THE DTSA AT ONE: AN EMPIRICAL STUDY OF THE FIRST YEAR OF LITIGATION UNDER THE DEFEND TRADE SECRETS ACT

David S. Levine[*] & *Christopher B. Seaman*[**]

This Article represents the first comprehensive empirical study of the new Defend Trade Secrets Act ("DTSA"), the federal law enacted by Congress in 2016 that expanded trade secret law beyond its traditional roots as a state law doctrine. The DTSA represents the most significant expansion of federal involvement in intellectual property law in at least thirty years. In this study, we examine publicly available docket information and pleadings to assess how private litigants have been utilizing the DTSA's new federal civil cause of action for trade secret misappropriation. Based upon an original dataset of nearly 500 newly filed DTSA cases in federal court, we analyze whether the law is beginning to meet its sponsors' stated goals of creating a more robust and efficient litigation vehicle for trade secret misappropriation victims, thereby helping protect valuable American intellectual property assets.

We find that, similar to state trade secrets law, the paradigm misappropriation scenario under the DTSA involves a former employee who absconds with alleged trade secrets to a competitor. Other results, however, raise

[*] Jennings Professor and Associate Professor of Law, Elon University School of Law; Affiliate Scholar, Stanford Law School Center for Internet and Society; Founder and Host, *Hearsay Culture* (KZSU-FM, Stanford University). Email: dlevine3@elon.edu.

[**] Associate Professor of Law and Director, Frances Lewis Law Center, Washington and Lee University School of Law. Email: seamanc@wlu.edu.

The authors thank Tim Holbrook, Mark Lemley, Dave Schwartz, and Sean Seymore, as well as participants of the 17th Annual Intellectual Property Scholars Conference at Benjamin N. Cardozo School of Law, the Patent Scholars Roundtable at American University Washington College of Law, and a faculty workshop at Wake Forest University School of Law, for feedback on this project. We gratefully acknowledge the valuable research assistance of Lauren Bond, Lauren Johnson, Will Knapp, Y.J. Miller, Benton Morton, Kalie Pritchett, Daniele San Roman, Rachel Stariha, and N. Winston West. Financial support was provided by research grants from the Frances Lewis Law Center at Washington and Lee University School of Law and from the Elon University School of Law.

questions about the law's ability to effectively address modern cyberespionage threats, particularly from foreign actors, as well as the purpose (or lack thereof) of trade secret law more broadly. We conclude by discussing our data's implications for trade secret law and litigation as well as by commenting on the DTSA's potential impact on the broader issues of cybersecurity and information flow within our innovation ecosystem.

TABLE OF CONTENTS

I. INTRODUCTION

The Defend Trade Secret Act of 2016[1] is one of the most significant developments in intellectual property ("IP") law in recent years.[2] Long neglected within IP law,[3] the enactment of the DTSA brings new prominence to trade secrecy by creating for the first time a federal civil cause of action for misappropriation, thus placing trade secrets on par with patents, copyrights, and trademarks. This development, although widely praised by the business community[4] and passed through Congress by near-unanimous margins,[5] was not without controversy. Concerns were raised about the DTSA's potential impact on startups and other innovators, its affect on labor mobility, and its inability to meaningfully combat cyberespionage.[6] Most notably, the DTSA passed despite a paucity of rigorous empirical evidence regarding the role of trade secret law and litigation in promoting innovation.[7]

[1] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

[2] *See* PETER S. MENELL, MARK A. LEMLEY & ROBERT P. MERGES, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2017, at iv (2017) ("[T]he Defend Trade Secrets Act of 2016 [is] one of the most momentous changes in the history of trade secret protection."); Christopher B. Seaman, *Introduction: The Defend Trade Secrets Act of 2015*, 72 WASH. & LEE L. REV. ONLINE 278, 279 (2015) ("[T]he DTSA . . . represent[s] the most significant expansion of federal law in IP since the Lanham Act of 1946."); Eric Goldman, *The New 'Defend Trade Secrets Act' Is The Biggest IP Development In Years*, FORBES: TECH (Apr. 28, 2016, 1:04 PM), https://www.forbes.com/sites/ericgoldman/2016/04/28/the-new-defend-trade-secrets-act-is-the-biggest-ip-development-in-years/#24401ea84261 ("While creating a new federal trade secret claim to complement existing state law may sound more procedural than substantive, the DTSA actually has major consequences for intellectual property law and for our economy.").

[3] *See, e.g.*, 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 ("For decades, trade secrets have been the poor stepchild of intellectual property law."). As coauthor David S. Levine has put it, trade secret law is often viewed as the fourth of three areas of IP law because of its relatively limited treatment by scholars compared to copyright, patent, and trademark law. *See* UNCMJschool, *David S. Levine, Mary Junck Research Colloquium*, YOUTUBE (July 11, 2011), https://www.youtube.com/watch?v=uJGGg5lwLBs (at approximately 4:45).

[4] *See infra* notes 50–58 and accompanying text (describing support for the DTSA).

[5] The roll call vote on the DTSA was 87–0 in the Senate and 410–2 in the House of Representatives. 162 CONG. REC. S1635–36 (daily ed. Apr. 4, 2016); 162 CONG. REC. H2046–47 (daily ed. Apr. 27, 2016).

[6] *See infra* notes 59–63 and accompanying text (describing opposition to the DTSA). The authors were among the group of academics that opposed the DTSA. *See infra* note 59.

[7] *See* Michael Risch, *Empirical Methods in Trade Secret Research*, *in* 2 RESEARCH HANDBOOK ON THE ECONOMICS OF INTELLECTUAL PROPERTY LAW (Peter S. Menell & David L. Schwartz eds., forthcoming 2018) (manuscript at 1), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2658685 (surveying the relevant empirical literature and concluding that "the reality is that we know

This Article will help fill an empirical void regarding the most important development in modern trade secret law by examining the early evidence on how the DTSA is being utilized by industry and the bar. Even though the DTSA has been in force for less than two years, it is ripe for a preliminary evaluation. Through a detailed examination of the nearly 500 cases filed in the DTSA's first year,[8] this Article presents a robust dataset from which to identify early trends and implications. In short, this Article will help inform courts,[9] practitioners,[10] policymakers,[11] and

very little about trade secrets, despite the best efforts of a handful of scholars conducting research in this area"). *See generally* David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94 NOTRE DAME L. REV. (forthcoming 2018) (reviewing the existing empirical literature regarding startups' use of trade secrecy and noting the limited extent of trade secret empirical study).

[8] The DTSA's effective date is May 11, 2016. *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

[9] Some early commentary has described challenges that courts will face in interpreting and applying various provisions of the DTSA. *See* Peter S. Menell, *Misconstruing Whistleblower Immunity Under the Defend Trade Secrets Act*, 1 NEV. L.J. FORUM 92, 94–95 (2017) (contending that the district court in *Unum Group v. Loftus*, 220 F. Supp. 3d 143 (D. Mass. 2016), misinterpreted the whistleblower protection provision of the DTSA); Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L.J. 829, 887–911 (2017) (describing various issues that federal courts likely must address in interpreting and applying the DTSA).

[10] There has been substantial practitioner commentary about how the DTSA may impact IP disputes. *See, e.g.*, Dave Bohrer, *Extending US Trade Secret Law to Reach IP Theft in China*, FLAT FEE IP BLOG (Apr. 11, 2017), http://www.flatfeeipblog.com/2017/04/articles/trade-secrets/extending-us-trade-secret-law-to-reach-ip-theft-in-china ("Bringing suit in federal court provides several procedural advantages over state court and asserting a claim under the DTSA gives the federal court federal question jurisdiction."); *The Defend Trade Secrets Act 2016, a Strong Argument to Mediate IP Disputes*, BOILEAU CONFLICT SOLUTIONS: BCS MEDIATION BLOG (July 27, 2017), http://www.boileaucs.com/defend-trade-secrets-act-2016-strong-argument-mediate-ip-disputes ("Mediation privacy is the obvious reason to choose this option, but it is only one reason amongst many. There are plenty of other reasons, including reasons that lie within the provisions of the Uniform Trade Secrets Act and the recent Defend Trade Secrets Act (2016) themselves."); George L. Kanabe & Diana Fassbender, *Pillow Talk: A Threat to Trade Secrets?*, TRADE SECRETS WATCH (July 20, 2017), http://blogs.orrick.com/trade-secrets-watch/2017/07/20/pillow-talk-a-threat-to-trade-secrets (describing a recent DTSA complaint).

