineering while also highlighting the role of the adversary process in exposing weaknesses in arguments on both sides).

140 *See* 18 U.S.C. § 1836(b)(2)(B)(vi) (specifying that orders "require the person obtaining the order to provide the security determined adequate by the court for the payment of the damages that any person may be entitled to recover as a result of a wrongful or excessive seizure or wrongful or excessive attempted seizure").

141 *See* Aswath Damodaran, Valuing Young, Start-up and Growth Companies: Estimation Issues and Valuation Challenges 5–11 (May 2009) (unpublished manuscript),

of the security to be posted diminishes the efficacy of the security in incentivizing only economically efficient use of the seizure provision.

Companies also have practical alternatives outside of ex parte seizures for ensuring that trade secrets remain protected, including better protocols for internal security and for managing employees' access to sensitive information.[142] In fact, integral to the requirements for information to receive trade secret protection is firms' reasonable diligence in securing the information themselves.[143] Beyond the immediate due process question, there is a considerable concern that the availability of downstream remedies may affect companies' incentives to adopt efficient levels of self-help in securing information and incentivize firms to rely on the (over)deterrence created by the statute.

Perhaps the point at which the law creates the greatest potential risk of error is with respect to third-party firms. Again, the DTSA on its face recognizes the potential impact of seizures on third parties, so it cannot be the mere failure to acknowledge the risk that creates a due process issue. Rather, the fundamental premises of ex parte adjudication create a framework in which the ultimate decider is ill equipped to quantify and comparatively assess these risks. The legislative history of the DTSA itself reflected concerns about the management and seizure of third-party data.[144] One witness testifying before the House Judiciary Committee called attention to the fact that data stored on technological systems often belongs to customers, and that that data is often not physically isolated from other data.[145] While supporters may counter that the provision specifically provides for the court to weigh the extent of deleterious impact to third-party customers, absent testimony from the defendant, it is impossible to deter-

---

http://people.stern.nyu.edu/adamodar/pdfiles/papers/younggrowth.pdf (assessing the characteristics of young companies and describing several valuation issues that arise).

142 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1070 ("[B]usiness[es] should use [their] rights under existing law to 'search company premises, requiring the return of company property, or engage[ ] in timely exit interviews.' ").

143 *See* Dreyfuss & Lobel, *supra* note 5, at 430 (discussing the "reasonable measures" requirement).

144 *See* John Cannan, *A (Mostly) Legislative History of the Defend Trade Secrets Act of 2016*, 109 L. LIBR. J. 363, 374–75 (2017) (describing the legislative history and industry testimony which prompted the inclusion of "narrowly tailored" ex parte seizure provisions) [hereinafter Cannan, *A (Mostly) Legislative History*]; *see also* John Cannan, *A Legislative History of the Defend Trade Secrets Act of 2016*, IPWATCHDOG (May 20, 2016), http://www.ipwatchdog.com/2016/05/20/a-legislative-history-of-the-defend-trade-secrets-act-of-2016/id=69082/ (noting the practical and technical concerns raised to Congress about the "seizure of third-party data storage containing misappropriated trade secrets").

145 *See Hearing*, *supra* note 116, at 21–22 (testimony of David M. Simon, Senior Vice President for Intellectual Property, Salesforce.com, Inc.) (describing the risks to third parties).

mine whether the collateral effects will be felt by five firms or one thousand. While the severely limited ability of the courts to assess collateral harms in an ex parte hearing may not represent an intrinsic and irreparable flaw in the statute's constitutionality, it strongly suggests the practical and legal challenges making any type of ex parte procedure both operable and compliant with due process requirements. No matter the wording of the statute, or its exact requirements, there is likely to be a danger that the courts lack the technological expertise to weigh the potential risks and government marshals lack the skills to effectuate the seizure without causing further collateral harms.[146]

D. Benefits of Additional Process

The fourth and last factor in the *Mathews* constitutional due process analysis concerns the potential benefits of additional process and procedural protections.[147] Here too, the ex parte seizure provision of the DTSA cannot withstand constitutional due process scrutiny because the law provides insufficient protection to the interests of the accused violator and parties likely to suffer collateral harms following seizures. One challenge in weighing the potential benefits of additional procedures is the seeming comprehensiveness of the existing measures and their seeming correspondence with the Lanham Act procedures.[148] This is not to suggest, however, that additional steps could not be taken to ensure adequate procedures capable of protecting the interest of defendants and third parties. For example, an even shorter time period between the seizure and hearing would decrease, though not fully ameliorate, the disruption caused by any seizure of technological infrastructure. In addition, the more fact-based inquiry associated with trade secrets vis-à-vis counterfeits may

---

[146] The use of special masters may assist courts in managing the seizures. *See* 18 U.S.C. § 1836(b)(2)(D)(iv) (2012 & Supp. IV 2017) ("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."); FED. R. CIV. P. 53(a)(1)(C) (authorizing the appointment of a master to "address pretrial and posttrial matters that cannot be effectively and timely addressed by an available district judge or magistrate judge of the district"); *see also* Kenneth Kuwayti, Bryan Wilson & Christian Andreu-von Euw, *The Defend Trade Secrets Act: Some Practical Considerations*, MORRISON & FOERSTER 3 (May 11, 2016), https://media2.mofo.com/documents/160511defendtradesecretsact.pdf (citing the appointment of special masters and the use of encryption as two ways for overburdened courts to administer DTSA procedures). Third-party harm concerns may also be somewhat mitigated by a possession requirement. *See* Cannan, *A (Mostly) Legislative History*, *supra* note 144, at 376 (assessing the DTSA provision requiring applicants to show that the party subject to the order had misappropriated the trade secret and was in possession of it).

[147] Mathews v. Eldridge, 424 U.S. 319, 343 (1976).

[148] *See* Pooley, *Why We Need a Seizure Remedy*, *supra* note 44 (comparing the DTSA seizure procedures to those of the Lanham Act).

altogether preclude ex parte procedures as viable forums for courts to adjudicate facts of this kind. Undoubtedly, however, the most significant procedural improvement would be to eliminate the ex parte provision altogether and rely solely on adversarial proceedings to adjudicate trade secret questions. In that context, courts would not be required to make fact-intensive inquiries in the absence of a challenging counternarrative.

The case for additional procedural protections for defendants is particularly compelling in light of the substantial procedural alternatives available to plaintiffs and the relatively marginal benefits of the additional DTSA remedy.[149] The prior framework providing for ex parte relief was hardly insubstantial; both preliminary injunctions and TROs were already available to parties.[150] Importantly, for the DTSA to work, plaintiffs must not have been able to avail themselves of the prior statutory framework, but on the other hand, defendants must not be so stealthy or agile as to escape detection or apprehension even with the enhanced seizure measures under the DTSA. The remaining cases falling in the middle, properly measured, then may be quite few in number.

In addition, many cases of trade secret theft are ultimately criminal in nature,[151] so the fastest option for stopping individuals allegedly misappropriating trade secrets may continue to be directly notifying law enforcement officials.[152] This remedy does not require engaging the courts in their capacity to grant ex parte seizure orders at all.[153] As a result, private parties may have relatively little at stake in availing themselves of the new DTSA procedure because of the limited difference in the utility of the civil ex parte seizure provision vis-à-vis making a criminal complaint to a U.S. Attorney. Put differently, a new tool in the box that replicates another, without much practical

149 *See* Goldman, *supra* note 8, at 287 (observing the restricted scope of the DTSA seizure provision's benefit).

150 *See* Levine & Sandeen, *supra* note 10, at 252–53 ("Under applicable law governing the grant of temporary restraining orders and preliminary injunctions, courts already have broad discretion to order the seizure of information . . . ." (citing Daniels Health Scis., L.L.C. v. Vascular Health Scis., L.L.C., 710 F.3d 579, 586 (5th Cir. 2013) (upholding a preliminary injunction granted in a case for trade secret misappropriation))); *supra* Section I.C.

151 Levine & Sandeen, *supra* note 10, at 240, 257.

152 *Id.* at 250 ("[C]ontacting or tipping off law enforcement requires no court process and, if an actual threat exists, is undoubtedly a faster route to intercepting a rogue employee at an airport than attempting to get a court involved.").

153 *See id.*; *see also* Caracappa & Theodore, *supra* note 48 ("[F]ederal law enforcement agencies already have the authority to seize stolen trade secret material after proper law enforcement investigation. . . . The key difference with the DTSA's seizure right is that prior remedies operate based on the initiative and decision-making of disinterested and independent law enforcement.").

advantage, appears to be of limited value, at least for its advertised purpose. In the most salient cases of alleged foreign espionage, prosecutors may use search warrants to gain access to evidence; there has been no shortage of interest in prosecuting and raising awareness of these offenses.[154] In addition, the law and its seizure provision ultimately do not directly assist potential victim companies in recognizing that trade secrets theft is occurring in the first place.[155] Many firms have also established procedures for the preservation of evidence, so the additional value of court custody may not be nearly as high as expected, particularly in the domestic competitor-employer context, where there is no reasonable expectation that the competitor company itself will abscond to an inaccessible jurisdiction.[156]

III
DTSA: Policy and Reforms

Section III.A considers the strongest policy justifications for implementing a more strict trade secret enforcement regime. Section III.B describes the policy harm resulting from excessive enforcement of trade secret protections. Section III.C explains mechanisms for courts to prevent the over-application of the DTSA, and Section III.D describes one approach for legislative reform.

A. The Policy Case for the Ex Parte Seizure Provision

Comprehensive analysis of the policy tradeoffs at play in the DTSA requires some attention to the supporters of the new statute. Their arguments generally focus on the extent of the harm to trade secret holders, the practical protection the procedures afford, and the extent to which the new law represents a continuation of policies used elsewhere in the IP space. Much of the literature and commentary on the DTSA's new ex parte seizure provision is highly supportive of the enforcement power that the statute creates.[157] The DTSA benefitted

---

154 *See* Levine & Sandeen, *supra* note 10, at 254 (discussing the distinction between potential DTSA-use cases comparing foreign operatives with more traditional domestic competitor suits, where evidence of trade secret misappropriation may be less obvious).

155 *See id.* at 250 (discussing the inability of the DTSA to improve detection of trade secret misappropriation).

156 *Id.* at 253 ("[I]t is standard practice for larger and more sophisticated companies to place a 'legal hold' on documentary and digital information once the threat of litigation is known.").