[11] For example, the lack of hacking claims under the DTSA, *see infra* Subpart IV.B.7, suggests that Congress may pursue additional legislation that more directly targets the problem of cyberespionage. *See, e.g.*, Morgan Chalfant, *Congress Set to Vote on Cyber Bills*, HILL (May 15, 2017, 11:26 AM), http://thehill.com/policy/cybersecurity/333421-congress-eyes-movement-on-cyber-bills.

scholars[12] about the potential benefits, drawbacks, and limitations of the DTSA.

More generally, this Article addresses a timely issue, as trade secret theft and litigation are on the rise.[13] The theft of valuable

[12] There was and has been a significant uptick in trade secret law scholarship concurrent with and since the DTSA's passage. *See, e.g.*, Derek E. Bambauer, *Secrecy is Dead – Long Live Trade Secrets*, 93 DENV. L. REV. 833 (2016); John Cannan, *A (Mostly) Legislative History of the Defend Trade Secrets Act of 2016*, 109 L. LIBR. J. 363 (2017); Stephen Y. Chow, *DTSA: A Federal Tort of Unfair Competition in Aerial Reconnaissance, Broken Deals, and Employment*, 72 WASH. & LEE L. REV. ONLINE 341 (2016); Richard F. Dole, Jr., *Identifying the Trade Secrets at Issue in Litigation Under the Uniform Trade Secrets Act and the Federal Defend Trade Secrets Act*, 33 SANTA CLARA HIGH TECH. L.J. 470 (2017); Rochelle Cooper Dreyfuss & Orly Lobel, *Economic Espionage as Reality or Rhetoric: Equating Trade Secrecy with National Security*, 20 LEWIS & CLARK L. REV. 419 (2016); Robin J. Effron, *Trade Secrets, Extraterritoriality, and Jurisdiction*, 51 WAKE FOREST L. REV. 765 (2016); Michelle Evans, *Plausibility Under the Defend Trade Secrets Act*, 16 J. MARSHALL REV. INTELL. PROP. L. 188 (2017); Eric Goldman, *The Defend Trade Secrets Act Isn't an "Intellectual Property" Law*, 33 SANTA CLARA HIGH TECH L.J. 541 (2017); Eric Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, 72 WASH. & LEE L. REV. ONLINE 284 (2015) [hereinafter Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*]; Robert A. Kearney, *Why the Burden of Proving Causation Should Shift to the Defendant Under the New Federal Trade Secrets Act*, 13 HASTINGS BUS. L.J. 1 (2016); David S. Levine, *School Boy's Tricks: Reasonable Cybersecurity and the Panic of Law Creation*, 72 WASH. & LEE L. REV. ONLINE 323 (2015); David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015); Menell, *supra* note 9; Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CALIF. L. REV. 1 (2017); Laura G. Pedraza-Fariña, *Spill Your (Trade) Secrets: Knowledge Networks as Innovation Drivers*, 92 NOTRE DAME L. REV. 1561 (2017); 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); Elizabeth A. Rowe, *RATs, TRAPs, and Trade Secrets*, 57 B.C. L. REV. 381 (2016); Elizabeth A. Rowe, *Unpacking Trade Secret Damages*, 55 HOUS. L. REV. 155 (2017); Sharon K. Sandeen, *The DTSA: The Litigator's Full-Employment Act*, 72 WASH. & LEE L. REV. ONLINE 308 (2015); Sharon K. Sandeen & Elizabeth A. Rowe, *Debating Employee Non-Competes and Trade Secrets*, 33 SANTA CLARA HIGH TECH. L.J. 438 (2017); Sandeen & Seaman, *supra* note 9; Christopher B. Seaman, *The Case Against Federalizing Trade Secrecy*, 101 VA. L. REV. 317 (2015); Seaman, *supra* note 2; Conor D. Tucker, *Interstate Trade Secrets? A Principled Framework for Identifying Federal Trade Secrets*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2017); Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357 (2017); Brennan R. Block, Note, *Nebraska Trade Secret Protection: The Forum Selection Conundrum Facing Trade Secret Owners After the Defend Trade Secrets Act of 2016*, 50 CREIGHTON L. REV. 559 (2017); Patrick J. Manion, Note, *Two Steps Forward, One Step Back: The Defend Trade Secrets Act of 2016 and Why the Computer Fraud and Abuse Act of 1984 Still Matters for Trade Secret Misappropriation*, 43 J. LEGIS. 289 (2017).

[13] *See* David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L.J. 1091, 1092 (2012) ("Over the past three decades, trade secret litigation in federal courts has grown exponentially, doubling roughly every decade, while federal litigation has

information through cyberespionage has become front-page news,[14] with companies ranging from entertainment[15] to defense[16] coming under attack, encompassing significant threats to U.S. national security and democracy. In response, companies that are developing "blockbuster new technologies in fields such as robotics, virtual reality and self-driving cars are increasingly hauling each other into court to protect their trade secrets in a series of legal fights that signal

decreased overall. And over the past two decades, trade secret litigation in state court has increased at a rate faster than that of state litigation in general.").

[14] *See, e.g.*, Eric Lipton et al., *Hacking the Democrats: How Russia Honed Its Cyberpower and Trained It on an American Election*, N.Y. TIMES, Dec. 14, 2016, at A1 (recounting a "cyberespionage and information-warfare campaign devised to disrupt the 2016 presidential election" by "a cyberespionage team linked to the Russian government"); Ali Breland, *Target to Pay States $18.5M Over Hack*, HILL (May 23, 2017, 12:59 PM), http://thehill.com/policy/cybersecurity/334747-target-agrees-to-185-million-settlement-for-2013-data-breach ("The hack compromised millions of customer accounts, including credit card and contact information."); Samuel Gibbs, *Dropbox Hack Leads to Leaking of 68m User Passwords on the Internet*, GUARDIAN (Aug. 31, 2016, 6:43 PM), https://www.theguardian.com/technology/2016/aug/31/dropbox-hack-passwords-68m-data-breach ("The company had around 100m customers at the time, meaning the data dump represents over two-thirds of its user accounts."); Nicky Woolf, *DDoS Attack That Disrupted Internet Was Largest of its Kind in History, Experts Say*, GUARDIAN (Oct. 26, 2016, 4:42 PM), https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet ("The victim was the servers of Dyn, a company that controls much of the internet's domain name system (DNS) infrastructure. It was hit on 21 October and remained under sustained assault for most of the day, bringing down sites including Twitter, the Guardian, Netflix, Reddit, CNN and many others in Europe and the US.").

[15] *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Is Said to Find North Korea Ordered Cyberattack on Sony*, N.Y. TIMES, Dec. 18, 2014, at A1 (reporting that "American officials have concluded that North Korea was 'centrally involved' in the hacking of Sony Pictures computers"); Daniel Victor, *HBO is Hacked; Intruder Claims to Have Details from Top Series*, N.Y. TIMES, Aug. 1, 2017, at B4 (reporting HBO's confirmation that it "had been the target of a cyberattack" involving data and material from several unaired HBO shows).

[16] *See, e.g.*, Jon Ostrower, *Chinese Executive Pleads Guilty to Hacking U.S. Defense Contractors*, WALL ST. J. (Mar. 24, 2016, 10:02 AM), https://www.wsj.com/articles/chinese-executive-pleads-guilty-to-hacking-u-s-defense-contractors-1458774419 (reporting that Chinese aviation executive Su Bin pled guilty in federal court for "conspiring to hack and steal sensitive data from Boeing Co. and other U.S. defense contractors"); Adam Segal, *Why China Hacks the World*, CHRISTIAN SCI. MONITOR (Jan. 31, 2016), https://www.csmonitor.com/World/Asia-Pacific/2016/0131/Why-China-hacks-the-world (reporting that between 2009 and 2011, "hackers stole some 630,000 files from Boeing related to the C-17, the third most expensive plane that the Pentagon has ever developed, with research and development costs of $3.4 billion"); *see also* Aaron J. Burstein, *Trade Secrecy As an Instrument of National Security? Rethinking the Foundations of Economic Espionage*, 41 ARIZ. ST. L.J. 933, 938 (2009) (contending there is a "mismatch between the means of trade secrecy—providing private parties with an IP right—and the ends of protecting national security interests"); Dreyfuss & Lobel, *supra* note 12, at 434–46 (critically analyzing the use of national security rhetoric in trade secret policy).

the fierce competition in emerging fields."[17] Although it is difficult to quantify the economic losses from misappropriation,[18] there is no doubt cyberespionage is a significant and growing threat.[19]

Indeed, because of the breadth of personal and private information held by corporations, the damage from trade secret misappropriation now extends to private citizens, entwining trade secret law with privacy interests.[20] For example, in an alleged attack on 500 million Yahoo email accounts, hackers allegedly backed by the Russian government purportedly "stole the secret cryptographic values that Yahoo assigns to each user for generating cookies, the files on a person's computer that contain details of their login history."[21] Armed with this information, the attackers then were able to steal the "contents of 6,500 Yahoo[] accounts."[22] In light of the rapid expansion of knowledge and information as a source of both economic value[23] and national security (in light of constant efforts to

[17] Alexis Kramer, *Trade Secret Cases Surge as Race for New Tech, Top Talent Heats Up*, BLOOMBERG BNA (May 10, 2017), https://www.bna.com/trade-secret-cases-n73014450731 (noting "at least 35 cases" filed under the DTSA by companies in "robotics, alternative energies, semiconductors, online games and other emerging technologies").