157 *E.g.*, Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10; Pooley, *Inadequacy of Trade Secret Law*, *supra* note 44; see *supra* Sections I.A and I.B for an additional discussion of forces motivating passage of the EEA and DTSA.

from wide industry backing and robust bipartisan support.[158] This support undoubtedly reflects the strong economic interests concentrated in relatively few rights holders in comparison with the much more diffused group of workers and the still-unformed competitors and start-ups potentially affected by overenforcement.[159]

While this Note has suggested that this provision is ultimately ineffectual and unwarranted, the law's supporters argue that the imminent risk of harm from release of trade secrets enabled by modern technology underscores the need for this fast-acting remedy.[160] Indeed, a major impetus for the new law, aside from ongoing concerns about cyberespionage and cybersecurity, was ensuring that firms could respond and quickly seek relief from the courts following the detection of trade secret theft.[161] In addition, observers have cited the increased value of intangible information as a percentage of firm value as evidence that there is more at stake than ever before for protecting trade secrets.[162] Parallel to the rise in trade secret value, companies are increasingly perceiving trade secrets as more central than patents in their IP protection strategy.[163]

Supporters have suggested that the extent of the requirements that must be satisfied by a plaintiff before an application for an ex parte seizure is granted[164] is likely to create a high degree of confidence that use of the provision will be limited and fully justified by the circumstances.[165] Effectively, the procedures will be limited in use to extreme cases, according to supporters, and thus any expectation of

---

158 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1046 (describing legislative history and bipartisan support for the DTSA).

159 *See* David Post, *A Misguided Attempt to "Defend Trade Secrets*," WASH. POST (Dec. 2, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/12/02/and-we-need-stronger-protection-for-trade-secrets-because/?utm_term=.2d9dd7726f29 (characterizing the DTSA bill as anticompetitive and harmful to workers).

160 *See* Pooley, *Inadequacy of Trade Secret Law*, *supra* note 44; *supra* Section I.A, I.B.

161 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1058 ("[The DTSA's] main objective is to make it more practical for trade secret owners, now that their rights can be electronically compromised in mere seconds, to secure effective judicial relief.").

162 *Id.* at 1067 ("As reported by Ocean Tomo, the share of public company value represented by intangible information leapt from 17 percent in 1975 to 68 percent in 1995 to 84 percent in 2015.").

163 *See, e.g.*, *id.* ("[A]mong R&D-intensive firms—who collectively account for two thirds of U.S. R&D investment—secrecy was deemed important at more than twice the level of patents.").

164 18 U.S.C. § 1836(b)(2)(A) (2012 & Supp. IV 2017) (outlining the requirements); *see supra* Section I.B.2.

165 *See* Pooley, *Inadequacy of Trade Secret Law*, *supra* note 44 (describing DTSA procedural protections and damage provisions as safeguards for potential defendants).

widespread deployment of seizures is unfounded.[166] Moreover, despite longstanding concerns about the EEA, extensive prosecutions never materialized, and the annual number of prosecutions remains small.[167]

Adherents of more aggressive IP rights enforcement through the ex parte seizure provision have argued that the provision also sits firmly within a legal framework, including at the state level, that has provided for ex parte seizures in similar contexts.[168] In this way, they argue, the new provision is not unprecedented and may even account for recent technological developments.[169] Supporters have also suggested that the ex parte seizure provisions of the DTSA are a direct and natural extension of the Lanham Act and thus are no cause for concern.[170] In fact, supporters point out that the DTSA contains additional protections and limitations on seizures beyond those contained in the Lanham Act, so the risk of abuse is even lower.[171] In *Vuitton v. White*, the court found that the facts underlying the ex parte seizure at issue were consistent with the purpose of the Lanham Act.[172] Similarly, summary procedures for impounding materials under the Copyright Act have been found acceptable.[173] Nevertheless, constitutional claims for violation of due process in the course of a Lanham Act ex parte seizure have survived pleading.[174] Ultimately, however, the amorphous scope of trade secrets and a transformed technological landscape fundamentally distinguish trade secrets from the earlier trademark and copyright cases.[175]

---

166 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1070 (describing the narrowly drawn seizure remedy tailored to cases where trade secrets are in "immediate peril").

167 *See* Toren, *supra* note 21 ("The government has brought a total of approximately 124 cases.").

168 *See* Pooley, *Why We Need a Seizure Remedy*, *supra* note 44 (showing where state sequestration and attachment provisions have been applied in software cases).

169 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1066–69 (analyzing the statutory requirements against contemporary technology scenarios).

170 Pooley, *Why We Need a Seizure Remedy*, *supra* note 44.

171 *Id.*

172 945 F.2d 569, 575 (3d Cir. 1991) (noting a high degree of overlap between the statutory purpose of ex parte seizures to "thwart the bad faith efforts" of evasive defendants and an alleged fly-by-night operation of dealers (quoting 130 CONG. REC. H31,678 (daily ed. Oct. 10, 1984) (Joint Statement on Trademark Counterfeiting Legislation))).

173 *See* Duchess Music Corp. v. Stern, 458 F.2d 1305, 1308 (9th Cir. 1972) (affirming summary procedure for copyright impoundment and noting that courts do not have "any discretion to determine what to impound" under the Copyright Act).

174 *See* Elec. Lab. Supply Co. v. Motorola, Inc., No. 88-4494, 1989 WL 113127, at *6, *11 (E.D. Pa. Sept. 20, 1989) (denying motion to dismiss for due process and Fourth Amendment claims).

175 *See supra* Section II.C.

B. Overenforcement and Criminalization: Collateral Policy Harms

The DTSA fits within a growing trend of leveraging perceived national security threats to increase enforcement levels, with significant effects for individual actors. Government rhetoric surrounding trade secret enforcement policy strongly emphasizes national security, and information campaigns have particularly highlighted the perceived looming threat of China.[176] Interestingly, in the years immediately after the EEA's passage, government officials emphasized the intersection of terrorism and trade secret theft.[177] This pattern suggests that cynical officials may simply be exploiting the latest and most cogent fear or trend in xenophobic animus to drive increased trade secrets enforcement.[178] A similar rhetorical strategy may be at work in conflating economically valuable technologies with those technologies having direct military or national security applications.[179] The impact of cyberespionage on trade secret theft remains poorly understood, so efforts to address the former through heightened enforcement of the latter remain uncertain.[180] The majority of trade secret cases involve theft by insiders and thus do not involve or require computer-based hacking.[181] As a result, even if the United States could adopt successful policies to curb cyberespionage, such a coup may not have a significant effect in reducing trade secret theft.

At their root, the terms of the ex parte seizure provision represent a poor policy choice because they prioritize property rights enforcement over efficient use and lack sufficient safeguards against overzealous application. The risks of overenforcement are particularly acute for trade secrets because, unlike patents, there is no stipulated timeline for expiration and because trade secrets' impact on innova-

---

176 *See* FBI, *supra* note 6 (providing an example of such a campaign depicting Chinese cyberespionage in a short film); *see also* Dreyfuss & Lobel, *supra* note 5, at 420 (noting that the FBI release of *The Company Man* film occurred during a "nationwide economic espionage awareness campaign" in July 2015).

177 *See* Effron, *supra* note 29, at 1492 ("As the nation braces for global terrorism and war with Iraq, corporate espionage on the home front by foreign spies may be intensifying, security and law enforcement officials warn." (quoting Edward Iwata, *More U.S. Trade Secrets Walk out Door with Foreign Spies*, USA TODAY (Feb. 13, 2003), http://usatoday30.usatoday.com/tech/news/2003-02-12-espionage_x.htm)).

178 *See* Dreyfuss & Lobel, *supra* note 5, at 426 (suggesting xenophobia as a core rhetorical driver for heightened trade secrets enforcement).

179 *Id.* at 426 n.37.

180 *See* Levine & Sandeen, *supra* note 10, at 238 ("[T]he threat to trade secrets as a result of cyberespionage [cannot] be accurately measured. . . . [I]t is 'impossible to know how many trade secret misappropriation incidents are tied to cybersecurity breaches.'").

181 Argento, *supra* note 10, at 222.

tion is uncertain.[182] Beyond the previously discussed concerns, the DTSA presents a looming risk that the ex parte seizure provisions may evolve from limited responses for exigent circumstances to sanction-like tools at the ready disposal of private parties. In *Young v. United States* ex rel. *Vuitton et Fils S.A.*,[183] the Supreme Court expressed concerns about the wisdom of deputizing private actors for enforcement purposes, recognizing the likelihood of conflicts of interest.[184]

The policy concerns raised in *Young* are particularly relevant to the discussion of trade secret enforcement because there is a disconnect between the enforcement measures sought and the government apparatus required to administer them. In contrast to the IP domain, the U.S. government has complex, if at times redundant, expert agencies in place for the regulation of antitrust, securities, and financial activities.[185] In these areas, compliance standards are high and enforcement is government-driven.[186]

In contrast, registering for patent or copyright protection is a comparatively, though not completely, low-cost exercise, but the burden of enforcement also comparatively falls on private parties.[187]

---

[182] *See* Dreyfuss & Lobel, *supra* note 5, at 424–25 (emphasizing the substitution potential of trade secrets for patents).

[183] 481 U.S. 787, 810 (1987) ("[A]ppointment of an interested prosecutor raises such doubts. Prosecution by someone with conflicting loyalties 'calls into question the objectivity of those charged with bringing a defendant to judgment.' . . . It is a fundamental premise . . . that the state wield its formidable criminal enforcement powers in a rigorously disinterested fashion . . . ." (internal citation omitted)).

[184] *Id.*

[185] Compare the privately-directed enforcement in Young v. United States *ex rel.* Vuitton et Fils S.A., 481 U.S. 787, 793 (1987), with the Federal Trade Commission, Securities and Exchange Commission, and Consumer Financial Protection Bureau, though the picture is admittedly complicated by outsourced enforcement. *See* Margaret H. Lemos, *Privatizing Public Litigation*, 104 GEO. L.J. 515, 516–17 (2016) (offering as examples hiring of special counsel for an antitrust enforcement action, mortgage litigation, tobacco litigation, and the use of private donations for special prosecutors).

[186] *See, e.g.*, Piper v. Chris-Craft Indus., Inc., 430 U.S. 1, 25 (1977) (stating that in securities law, private enforcement is a "necessary supplement" to SEC actions "because of practical limitations upon the SEC's enforcement capabilities" (quoting J. I. Case Co. v. Borak, 377 U.S. 426, 432 (1964))); Megan M. La Belle, *Public Enforcement of Patent Law*, 96 B.U. L. REV. 1865, 1870 (2016) (describing how private enforcement supplements agency enforcement).