[18] *See infra* note 23 and accompanying text.

[19] *See* Levine, *supra* note 12, at 325 ("To be sure, there is a major problem in how we approach cybersecurity as a country.").

[20] *See* David S. Levine, *Secrecy and Accountability: Trade Secrets in Our Public Infrastructure*, 59 FLA. L. REV. 135, 135 (2007) (arguing that although there are good reasons to promote trade secrecy in private commerce, "trade secrecy must give way to traditional notions of transparency and accountability" in some circumstances).

[21] Michael Riley et al., *Russian Agents Accused by U.S. of Masterminding Yahoo Hack*, BLOOMBERG (Mar. 15, 2017, 6:26 PM), https://www.bloomberg.com/news/articles/2017-03-15/russian-spy-agents-accused-by-u-s-of-masterminding-yahoo-hack.

[22] *Id.*

[23] While hard numbers about the cost of IP theft, including trade secret misappropriation, are hard to determine and potentially exaggerated, they are commonly claimed to be in the hundreds of billions of dollars. *See, e.g.*, COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., THE IP COMMISSION REPORT 1 (2013), http://ipcommission.org/report/IP_Commission_Report_052213.pdf ("The scale of international theft of American [IP] is unprecedented—hundreds of billions of dollars per year . . . ."); COMM'N ON THE THEFT OF AM. INTELLECTUAL PROP., UPDATE TO THE IP COMMISSION REPORT 1 (2017), http://www.ipcommission.org/report/IP_Commission_Report_Update_2017.pdf ("[T]he theft of IP remains a grave threat to the United States . . . . We estimate that the annual cost to the U.S. economy . . . [of] counterfeit goods, pirated software, and theft of trade secrets . . . could be as high as $600 billion." (emphasis omitted)); Ellen Nakashima & Andrea Peterson, *Report: Cybercrime and Espionage Costs $445 Billion Annually*, WASH. POST (June 9, 2014), https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html?utm_term=.852a2c59de90 (citing an estimate from the Center for Strategic and International Studies that "the likely annual cost of cybercrime and economic

steal U.S.-defense-related trade secrets),[24] combined with the amount of private information held by corporate entities about their customers, trade secret law has never been more important to understand.

While cyberespionage often results in headline-grabbing stories, previous studies have shown that the bulk of trade secret litigation involves more mundane misconduct—a rogue employee who departs with trade secret information and joins a competitor or launches a new company.[25] The data collected in this study suggest that litigation under the DTSA follows a similar trend.[26] It also supports the existing understanding that trade secret misappropriation is most often committed by a person in some sort of fiduciary or confidential relationship with the victim.[27] In short, instances of hacking and other intrusions, while high profile and often devastating to their victims, remain low compared to bread-and-butter departing employee claims.[28]

The remainder of this Article proceeds as follows. Part II provides an overview of trade secrecy generally, including the state of

espionage to the world economy [is] more than $445 billion," including about $100 billion in the United States alone); *see also* David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 292 (2010) ("There is little data on the exact value of trade secrets because trade secrets are, by definition, secret. Economists nonetheless estimate that trade secrets are a large and increasing percentage of IP."); 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, 197–99 (2014) (stating "there is little to no basis" for many estimates regarding "the level of cyber-hacking damage" and explaining why "calculating losses from . . . trade secret theft is very difficult").

[24] *See* U.S. DEP'T OF HOMELAND SEC. & FBI, GRIZZLY STEPPE – RUSSIAN MALICIOUS CYBER ACTIVITY 1 (2016), https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf ("These cyber operations have included spearphishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations leading to the theft of information."); *see also* Jon Swartz & Rachel Sandler, *Petya Cyberattack Spreads, Hitting U.S. Businesses*, USA TODAY (Jun. 27, 2017, 1:45 PM), https://www.usatoday.com/story/tech/news/2017/06/27/large-cyberattack-hits-europe-disrupts-power-grid-banks/103226268 ("A virulent new strain of ransomware named Petya wreaked havoc on some of the most-established companies in Europe and North America on Tuesday, capitalizing on the same vulnerabilities that froze hundreds of thousands of computers.").

[25] *See* Almeling et al., *supra* note 23, at 294 ("In over 85% of trade secret cases, the alleged misappropriator was someone the trade secret owner knew—either an employee or a business partner."); David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 69 (2011) (noting that 93% of trade secret cases in state court involved an employee or a business partner).

[26] *See infra* Subpart IV.B.5.

[27] *See infra id.*

[28] *See infra* Part I.

the field prior to the DTSA's passage, the DTSA's history and key provisions, and the current state of empirical research on trade secret law and litigation. Part III explains the study's objective, methodology, and limitations. Part IV describes and analyzes the results from the study, while Part V identifies implications for information system, cybersecurity, and trade secret law and policy, as well as areas for potential future research.

II. AN OVERVIEW OF TRADE SECRECY

To provide context for our study's findings, a brief overview of trade secret law and its use by businesses is helpful.[29] This Part first summarizes the evolution of trade secret law in the United States prior to the DTSA. It then offers an introduction to the DTSA and its main provisions. Finally, it highlights the current state of empirical research into trade secrecy.

A. Trade Secret Law prior to the DTSA

Historically, trade secrecy has been governed by state law.[30] Prior to the DTSA, the dominant trade secret doctrine in the United States was the Uniform Trade Secrets Act ("UTSA"),[31] which has been adopted by forty-seven states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.[32] The UTSA defines a trade secret as

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known or readily ascertainable by other who can obtain economic value from its disclosure or use, and (ii) is the

[29] For a more detailed treatment of trade secret law, see generally Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311 (2008); Levine, *supra* note 20; Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1 (2007); Sandeen & Rowe, *supra* note 12. *See also* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of a Justification* 86 CALIF. L. REV. 241, 243 (1998) (providing a detailed survey of the history of trade secret law and arguing that "there is no such thing as a normatively autonomous body of trade secret law").

[30] *See* Sandeen & Seaman, *supra* note 9, at 832 ("For over 175 years, state law governed civil trade secret principles in the United States . . . .").

[31] UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985).

[32] *Trade Secrets Act: Enactment Status Map*, UNIFORM L. COMMISSION, http://www.uniformlaws.org/Act.aspx?title=trade%20Secrets%20Act (last visited Apr. 10, 2018). The only states not to adopt the UTSA are New York, Massachusetts, and North Carolina, although North Carolina has a statute that is similar to the UTSA. *See* N.C. GEN. STAT. §§ 66-152 to -157 (2017). A number of other states have modified various provisions of the UTSA in adopting it as statutory law. *See generally* BRIAN M. MALSBERGER, TRADE SECRETS: A STATE-BY-STATE SURVEY (5th ed. 2015).

> subject of reasonable efforts, under the circumstances, to maintain its secrecy.[33]

This definition is very broad.[34] As the Iowa Supreme Court has explained, "There is virtually no category of information that cannot, as long as the information is protected from disclosure to the public, constitute a trade secret."[35]

A trade secret is misappropriated when it is acquired through improper means, such as theft, bribery, misrepresentation, breach of a fiduciary duty or a duty to maintain secrecy, or espionage through electronic or other means.[36] Misappropriation also occurs when a party discloses or uses a trade secret without consent if the party "knew or had reason to know" that the trade secret was originally acquired by improper means or in violation of a duty of secrecy.[37] Injunctive and monetary remedies are available against a misappropriator.[38] This basic structure has driven nearly all U.S. trade secret law and litigation over the past several decades.[39]

Prior to the DTSA, federal involvement in trade secret law was largely confined to the Economic Espionage Act of 1996 ("EEA"),[40] which was the "first major federal statute to address trade secret misappropriation" by "criminaliz[ing] trade secret misappropriation and authoriz[ing] broad domestic and international enforcement measures against trade secret misappropriation."[41] Similar to subsequent justifications for the DTSA, the EEA was enacted in response to the seemingly increased risk of misappropriation using

[33] UNIF. TRADE SECRETS ACT § 1(4).