[187] *See* Dreyfuss & Lobel, *supra* note 5, at 424–25; La Belle, *supra* note 185, at 1883; Dotan Oliar, Nathaniel Pattison & K. Ross Powell, *Copyright Registrations: Who, What, When, Where, and Why*, 92 TEX. L. REV. 2211, 2212–13, 2212 n.4 (2014) (explaining the publicly accessible and widely used copyright registration system in the United States); Justin D. Fitzdam, Note, *Private Enforcement of the Digital Millennium Copyright Act: Effective Without Government Intervention*, 90 CORNELL L. REV. 1085, 1095 (2006) (describing the challenges and problems with private enforcement of the Digital Millennium Copyright Act).

In this way, there may be an emerging disconnect in trade secret enforcement: Trade secrets require no registration, forgoing any type of quid pro quo disclosure fundamental to the bargain of patent law.[188] At the same time, trade secret holders are seeking to leverage powerful government-sanction enforcement tools such as ex parte seizures to further their interests, even as generalist enforcement authorities at the Department of Justice and the U.S. Attorneys' Offices have declined to bring widespread trade secret prosecutions.[189] In this way, rights holders may be seeking to co-opt state enforcement power to expand enforcement of a private right without any commensurate trade-off in either regulatory compliance or disclosure. While trade secret protection may encourage innovation, an efficient level of firm investment in secrecy, and, in some instances, additional disclosures,[190] it is important for the public to capture at least some of the resulting benefit.

Applying this framework to the present, interested corporations, which benefit both from the chilling of employee mobility and from disruptions to competitors, have increasingly powerful tools to effect sanction-like responses to employees and rivals. This risk fits within a broader pattern of privatizing public enforcement activity and litigation.[191] Even before the introduction of a private cause of action for the enforcement of trade secrets, companies have played a prominent role in supporting attention-grabbing cases brought by U.S. Attorneys's Offices and the Department of Justice, such as *United States v. Nosal*, in which the government sought $964,929.65 in attorney's fees alone in restitution for the victim company after it pro-

---

188 *See* Universal Oil Prods. Co. v. Globe Oil & Ref. Co., 322 U.S. 471, 484 (1944) ("As a reward for inventions and to encourage their disclosure, the United States offers a . . . monopoly to an inventor who refrains from keeping his invention a trade secret. But the quid pro quo is disclosure of a process or device in sufficient detail . . . .").

189 *See* Toren, *supra* note 21 (finding relatively few EEA prosecutions since its enactment).

190 *See* Dreyfuss & Lobel, *supra* note 5, at 425 (discussing how trade secret protection may increase innovation by providing value and exclusivity guarantees to innovators); Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 313, 332–35 (2008) ("[P]aradoxically, trade secret law actually encourages disclosure, not secrecy. Without legal protection, companies in certain industries would invest *too much* in keeping secrets. Trade secret law develops as a substitute for the physical and contractual restrictions those companies would otherwise impose. . . . [T]he secrecy requirement serves a channeling function.").

191 *See* Lemos, *supra* note 184, at 516–17 (offering as examples hiring of special counsel for an antitrust enforcement action, mortgage litigation, tobacco litigation, and the use of private donations for special prosecutors).

vided aid to the government in investigating and prosecuting the charges, including EEA violations.[192]

DTSA critics have raised concerns about a further risk that enhanced ex parte seizure provisions, combined with a federal cause of action, could unleash increased litigation where so-called "trade secret troll[s]" (TSTs)[193] could leverage their additional procedural powers to extract *in terrorem* value.[194] While supporters of the ex parte seizure provision rightly identify that it is impossible to make a threat of an ex parte seizure without providing some sort of notice, viewed from a more general lens, this threat may still carry weight. Depending on the size of the firm, the potential liability faced, even if under a dubious claim, may be substantial. In addition, a demand for payment may not be sufficiently specific, in spite of provisions within the law itself,[195] for a firm to be confident that any subsequent seizure would remain cabined to an individual employee or trade secret in question and not implicate other aspects of the business, magnifying the harm and increasing the cost of resisting.

The risk of error and collateral harm from seizures further increases in an environment in which companies have even greater incentives to extract settlements.[196] Although the ex parte seizures themselves cannot play a direct ex ante role in extracting value, because the defendant would require notice before paying a settlement,[197] the disruption of an ex parte seizure may shift the defendant's interests in settling. Though the statute itself precludes issuing ex parte seizure orders in cases where the requested seizure has already been publicized,[198] it is not only an immediate risk of seizure

---

192 828 F.3d 865, 885–88, 897 (9th Cir. 2016) (noting that the plaintiff provided the government with "private assistance of such magnitude" in its EEA prosecution of the plaintiff's economic competitor that it "blur[red] the line between civil and criminal law").

193 *E.g.*, Brees, *supra* note 10, at 278–79 (2017) (describing trade secret trolls as private entities used to collect trade secret rights, initiate misappropriation lawsuits against "unsuspecting" parties, and demand some form of payment in return).