[34] *See* MELVIN F. JAGER, TRADE SECRETS LAW § 3:34 (2017) ("The statutory definition of trade secrets is very broad.").

[35] US W. Commc'ns, Inc. v. Office of Consumer Advocate, 498 N.W.2d 711, 714 (Iowa 1993).

[36] UNIF. TRADE SECRETS ACT § 1(2)(i). "Improper means" also may include "otherwise lawful conduct which is improper under the circumstances." *Id.* § 1 cmt. The UTSA also specifies some "proper means," including discovery of the trade secret through "independent invention," "reverse engineering," or by "observation of [an] item in public use or on public display." *Id.*

[37] *Id.* § 1(2)(ii).

[38] *Id.* §§ 2–4.

[39] *See* Seaman, *supra* note 12, at 353 (explaining that "[t]he UTSA effectively serves as a de facto national standard" governing trade secrecy).

[40] Pub. L. No. 104-294, 110 Stat. 3488 (1996) (codified at 18 U.S.C. §§ 1831–1839 (2012)). The Trade Secrets Act, 18 U.S.C. §§ 1905–1909 (2012), makes it a misdemeanor offense for federal employees to publicly disclose trade secret information learned in their official duties, but this statute does not apply to private actors and is rarely invoked. More commonly, some private plaintiffs used other federal statutes, such as the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012), to assert claims related to the misappropriation of trade secrets and other proprietary and confidential information. *See* Seaman, *supra* note 12, at 330–38 (summarizing other federal statutes that are potentially applicable to trade secret theft).

[41] Effron, *supra* note 12, at 765.

new technologies like the internet.[42] However, in the intervening twenty years, EEA prosecutions were sparse,[43] while the United States faced a growing threat of cyberespionage by foreign actors, notably China[44] and Russia.[45] Moreover, a growing chorus of industry lobbyists and related entities complained that U.S. trade secret law was not up to the cyberespionage challenge,[46] while others criticized the use of "criminal law to enforce trade secret policy."[47]

B. The Defend Trade Secrets Act of 2016

With trade secret theft and litigation on the rise,[48] the DTSA was first introduced in Congress on April 29, 2014.[49] Senators Chris

[42] *See* Sandeen & Seaman, *supra* note 9, at 841–42 ("[I]n the wake of claims of widespread espionage by foreign actors against domestic industry (a theme revisited with the DTSA), Congress provided for criminal penalties for two forms of trade secret theft: (1) espionage on behalf of a foreign entity and (2) theft of trade secrets for pecuniary gain.").

[43] *See* Effron, *supra* note 12, at 768 ("[I]n practice, the United States has prosecuted very few cases under the EEA.").

[44] Recent reports suggest that Chinese cyberespionage has dropped, but the DTSA became law as this was transpiring. *See* Joseph Menn & Jim Finkle, *Chinese Economic Cyber-Espionage Plummets in U.S.: Experts*, REUTERS (June 20, 2016, 8:06 PM), http://www.reuters.com/article/us-cyber-spying-china-idUSKCN0Z700D ("FireEye Inc., the U.S. network security company best known for fighting sophisticated Chinese hacking, said in a report released late Monday that breaches attributed to China-based groups had plunged by 90 percent in the past two years."). Still, China remains a leading source of cyberespionage. *See id.* ("FireEye and CrowdStrike said they were confident that [the referenced cyberespionage] attacks are being carried out either directly by the Chinese government or on its behalf by hired contractors."). Additionally, the current U.S. administration's dealings with China could lead to an uptick in Chinese cyberespionage. *See* Brian Bennett, *Trump's Erratic Style Could Undermine China's Agreement to Stop Hacking U.S. Businesses*, L.A. TIMES (Apr. 3, 2017, 4:10 PM), http://www.latimes.com/politics/la-fg-us-china-cyber-20170403-story.html ("President Trump's erratic style and free-form diplomacy have U.S. cybersecurity experts concerned that he might undermine an Obama-era deal with Beijing that sharply curbed widespread Chinese cyberthefts for economic gain and unleash a new flood of hacks against U.S. companies.").

[45] U.S. DEP'T OF HOMELAND SEC. & FBI, *supra* note 24 ("In foreign countries, [Russian civilian and military intelligence services ("RIS")] actors conducted damaging and/or disruptive cyber-attacks, including attacks on critical infrastructure networks. In some cases, RIS actors masqueraded as third parties, hiding behind false online personas designed to cause the victim to misattribute the source of the attack.").

[46] *See infra* notes 50–51 and accompanying text.

[47] Effron, *supra* note 12, at 765.

[48] *See* Almeling et al., *supra* note 23, at 293 ("Trade secret litigation is growing exponentially.").

[49] S. 2267, 113th Cong. (2014); *see also* 160 CONG. REC. S2470 (daily ed. Apr. 29, 2014) (introducing S. 2267, the Defend Trade Secrets Act of 2014). Senator Coons, as well as other members of Congress, previously introduced proposals to create a federal civil cause of action for trade secret misappropriation, but none of those bills received a floor vote in either chamber prior to 2016. *See* Seaman,

Coons (D-DE) and Orrin Hatch (R-UT) celebrated the DTSA's introduction with a flourish, stating that

> in today's electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor. These losses put U.S. jobs at risk and threaten incentives for continued investment in research and development. Current federal criminal law is insufficient.[50]

The DTSA was backed by "a number of high-technology and manufacturing firms, the U.S. Chamber of Commerce, and the Section of Intellectual Property Law of the American Bar Association,"[51] as well as by scholars affiliated with George Mason University's Center for the Protection of Intellectual Property.[52] From its inception, the DTSA allowed trade secret owners to bring a civil action in federal court for trade secret misappropriation.[53]

Despite robust trade secret law under the UTSA, bipartisan DTSA supporters initially asserted that existing law was insufficient to address the problem of state-sponsored and private corporate

supra note 12, at 340–48 (describing proposed federal civil trade secrets legislation prior to the DTSA); *see also* Sandeen & Seaman, *supra* note 9, at 843–57 (summarizing the legislative history of the DTSA, including prior bills).

[50] Press Release, Senators Orrin Hatch & Chris Coons, Hatch, Coons Introduce Bill to Combat Theft of Trade Secrets, Protect Jobs (Apr. 29, 2014), https://votesmart.org/public-statement/867567/hatch-coons-introduce-bill-to-combat-theft-of-trade-secrets-protect-jobs#.WXt_9dKGPIU ("American companies are losing jobs because of the theft of trade secrets every day. This bipartisan bill will empower American companies to protect their jobs by legally confronting those who steal their trade secrets.").

[51] Seaman, *supra* note 2, at 281–82 (footnotes omitted); *see also* Isaac Arnsdorf, *How a Bill (with Virtually No Opposition Still Takes Two Years Before It Almost) Becomes a Law (in 2016)*, POLITICO (May 9, 2016, 2:00 PM), http://www.politico.com/tipsheets/politico-influence/2016/05/how-a-bill-with-virtually-no-opposition-still-takes-two-years-before-it-almost-becomes-a-law-in-2016-214194 ("The Defend Trade Secrets Act of 2016 (S. 1890) is the result of a two-year effort by a broad business coalition from Bayer and 3M to GE and Google."); Mark Schultz, *Debunking Myths About the Proposed Federal Trade Secrets Act*, CTR. FOR PROTECTION INTELL. PROP. (Nov. 17, 2015), https://cpip.gmu.edu/2015/11/17/debunking-myths-about-the-proposed-federal-trade-secrets-act ("Vital proprietary information that once would have resided in file cabinets and that would have taken days to copy now can be downloaded at the speed of light.").

[52] *See* Schultz, *supra* note 51 ("The DTSA is needed to improve the speed and efficiency of trade secret protection in the U.S."). *See generally* Pooley, *supra* note 12 (advocating for the DTSA's enactment). Mr. Pooley's article was apparently sponsored and promoted by the Center for the Protection of Intellectual Property ("CPIP"). *See* Schultz, *supra* note 51 ("CPIP is proud to release a paper authored by . . . James Pooley. Mr. Pooley's paper explains the arguments in favor of the Defend Trade Secrets Act . . . .").