194 *See* Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1046–47 ("[F]ederalizing civil trade secret law would unleash a dangerous new class of litigants called 'trade secret trolls,' who—like their patent counterparts—would terrorize the community of legitimate innovators." (quoting Levine & Sandeen, *supra* note 10, at 230)); *see also* Brees, *supra* note 10, at 279–80 (arguing that "stringent requirements" for ex parte seizures under the DTSA will limit their use by trolls).

195 *See* 18 U.S.C. § 1836(b)(2)(A)(ii)(VI) (2012 & Supp. IV 2017) (requiring a description of the matter and location with "reasonable particularity").

196 Levine & Sandeen, *supra* note 10, at 234 ("By initiating lawsuits designed only to extract settlement payments or massive damage awards from scared defendants, trade secret trolls could cause the same drag on innovation and job growth that has been the hallmark criticism of the well-known 'patent troll.'").

197 Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1072.

198 18 U.S.C. § 1836(b)(2)(A)(ii)(VIII) (2012 & Supp. IV 2017).

but a generalizable threat that is troubling and a potential cause of altered corporate behavior.[199] Further, an environment in which ex parte seizures become common may lead to individual workers and smaller companies—actors with less economic clout—becoming concerned about the risks of an unexpected disruption. Risks are further heightened by the less-certain status of trade secrets vis-à-vis other forms of intellectual property.[200] Unlike patents and copyrights, there is no registration requirement for trade secrets, so they provide no notice of the metes and bounds of potential claims. As a result, trade secrets represent the best of both worlds to rights holders: minimal regulatory costs to secure and maintain, but the vigorous enforcement power of the state to enforce.

There has been a longstanding tension between patent and trade secret law. Whereas patent law requires disclosure of the technology as part of the quid pro quo struck in exchange for a state-sanctioned monopoly, trade secrets are not bound by any set term.[201] While some jurists have expressed skepticism that companies would willingly decline the robust protections of patent law in favor of the uncertainties of trade secret protections, others have been less certain, and doubts have likely only increased as trade secret protection's scope has increased and it has received the protection of federal criminal law.[202] From *Kewanee v. Bicron Corp.* onward, courts and theorists

---

[199] *E.g.*, Levine & Sandeen, *supra* note 10, at 232 (describing concerns about the possible emergence of trolling behavior in trade secret enforcement).

[200] For example, unlike patents, copyrights, and trademarks, trade secrets do not require registration. *See* Dreyfuss & Lobel, *supra* note 5, at 424–25, 428–29; *see also* Levine & Sandeen, *supra* note 10, at 236 ("Exacerbating the risks of passing the [expanded trade secrecy] Acts is the fact that businesses often believe that they own trade secrets when they do not and attempt legal actions on alleged misappropriations of information unworthy of protection . . . .").

[201] *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 493–94 (1974) (Marshall, J., concurring) (opining that "trade secret protection provides in some instances a substantial disincentive to entrance into the patent system," which "deprives society of the benefits of public disclosure of the invention which it is the policy of the patent laws to encourage"); *see also* Dreyfuss & Lobel, *supra* note 5, at 428–29 ("Patent law requires disclosure of the details of protected inventions and lasts only for a specified term . . . . In contrast, trade secrecy allows innovators to hide what they know from others, including from government regulators . . . .").

[202] *See Kewanee Oil Co.*, 416 U.S. at 493–94 ("I do not believe that the possibility that an inventor with a patentable invention will rely on state trade secret law rather than apply for a patent is 'remote indeed.' State trade secret law provides substantial protection to an inventor . . . which in its unlimited duration is clearly superior to . . . patent . . . ." (internal citations omitted)); Gregory V. Novak & Matthew Frontz, *Tipping the Scales: Weighing IP Protection Options Post-DTSA and Post-'Alice*,' TEX. LAW. (Dec. 1, 2016), http://www.texaslawyer.com/id=1202772652834/Tipping-the-Scales-Weighing-IP-Protection-Options-PostDTSA-and-PostAlice ("[The] DTSA, however, provide[s] the type of protection that could push more owners in the direction of trade secret protection over patent protection.").

have relied on twin legal theories for trade secrets: first, the tort theory, which aims to oppose wrongful conduct, e.g., the wrongful exposure of information by theft or breach of confidentiality, and second, the property theory, which classifies trade secrets with patents and copyrights and seeks to incentivize and reward innovative efforts.[203] The risk is particularly acute to the extent that more rigorous enforcement of trade secrets leads rational firms to forsake patent protection—robust in formal protections but requiring disclosure and delimited in time—for trade secret protections.

Beyond specific process-based policy concerns, strengthening enforcement procedures for trade secrets makes them a credible alternative to patents in enforcing IP rights. With the DTSA's shift of parties' incentive equilibrium towards trade secret protection, the United States may be accepting more negative outcomes, including decreased disclosure, fewer information-based externalities, lower employee mobility, reduced competition, suboptimal information levels for policymaking, and deadweight losses associated with monopoly or oligopoly pricing.[204]

C. Judicial Alternatives

Because Congress appears unlikely to engage the deficits in the DTSA, the courts provide the best opportunity to check the DTSA's application and limit its potentially pernicious effects.[205] Action by the courts further offers the advantage of scalability, since any response can be proportional to the ultimate deployment of the seizures under the DTSA. At the same time, this response, until realized, will mean a degree of ex ante uncertainty for potential litigants. In the past, when faced with ex parte seizure provisions not passing constitutional due process muster, courts have heightened procedural requirements to render the procedures consistent with procedures deemed sufficient, such as Rule 65 proceedings.[206] Commentators have also recommended looking to Rule 65 to ameliorate procedural and constitu-

---

[203] *See* Argento, *supra* note 10, at 182–85 (outlining the twin theoretical justifications for trade secrets).