[53] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376.

cyberespionage.[54] Closer to its passage, however, the sponsors changed course and argued that the primary need for the DTSA stemmed from alleged litigation inefficiencies and challenges facing plaintiffs under state law.[55] In addition, the sponsors contended (with the backing of entities like 3M, DuPont, the U.S. Chamber of Commerce, and the Section of Intellectual Property Law of the American Bar Association)[56] that the DTSA was justified to combat "the rise of trade secret theft by rogue employees" and to allow "uniformity" in trade secret law.[57] For example, Senator Coons explained that "[w]e need this bill now more than ever as more and

[54] *See* Press Release, Senators Orrin Hatch & Chris Coons, *supra* note 50. The argument that new laws are needed because of the internet has been advanced numerous times since the mid-1990s. *See* Mark A. Lemley, David S. Levine & David G. Post, *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34, 37 (2011) ("Laws protecting Internet intermediaries from liability for content on the Internet are responsible for transforming the Internet into the revolutionary communications medium that it is today. They reflect a policy that has not only helped make the United States the world leader in a wide range of Internet-related industries, but that has also enabled the Internet's uniquely decentralized structure to serve as a global platform for innovation, speech, collaboration, civic engagement, and economic growth."); Levine, *supra* note 12, at 324–25 ("Suggesting the breadth of the issue and the scope of legislative proposals, more than twenty bills [were] introduced in the 114th Congress purporting to address 'data-breach notification, incidents involving other nation-states, information sharing, law enforcement and cybercrime, protection of critical infrastructure . . . , workforce development, and education.'" (quoting RITA TEHAN, CONG. RESEARCH SERV., R43317, CYBERSECURITY: LEGISLATION, HEARINGS, AND EXECUTIVE BRANCH DOCUMENTS 2 (2015), https://www.fas.org/sgp/crs/misc/R43317.pdf)); David S. Levine, *Professors' Letter in Opposition to the "Cybersecurity Information Sharing Act" (S. 754)*, CTR. FOR INTERNET & SOC'Y, STAN. L. SCH. (Oct. 26, 2015, 8:41 PM), http://cyberlaw.stanford.edu/blog/2015/10/professors-letter-opposition-cybersecurity-information-sharing-act-s-754 ("Rather than encouraging companies to increase their own cybersecurity standards, [the Cybersecurity Information Sharing Act] ignores that goal and offloads responsibility to a generalized public-private secret information sharing network."); *see also* Risch, *supra* note 29, at 5 ("[T]rade secret law is not merely a result of irrational and inefficient decision making. Instead, trade secrets are justified by the economic benefits that flow from their existence, most notably for businesses to spend less money protecting secret information or attempting to appropriate secret information."); Press Release, Senators Orrin Hatch & Chris Coons, *supra* note 50.

[55] *See* David S. Levine, *The Anti-Cyberespionage Bill That Isn't, Or Never Was?*, CTR. FOR INTERNET & SOC'Y, STAN. L. SCH. (Jan. 23, 2016, 1:14 PM), http://cyberlaw.stanford.edu/blog/2016/01/anti-cyberespionage-bill-isnt-or-never-was.

[56] *See* Sandeen & Seaman, *supra* note 9, at 854–55 (describing the extensive lobbying efforts in support of the DTSA).

[57] *See* Levine, *supra* note 55 ("[I]f the new primary foci are the 'rogue employee' and a purported need for uniformity, then the DTSA's imbalance on the cost-benefit scale is even greater.").

more American companies are losing jobs and revenue because they lack the ability to defend their trade secrets under federal civil law."[58]

The only organized opposition to the DTSA came from a group of law professors.[59] In a series of letters and articles, these academics (including both authors) raised several concerns, including that the DTSA would (1) not meaningfully address cyberespionage; (2) likely result in less uniformity in trade secret law; (3) negatively impact information flows; and (4) potentially impose other costs on innovators, particularly startups and small businesses, through its ex parte seizure remedy and impact on labor mobility.[60] Similarly, in a 2015 letter to Congress, these academics identified the following potential drawbacks of the bill:

> (1) the DTSA's *ex parte* seizure provision may harm small businesses, startups and other innovators, (2) the DTSA appears to implicitly recognize the inevitable disclosure doctrine, (3) the DTSA likely will increase the length and cost of trade secret litigation, and (4) the DTSA will likely result in less uniformity in trade secret law.[61]

With particular regard to the question of the DTSA's impact on cyberespionage, David S. Levine and Sharon Sandeen argued that the "dearth of data, combined with a widely held but unsubstantiated belief that a federal private cause of action would help, will not help to address, much less solve, the unquantified problem of cyberespionage."[62] Perhaps due to this opposition, the controversial ex parte seizure provision was significantly modified to include requirements that renders such relief more difficult to award.[63]

[58] Corey Bennett, *Trade Secret Bill Targets Local Theft, Not Foreign Snooping*, HILL (Dec. 2, 2015, 1:43 PM), http://thehill.com/policy/cybersecurity/261807-trade-secret-bill-targets-local-theft-not-foreign-snooping ("[L]awmakers pointed to the inability of American companies to go after current and former employees who steal trade secrets, such as a secret recipe or a customer list.").

[59] *See, e.g.*, Eric Goldman et al., Professors' Letter in Opposition to the Defend Trade Secrets Act of 2015 (S. 1890, H.R. 3326) (Nov. 17, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699760 [hereinafter Professors' 2015 Letter]; *see also* David S. Levine et al., Professors' Letter in Opposition to the "Defend Trade Secrets Act of 2014" (S. 2267) and the "Trade Secret Protection Act of 2014" (H.R. 5233) (Aug. 26, 2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2699735 [hereinafter Professors' 2014 Letter]. Both authors were among the drafters of the professors' letters in opposition to the DTSA.

[60] *See* Professors' 2015 Letter, *supra* note 59; Professors' 2014 Letter, *supra* note 59. *See generally* Chow, *supra* note 12; Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, *supra* note 12; Levine & Sandeen, *supra* note 12; Seaman, *supra* note 12.

[61] *See* Professors' 2015 Letter, *supra* note 59, at 2 (emphasis omitted).

[62] Levine & Sandeen, *supra* note 12, at 240–41.

[63] *See* Sandeen & Seaman, *supra* note 9, at 849–51 (explaining the process that led to the modification of the ex parte seizure requirements).

In May 2016, the DTSA became law.[64] The DTSA allows trade secret owners to bring a civil action in federal court for trade secret misappropriation.[65] Structurally, the DTSA is similar in many respects to the UTSA, including the requirements for establishing the existence of a trade secret, an improper act, and use and/or disclosure of the trade secret.[66] Indeed, the law's sponsors argued that the DTSA was not intended to "alter the balance of current trade secret law or alter specific court decisions."[67] However, there are several significant differences between the DTSA and state law, including an ex parte seizure remedy[68] and limited protections for whistleblowers.[69] In addition, the DTSA confers original but not exclusive jurisdiction to federal courts;[70] thus, state courts can also hear claims under the DTSA.[71]

Notwithstanding these changes, the concern about the ex parte seizure provision remains, as the concern is the chilling effect of receiving a letter containing such a threat. *See* Levine & Sandeen, *supra* note 12, at 255 ("Even if the [DTSA] include[s] heightened requirements in order to obtain a seizure order, the courts may never get the chance to adjudicate the issue. Rather, the adjudication may happen in the marketplace, where the recipient of a trade secret troll's letter (which would threaten a seizure action) will have to decide if it has the capacity and resources to challenge the claim in court. If it does not—which would be the case for many potential recipients of such letters, from start-ups to struggling companies—the practical impact could be a settlement payment and, potentially, the end of the business.").

[64] *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C.A. §§ 1832–1833, 1385–1836, 1838–1839, 1961 (West 2018)).

[65] Goldman, *supra* note 2 (stating that the DTSA "gives trade secret owners a new and powerful option to bring trade secret lawsuits using federal law, whereas before only state law authorized their lawsuits").

[66] 18 U.S.C.A. §§ 1836(b)(2), 1839(3)–(5); *see also* Sandeen & Seaman, *supra* note 9, at 857 ("Since the DTSA is modeled after the UTSA, incorporating several of its provisions verbatim, some appear to assume that the two will be interpreted and applied consistently."); Mark Ridgway & Taly Dvorkis, *A Comparison of the EU Trade Secrets Directive and the US Defend Trade Secrets Act*, PATENTLY-O (May 16, 2016), https://patentlyo.com/patent/2016/05/comparison-secrets-directive.html ("[T]o be considered a trade secret the information must be kept confidential and derive an economic value from the fact that it is confidential.").

[67] S. REP. NO. 114-220, at 10 (2016).