[204] *See, e.g.*, *id.* at 175–76 (discussing economic and social policy drawbacks of trade secret overprotection); Dreyfuss & Lobel, *supra* note 5, at 457–60 (analyzing effects of enhanced trade secret protection on university selection, research, and reputation).

[205] *Cf*. Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1046, 1054 (detailing strong industry and bipartisan support for enhanced trade secret protections paving the way to passing the DTSA, despite broad criticism from academics).

[206] *See, e.g.*, Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 88 (E.D.N.Y. 1993) (analyzing a trend of applying Rule 65 requirements or general principles governing injunctive relief when disposing of ex parte orders of impoundment in copyright cases and citing cases).

tional deficiencies in the context of copyright seizures because its requirements are more substantial.[207]

Another route for courts to limit the potential pernicious effects of the ex parte seizure provision would be to rigorously enforce what protections are present in the statute and to engage plaintiffs' assertions with unusual skepticism. This approach may ultimately prove difficult to apply in practice, however, since courts lack both the technical skill to anticipate downstream and collateral effects of seizures and the experience weighing fact-intensive arguments in the absence of an adversarial process.[208] The DTSA's ex parte seizures may also follow a pattern established by the Lanham Act seizures, in which uncritical procedures led to thousands of seizure orders but surprisingly little case law to develop the doctrine or refine the requirements for subsequent seizures.[209]

A more ambitious course of action might be for courts to look favorably upon constitutionally-based counterclaims in cases where, in spite of compliance with DTSA procedures, the seizure does not meet due process standards. As a result, similar to a prior seizure case under the Trademark Counterfeiting Act, the court would not confine the defendant's recourse for wrongful seizure to the remedy specified in the statute.[210] While this vehicle would provide only ex post relief to harm already realized, the forward-looking deterrent effect of these suits could severely mute the deployment of ex parte seizures. Sophisticated IP rights holders would recognize that effecting such a seizure would entail a not-insignificant financial and legal risk and internally weigh that risk against any perceived benefit of seeking an ex parte seizure under the DTSA. These firms could decide that the marginal benefits are simply not worth the risk and work through more established channels of relief, including Rule 65.

D. Law Reform

Because of potential due process challenges to the ex parte seizure provisions of the EEA and the generally pernicious effects

---

[207] *Cf.* Owens, *supra* note 89, at 250 ("Rule 65 of the Federal Rules of Civil Procedure[ ] . . . should be used to cure the constitutional infirmities of the present impoundment procedures, and would better effectuate the policies underlying the copyright act."); *see supra* Section I.C., notes 83–87 and accompanying text.

[208] *See* discussion *supra* Section II.C.

[209] Baker & Fesak, *supra* note 7, at 742 (quoting Zalon, *supra* note 76, at 191) ("[T]he very ease with which [seizure] orders are granted probably explains the dearth of cases upholding the procedures . . . .").

[210] *See, e.g.*, Gucci Am., Inc. v. Accents, 955 F. Supp. 279, 281 (S.D.N.Y. 1997) (declining in dicta to limit the defendant to statutory remedy as sole recourse in a situation where the defendant's property was "the subject of an improperly-issued seizure order").

they are likely to have on innovation and employee mobility, the most prudent course of action would be legislative reform to significantly pare back the scope of the provision, if not eliminate it entirely.[211]

Given the barriers to the legislative process and extent of national security rhetoric deployed in the defense of trade secrets enforcement, however, legislative change appears unlikely in the immediate term. Although the bill received "unusually bipartisan political sponsorship,"[212] the current President has continued to take a hard line on trade secret theft.[213] But Congress would be wise to correct the DTSA's constitutional infirmity by repealing its ex parte seizure provision in its entirety, requiring plaintiffs to either provide notice or to rely on existing, and more protective, means of relief. In the absence of further congressional action, however, courts are best equipped to act with both the speed and deftness to address the disruption of overenforcement as it emerges.

Conclusion

While technology has magnified the influence of information on commerce both in the United States and worldwide, it has also magnified the risks of disruption. In a highly interconnected and interdependent economy, disruptive risk is not only greater but more difficult to perceive and evaluate ex ante. The ex parte seizure provisions of the DTSA fail both to account for these changes and to protect the interests of defendants and third parties implicated in potential seizures.

The impact of the seizure provision has the potential to reach far beyond the seizures themselves to the extent that a rise in seizures may ultimately lead to changed firm behavior as companies begin to understand the potential disruptive risks and adjust their collective approach to hiring accordingly. Employee mobility is a linchpin of innovation.[214] Organizations and regions alike prosper when individ-

---

211 Some observers recommended this course of action prior to the law's passage. *See, e.g.*, Goldman, *supra* note 8, at 307 (arguing that the provision should be removed because the fact-intensive inquiry defining trade secrets inevitably leads to a high risk of error for trade secret-based ex parte seizures).