[68] 18 U.S.C.A. § 1836(b)(2).

[69] *Id.* § 1833(b); *see also* Sandeen & Seaman, *supra* note 9, at 852 ("In addition, Senators Charles Grassley (Iowa) and Patrick Leahy (Vermont) offered a new amendment intended to 'provide protection to whistleblowers who disclose trade secrets to law enforcement in confidence for the purpose of reporting or investigating a suspected violation of law.'").

[70] 18 U.S.C.A. § 1836(c).

[71] Of course, if a trade secret owner asserts a DTSA claim in state court, the defendants may remove the case to federal court. *See* 28 U.S.C. §§ 1441, 1446 (2012). There are other wrinkles to the DTSA, as well as practice variances, which are beyond the scope of this Article. For example, one North Carolina law firm explained that trade secret plaintiffs may prefer to utilize North Carolina trade secret law instead of the DTSA because awardable damages may be greater under North Carolina law. *See* Brian L. Church, *Congress Enacts the Defend*

In sum, the DTSA has been described as a "wake-up call" to companies that value and protect their IP as trade secrets.[72] As a result, one can reasonably expect that the DTSA will continue to be utilized by trade secret plaintiffs and interpreted by both federal and state courts. However, the details of the DTSA's early use, as described in Part IV, indicate that the DTSA may not be achieving as much as was predicted by its sponsors, particularly with respect to cyberespionage by foreign actors, and suggest trends that may not have been predicted prior to the DTSA's enactment.

C. Empirical Research regarding Trade Secrecy

As previously mentioned, trade secret law operates in a relative empirical information vacuum. While other IP law doctrines like copyright and patent have benefitted from an active and growing body of both theoretical and empirical work upon which to understand their parameters,[73] trade secrecy remains understudied.[74] In particular, despite being a heavily litigated area of IP law,[75] trade secrecy has received very little attention from empirical scholars.[76]

Trade Secrets Act: Time to Revisit Employment Agreements and Protection of Confidential Information, ROBINSON BRADSHAW (June 28, 2016), http://www.robinsonbradshaw.com/newsroom-publications-375.html ("[F]or the time being, the DTSA may not have much effect in steering traditional state law cases into the federal forum. For one, North Carolina law provides for treble damages for trade secret misappropriation, while the DTSA provides only for double damages on a showing of willful and malicious misappropriation.").

[72] Manny Schecter, *The Changing Trade Secret and Patent Equilibrium*, TECHCRUNCH (June 20, 2016), https://techcrunch.com/2016/06/20/the-changing-trade-secret-and-patent-equilibrium.

[73] Examples of recent patent and copyright scholarship include Colleen V. Chien & Mark A. Lemley, *Patent Holdup, the ITC, and the Public Interest*, 98 CORNELL L. REV. 1 (2012); Mark A. Lemley et al., *Life After* Bilski, 63 STAN. L. REV. 1315 (2011); Neil Weinstock Netanel, *Making Sense of Fair Use*, 15 LEWIS & CLARK L. REV. 715 (2011); Aaron Perzanowski & Jason Schultz, *Digital Exhaustion*, 58 UCLA L. REV. 889 (2011); Ted Sichelman, *Commercializing Patents*, 62 STAN. L. REV. 341 (2010); and Rebecca Tushnet, *Worth a Thousand Words: The Images of Copyright*, 125 HARV. L. REV. 684 (2012).

[74] For the most cited trade secret law review articles, which is a significantly shorter list than comparable lists for copyright, patents, and trademarks, see Ted Sichelman, *Most-Cited IP Law Articles Published in the Last 10 Years*, WRITTEN DESCRIPTION (Mar. 23, 2016), http://writtendescription.blogspot.com/2016/03/most-cited-ip-law-articles-published-in.html.

[75] Almeling et al., *supra* note 23, at 293 ("[T]rade secret cases doubled in the seven years from 1988 to 1995, and doubled again in the nine years from 1995 to 2004. At the projected rate, trade secret cases will double again by 2017."). For an argument that trade secrets can be justified as a form of IP, as opposed to traditional property, see generally Lemley, *supra* note 29.

[76] *See* Risch, *supra* note 7 ("[T]he reality is that we know very little about trade secrets, despite the best efforts of a handful of scholars conducting research in this area."). *See generally* Levine & Sichelman, *supra* note 7.

There are few major empirical studies of trade secret law or litigation involving trade secrets, and most are dated.[77] Similarly, while there has been some excellent theoretical and policy analysis regarding trade secret law and its role in innovation policy,[78] many more scholars focus on copyright, patent, and trademark law.[79]

Among the reasons for trade secrecy's scant treatment by scholars are its aforementioned state law status[80] and the general reticence of companies to disclose their trade secret practices and misappropriations.[81] Additionally, as trade secrecy often fills in the gaps between other forms of IP protection[82] and has no registration requirement with a governmental body,[83] it is a challenging area for empirical study. For example, because trade secrecy overlaps heavily with employment law in areas like covenants not to compete and the inevitable disclosure doctrine,[84] crafting empirical trade secret studies that would not be subsumed in contract and employment law concepts requires careful tailoring and analysis.

[77] *See, e.g.*, Almeling et al., *supra* note 23; Almeling et al., *supra* note 25; Richard C. Levin et al., *Appropriating the Returns from Industrial Research and Development*, 3 BROOKINGS PAPERS ECON. ACTIVITY 783 (1987); Wesley M. Cohen et al., *Protecting Their Intellectual Assets: Appropriability Conditions and Why U.S. Manufacturing Firms Patent (or Not)* (Nat'l Bureau of Econ. Research, Working Paper No. 7552, 2000), http://www.nber.org/papers/w7552.pdf; Bronwyn H. Hall et al., *The Choice Between Formal and Informal Intellectual Property: A Literature Review* (Nat'l Bureau of Econ. Research, Working Paper No. 17983, 2012), http://www.nber.org/papers/w17983; Joshua Lerner, Using Litigation to Understand Trade Secrets: A Preliminary Exploration (Aug. 7, 2006) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=922520. For more recent empirical work on trade secrecy, see, for example, NATHAN WAJSMAN & FRANCISCO GARCIA-VALERO, EU INTELLECTUAL PROP. OFFICE, PROTECTING INNOVATION THROUGH TRADE SECRETS AND PATENTS: DETERMINANTS FOR EUROPEAN UNION FIRMS (2017), https://euipo.europa.eu/tunnelweb/secure/webdav/guest/document_library/observatory/documents/reports/Trade%20Secrets%20Report_en.pdf; Levine & Sichelman, *supra* note 7.

[78] *See, e.g.*, Bone, *supra* note 29; Lemley, *supra* note 29; Levine, *supra* note 20; Risch, *supra* note 29; Sharon K. Sandeen, Kewanee *Revisited: Returning to First Principles of Intellectual Property Law to Determine the Issue of Federal Preemption*, 12 MARQ. INTELL. PROP. L. REV. 299 (2008); *see also* Robert G. Bone, *The (Still) Shaky Foundations of Trade Secret Law*, 92 TEX. L. REV. 1803 (2014) (responding to Professor Lemley's article).

[79] *See* Sichelman, *supra* note 74 (listing the most-cited scholars in these doctrines).

[80] *See supra* Subpart II.A.

[81] *See generally* Levine & Sichelman, *supra* note 7.

[82] *See id.*

[83] *See* Robert Klinck, *Keeping Your Trade Secrets Secret*, KLINCK LLC, https://www.klincklc.com/trade-secrets/keeping-trade-secrets-secret (last visited Apr. 10, 2018) ("Because trade secrets do not require registration or any kind of application, they are arguably an inexpensive form of intellectual property.").

[84] *See* Sandeen, *supra* note 12, at 320 ("The remedies provision of the DTSA contains language that, at once, might be interrupted to both endorse and reject the doctrine of inevitable disclosure.").

Existing empirical studies, although limited, have indicated some basic trends that are worth noting in the context of understanding the DTSA's impact. The ability of companies to acquire knowledge and employees, and therefore become "disruptors" in the market sense of the word, is directly related to their willingness to employ and deploy trade secrecy.[85] To the extent that a company is engaged in businesses where reverse engineering is a primary concern, like pharmaceuticals, the prevalence of trade secrecy diminishes.[86] Additionally, it is difficult to market the existence of valuable trade secrets within a firm to its investors. Thus, some studies theorize that companies use trade secrecy primarily in the initial research and development ("R&D") phase and later move toward patenting as a way to publicly disclose their potential for success to investors.[87] At the same time, other studies find that small- and medium-sized entities are less likely to use patents and prefer secrecy due to the cost of patenting and the desire to be first to market.[88] Particularly where a company perceives that it has a strong advantage in R&D over competitors, it may prefer trade secrecy to maintain that advantage.[89]

[85] *See* Marcus Holgersson, *Patent Management in Entrepreneurial SMEs: A Literature Review and an Empirical Study of Innovation Appropriation, Patent Propensity, and Motives*, 43 R&D MGMT. 21, 33 (2013) ("[P]atents can be used as an internal governance tool . . . safeguarding . . . the knowledge and intellectual capital of the investment object, often centered among a few single individuals.").

[86] *See* Alexandra K. Zaby, *Losing the Lead: The Patenting Decision in the Light of the Disclosure Requirement*, 19 ECON. INNOVATION & NEW TECH. 147, 159–60 (2010) ("In an industry sector with a high propensity to patent, such as [p]harmaceuticals[,] the easiness of reverse engineering is rather high so that the effective headstart of an inventor is low." (emphasis omitted)).

[87] *See* Levine & Sichelman, *supra* note 7 (manuscript at 9) ("Thus, keeping information secret in the R&D stage is a particularly strong reason for startups to use trade secrecy, especially if the trade secret is the firm's sole asset." (emphasis omitted)); *see also* R. Mark Halligan, *Trade Secrets v. Patents: The New Calculus*, LANDSLIDE, July/Aug. 2010, at 10, 11 ("The birth of every patent starts out as a trade secret. At the time of conception, the idea or information can only be protected by keeping it secret. However, a subsequent decision needs to be made to determine whether or not to convert the trade secrets . . . into a patent . . . .").

[88] *See* Anthony Arundel, *The Relative Effectiveness of Patents and Secrecy for Appropriation*, 30 RES. POL'Y 611, 615 fig.1 (2001) (surveying 2,849 R&D-performing firms and finding that lead-time advantage is far more important than patents).

[89] *See* Pia Hurmelinna-Laukkanen & Kaisu Puumalainen, *Nature and Dynamics of Appropriability: Strategies for Appropriating Returns on Innovation*, 37 R&D MGMT. 95, 106 (2007) (finding a positive relationship between seeking short-term value, the use of lead time, and secrecy).

III. Methodology

This Part describes the methodology employed by the authors to empirically analyze the first year of litigation under the DTSA. It first summarizes the objective of our empirical study. Next, it explains the study design, including the process used for identifying relevant cases and collecting and coding data regarding these cases. Finally, it notes some potential limitations of the study and its methodology.

A. Objectives

The principal objective of this study is to provide a detailed empirical assessment of trade secret litigation in federal court under the DTSA. Through this examination, it attempts to better understand how litigants are employing this new law to pursue judicial relief for alleged trade secret misappropriation.

In particular, this study seeks to empirically evaluate several claims about the need for the DTSA and whether it is achieving the goals of its sponsors at this early stage. For example, the DTSA's proponents frequently pointed to the problem of theft of trade secrets stored in a digital format, such as by hacking into computer systems.[90] They also focused heavily on the peril of trade secret misappropriation allegedly committed by foreign actors and entities, especially from China.[91] In addition, they stressed the need for stronger civil remedies to prevent the disclosure and dissemination of trade secrets, most notably expedited judicial relief via the ex parte seizure of property containing trade secret information.[92] The

[90] *See* H.R. Rep. No. 114-529, at 3 (2016) ("Trade secrets are an integral part of a company's competitive advantage in today's economy, and with the increased digitization of critical data and increased global trade, this information is highly susceptible to theft."); S. Rep. No. 114-220, at 2 (2016) ("Protecting trade secrets has become increasingly difficult given ever-evolving technological advancements. Thieves are using increasingly sophisticated methods to steal trade secrets and the growing use of technology and cyberspace has made trade secret theft detection particularly difficult."); 162 Cong. Rec. S1626 (daily ed. Apr. 4, 2016) (statement of Sen. Klobuchar) ("Thumb drives and the cloud have replaced filing cabinets for storage [of] information, making stealing a trade secret as easy as clicking a button or touching a screen.").

[91] *See* H.R. Rep. No. 114-529, at 4 (recognizing the "significant and growing threat presented by criminals who engage in espionage on behalf of foreign adversaries and competitors" (quoting H.R. Rep. No. 12-610, at 1 (2012))); 162 Cong. Rec. S7251 (daily ed. Oct. 8, 2015) (statement of Sen. Coons) ("There is no doubt that China and other foreign competitors are working furiously to steal American innovation . . . . That is why Congress must act now to pass the . . . Defend Trade Secrets Act.").

[92] *See* S. Rep. No. 114-220, at 3 ("[The DTSA] also provides for expedited relief on an ex parte basis in the form of a seizure of property from the party accused of misappropriation, a remedy available under extraordinary circumstances where necessary to preserve evidence or prevent dissemination of a trade secret. The ex parte seizure provision is an important remedy for trade

frequency of claims involving cyberespionage, cases against foreign defendants, and ex parte seizure orders in DTSA litigation can help assess whether these goals have been met.

B. Study Design and Data Collection

An original dataset of DTSA claims was created for this study.[93] We sought to identify all federal court cases where a claim of trade secret misappropriation under the DTSA was made in the first year following the law's passage (i.e., from May 11, 2016, until May 11, 2017).[94] This was a time-intensive process, as no comprehensive database of DTSA cases is publicly available. In addition, Public Access to Court Electronic Records ("PACER"), the federal courts' online docketing system, does not specifically identify cases as involving a DTSA claim, unlike suits filed under patent, copyright, or trademark law.[95]

As a result, we conducted searches in several commercial legal databases to help identify relevant DTSA cases. The primary resource used was Bloomberg Law.[96] For our purposes, Bloomberg Law is markedly superior to PACER.[97] First, it allows full-text searches of entire court dockets, whereas PACER is limited to certain types of queries (such as party names, case numbers, and nature of

secret owners . . . ."); *see also supra* notes 60–63 (further explaining the ex parte seizure provisions of the DTSA).

[93] The data collected for this study will be made publicly available at the following website upon publication: DTSA LITIGATION, http://www.dtsalitigation.com (last visited Apr. 21, 2018). *See* Robin Feldman et al., *Open Letter on Ethical Norms in Intellectual Property Scholarship*, 29 HARV. J.L. & TECH. 339, 348 (2016) (recommending that "data needed to replicate the results in a published empirical paper should be made accessible to other academics at the time the paper is published"); *see also* Gregory Mitchell, *Empirical Legal Scholarship as Scientific Dialogue*, 83 N.C. L. REV. 167, 176 (2004) (recommending that law reviews require disclosure of "raw data for replication and review" for empirical legal scholarship).

[94] As described below, most of these cases involved a DTSA claim made by a plaintiff, but a few involved a counterclaim or third-party claim made by a defendant. *See infra* text accompanying note 195.

[95] This is done through an NOS code selected by attorneys on a Civil Cover Sheet at the time of the case's filing. *See, e.g.*, FORM JS 44, CIVIL COVER SHEET (June 2017), http://www.uscourts.gov/sites/default/files/js_044_1.pdf. Empirical scholars who study litigation for various areas of the law (e.g., employment, criminal, and patent) commonly use NOS codes to identify relevant cases. *See* Christina L. Boyd & David A. Hoffman, *The Use and Reliability of Federal Nature of Suit Codes*, MICH. ST. L. REV. (forthcoming) (manuscript at 4–7), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3000386.

[96] *Dockets*, BLOOMBERG LAW, https://www.bloomberglaw.com/dockets (last visited Apr. 10, 2018).

[97] *See* Mindy Kent, *Records, Briefs & Court Filings*, HARV. L. SCH. LIBR., http://guides.library.harvard.edu/recordsandbriefs (last updated Mar. 29, 2018) ("BloombergLaw is your best starting point for access to electronically available federal and state case filings.").

suit ("NOS") codes). Second, Bloomberg Law permits simultaneous searches of all federal district courts, while PACER requires separate searches for each court. Third, and perhaps most importantly, the full text of pleadings and other court documents for many cases is searchable in Bloomberg Law, unlike in PACER.[98] Using broad search criteria,[99] we reviewed all results generated by Bloomberg Law and identified 473 cases that raised a DTSA claim. We also searched databases of district court opinions in WestlawNext[100] and Lexis Advance[101] to identify an additional 13 cases that raised a DTSA claim. In total, our dataset comprises 486 federal cases.