212 Pooley, *The Myth of the Trade Secret Troll*, *supra* note 10, at 1046.

213 *See* David J. Lynch, *Trump Orders Larger Tariffs to Punish China for Stealing Trade Secrets*, Wash. Post (Mar. 13, 2018), https://www.washingtonpost.com/business/economy/trump-orders-larger-tariffs-to-punish-china-for-stealing-trade-secrets/2018/03/13/16d109ae-270e-11e8-bc72-077aa4dab9ef_story.html (detailing President Trump's policy of tougher tariffs on Chinese goods in response to trade secret theft).

214 *See* Lobel, *supra* note 18, at 835; *id.* at 837 (citing Kenneth Arrow, *Economic Welfare and the Allocation of Resources for Invention*, *in* The Rate and Direction of Inventive Activity: Economic and Social Factors 609, 615 (Nat'l Bureau of Econ. Research ed., 1962) ("Kenneth Arrow hailed mobility of employees as a central way of spreading information.").

uals are able to apply ideas and technical skills to new problems, and labor markets operate efficiently when employees are able to identify and accept the highest bids for their services.[215] Where companies do not face the threat of employee mobility, they face no incentives to compete to hire or retain better employees.[216] In fact, a recent analysis attempted to place declining competition for employees, described as "labor market monopsony," within the context of a larger policy debate about social mobility and economic inequality.[217] When companies are actively facing a costly problem, it is natural for Congress and enforcement authorities to respond to political pressure and attempt to forestall any adverse political consequences, but it is less obvious how to protect the interests of those likely to be harmed by overzealous enforcements, or the downstream consumers and business partners expected to benefit from their innovative activities.[218]

Both a lack of innovation and creative stagnation can blight institutions that possess little cross-pollination; this problem can occur in even formerly dynamic corporations and economic communities.[219] While these companies may benefit from short- and intermediate-term gains from anticompetitive labor market rents, longer-term prospects may dim under the specter of more innovative and disruptive

---

[215] *See id.* at 793 ("[R]egions that promote employee mobility encourage positive spillovers and densification of knowledge networks, which lead to economic growth and innovation, and conversely . . . regions that restrict employee mobility stifle growth.").

[216] *See* Argento, *supra* note 10, at 185 ("[W]hen employees cannot leave, employers do not compete for the best employees either through compensation or hiring.").

[217] *See* COUNCIL OF ECON. ADVISERS, LABOR MARKET MONOPSONY: TRENDS, CONSEQUENCES, AND POLICY RESPONSES 1 (2016), https://obamawhitehouse.archives.gov/sites/default/files/page/files/20161025_monopsony_labor_mrkt_cea.pdf ("There is also growing concern about an additional cause of inequity—a general reduction in competition among firms, shifting the balance of bargaining power towards employers.") (internal citations omitted); Neil Irwin, *A New Movement in Liberal Economics That Could Shape Hillary Clinton's Agenda*, N.Y. TIMES (Nov. 4, 2016), http://www.nytimes.com/2016/11/06/upshot/monopsony-liberal-economics-policy-hillary-clintons-agenda.html.

[218] *See* Levine & Sandeen, *supra* note 10, at 242–43 (describing the lower political and rhetorical profile of stakeholders supporting broader labor mobility).

[219] *See* Dreyfuss & Lobel, *supra* note 5, at 471 (citing Ajay Agrawal, Iain Cockburn & Carlos Rosell, *Not Invented Here? Innovation in Company Towns*, 67 J. URB. ECON. 78 (2010) (discussing how xenophobic rhetoric surrounding current cyberespionage concerns harms innovation by inhibiting collaboration). Collaboration and information exchange between different enterprises leads to heightened performance in technology-centered environments. One example is MIT's Building 20, where a mix of scientific and technology groups, "who knew little about one another's work," collaborated to become "a legend of innovation, widely regarded as one of the most creative spaces in the world" over the span of fifty years. Jonah Lehrer, *Groupthink: The Brainstorming Myth*, NEW YORKER (Jan. 30, 2012), http://www.newyorker.com/magazine/2012/01/30/groupthink (providing examples of highly innovative institutions containing high rates of interdisciplinary information exchange).

competition from elsewhere.[220] As a result, efforts to pare the effects of the ex parte seizure provisions specifically, and trade secret enforcement more generally, may in fact produce greater innovation and economic growth. As antitrust enforcement activity has diminished in prominence,[221] the United States would be well advised not to swing enforcement on trade secrets so far as to sanction labor mobility or to penalize, however indirectly, those firms and employers seeking to foster increased competition and wage growth for skilled employees. Future innovation, economic growth, and thus—if the rhetoric is to be believed—national security is at stake.

---

220 *See* Argento, *supra* note 10, at 185 (citing Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 584–86 (1999) (explaining that industry cross-pollination leads to new product innovation, which in turn "reset[s] the industry life cycle")).

221 *See* Sam Peltzman, *The Decline of Antitrust Enforcement*, 19 REV. INDUS. ORG. 49, 49 (2001) (describing the loosening of antitrust enforcement practices); *see also* Timothy B. Lee, *Is Ronald Reagan to Blame for the Decline of St. Louis? Some Experts Think So*, VOX (Jul. 14, 2017), https://www.vox.com/new-money/2017/7/14/14702240/antitrust-enforcement-decline-st-louis (arguing that lax antitrust enforcement facilitated strings of mega-mergers, which led to the decline of Midwestern cities and exacerbated regional inequality).