Next, each case in the dataset was hand coded for a variety of information using a standardized set of coding instructions, which was a time-intensive process.[102] The coded variables fall into several categories.[103] We first coded for basic case information, including the names of the plaintiff[104] and defendant,[105] the date that the pleading asserting the DTSA claim was filed,[106] the district court where the

[98] KENT C. OLSON, PRINCIPLES OF LEGAL RESEARCH 300 (2d ed. 2015) ("The full text of documents that have been downloaded through Bloomberg are searchable, making it easy to search for particular motions or arguments.").

[99] *Dockets*, *supra* note 96. In Bloomberg Law, we searched all U.S. district court dockets for the date range of 05/11/2016 to 05/11/2017 using the following terms: "defend trade secrets act" OR DTSA OR (18 w/5 "U.S.C." w/5 (1831! or 1832! or 1833! or 1834! or 1835! or 1836! or 1837! or 1838! or 1839!)).

[100] WESTLAWNEXT, https://next.westlaw.com/ (last visited Apr. 10, 2018). In WestlawNext, we searched all federal district court decisions since May 11, 2016, using the following terms: "defend trade secrets act" OR DTSA or (18 /5 u.s.c. /5 (1831! or 1832! or 1833! or 1834! or 1835! or 1836! or 1837! or 1838! or 1839!)).

[101] LEXIS ADVANCE, https://advance.lexis.com/ (last visited Mar. 1, 2018). In Lexis Advance, we searched all federal district court decisions since May 11, 2016, using the following terms: "defend trade secrets act" OR (18 /4 u.s.c. /5 1831 1832 1833 1834 1835 1836 1837 1838 1839).

[102] The coding process took several hundred hours of time in the aggregate. *See* Michael Heise, *The Past, Present, and Future of Empirical Legal Scholarship: Judicial Decision Making and the New Empiricism*, 2002 U. ILL. L. REV. 819, 829 (2002) ("Unfortunately, data gathering is frequently labor-intensive and time-consuming and, consequently, often quite expensive." (footnote omitted)).

[103] Variable names are listed in brackets in the following footnotes.

[104] This was coded as a string (text) variable [plaintiff], with the named party abbreviated under *The Bluebook* if appropriate. If multiple plaintiffs existed, only the first named plaintiff was used.

[105] This was coded as a string variable [defendant], with the named party abbreviated under *The Bluebook* if appropriate. If multiple defendants existed, only the first named defendant was used.

[106] This variable [date] was coded in the following format: MM/DD/YYYY. In situations where the DTSA claim was asserted in something other than the original complaint—for example, a case originally filed in federal court before the DTSA's enactment to which the plaintiff subsequently added a DTSA claim in an amended complaint—the date of the amended pleading that added the DTSA claim was used.

case was filed,[107] the case's docket number,[108] the judge initially assigned to the case,[109] and the NOS code.[110]

We then coded for various information typically contained in the plaintiff's complaint (or, in a few cases, in a counterclaim or third-party claim by a defendant that alleged a DTSA violation). Although a complaint contains only allegations, not factual findings or legal conclusions like a court opinion, it nonetheless can be a valuable source of information for empirical research.[111] Under the Federal

[107] This was initially coded as a string variable [court] using a three- or four-letter abbreviation consistent with PACER. For example, the Northern District of California was abbreviated as "CAND." *See CM/ECF Filer or PACER Login*, U.S. DISTRICT CT., N. DISTRICT CAL., https://ecf.cand.uscourts.gov/cgi-bin/login.pl (last visited Apr. 10, 2018). This variable was then encoded into a separate, categorical (numeric) variable [court_n] for purposes of data analysis. Note that both variables only reflect the court where the case was originally filed (or, in a handful of cases, removed to from state court); they do not capture any subsequent transfers to another district pursuant to 28 U.S.C. § 1404 (2012).

[108] This variable [docket] was coded in the following format: N:NN-CV-NNNN (where N is a number).

[109] This was coded as a string variable [judge].

[110] This variable [nos] was coded as a three-digit number. *See* ADMIN. OFFICE OF THE U.S. COURTS, NATURE OF SUIT (n.d.), https://www.pacer.gov/documents/natsuit.pdf; *see also supra* note 95 and accompanying text (explaining NOS codes).

[111] For other empirical studies that use complaints as a data source, see, for example, Christina L. Boyd et al., *Building a Taxonomy of Litigation: Clusters of Causes of Action in Federal Complaints*, 10 J. EMPIRICAL LEGAL STUD. 253 (2013) (examining the breadth of pleading and the interrelationship among causes of action in civil complaints); Jason A. Cantone et al., *Whither Notice Pleading? Pleading Practice in the Days Before* Twombly, 39 S. ILL. U. L.J. 23 (2014) (studying pleading practice in federal courts prior to *Twombly*); Theodore Eisenberg, *Section 1983: Doctrinal Foundations and an Empirical Study*, 67 CORNELL L. REV. 482 (1982) (examining the contents of complaints in civil rights cases); Kimberly A. Moore, *Empirical Statistics on Willful Patent Infringement*, 14 FED. CIR. B.J. 227 (2004) (studying allegations of willful infringement in patent complaints); A.C. Pritchard & Hillary A. Sale, *What Counts as Fraud? An Empirical Study of Motions to Dismiss Under the Private Securities Litigation Reform Act*, 2 J. EMPIRICAL LEGAL STUD. 125, 142 (2005) (empirically analyzing complaints under federal securities litigation statutes); Alexander A. Reinert, *The Costs of Heightened Pleading*, 86 IND. L.J. 119 (2011) (examining the connection between merits and pleadings by providing empirical data from appellate and trial court pleadings and decisions in order to "question the widespread assumptions about the costs and benefits of heightened pleading"); Margo Schlanger, *Inmate Litigation*, 116 HARV. L. REV. 1555 (2003) (examining the content of complaints in prisoner civil rights litigation); William Bennett Turner, *When Prisoners Sue: A Study of Prisoner Section 1983 Suits in the Federal Courts*, 92 HARV. L. REV. 610 (1979) (examining the content of complaints in prisoner civil rights litigation); Colleen McNamara, Note, Iqbal *as Judicial Rorschach Test: An Empirical study of District Court Interpretations of* Ashcroft v. Iqbal, 105 NW. U. L. REV. 401 (2011) (analyzing 10% of the federal district court complaints and subsequent decisions that cited *Iqbal* in order to determine whether the United States Supreme Court's decision in *Iqbal* created a workable pleading standard that is applicable uniformly across the federal circuits;

Rules of Civil Procedure, a complaint is required to provide "a short and plain statement of the claim showing that the pleader is entitled to relief" as well as "the grounds for the court's jurisdiction."[112] In addition, under the Supreme Court's decisions in *Bell Atlantic Corp. v. Twombly*[113] and *Ashcroft v. Iqbal*,[114] a plaintiff must plead sufficient facts to demonstrate that the asserted claims are plausible.[115]

In trade secret cases, this means the complaint must include enough factual detail that, if true, would plausibly satisfy several prerequisites for relief under the DTSA, including the existence of a trade secret,[116] ownership by the plaintiff(s),[117] use of the trade secret in connection with interstate or foreign commerce,[118] and misappropriation by the defendant(s).[119] For instance, "the plaintiff cannot simply state that a trade secret [is] involved."[120] Rather, the complaint must include sufficient information about the alleged trade secret—including whether it has "independent economic value" and whether the owner took sufficient steps to protect its alleged

specifically analyzing courts' interpretations of the "factual sufficiency" of a complaint as well as their subsequent analysis of said complaint).

[112] FED. R. CIV. P. 8(a).

[113] 550 U.S. 544 (2007).

[114] 556 U.S. 662 (2009).

[115] *See id.* at 678 ("To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." (quoting *Twombly*, 550 U.S. at 570)).

[116] *See* 18 U.S.C.A. § 1839(3) (West 2018) (defining the term "trade secret," including the requirement that the trade secret has "independent economic value, actual or potential, from not being generally known to, and not readily ascertainable by proper means by, another person," and that the trade secret owner "has taken reasonable precautions to keep such information secret").

[117] *See id.* § 1836(b)(1) (authorizing "[a]n owner of a trade secret that is misappropriated" to bring a "civil action"); *see also id.* § 1839(4) (defining the "owner" of a trade secret as one who has "legal or equitable title in, or license to, the trade secret").

[118] *See id.* § 1836(b)(1) (requiring that "the trade secret [be] related to a product or service used in, or intended for use in, interstate or foreign commerce").

[119] *See id.* § 1839(5) (defining misappropriation of a trade secret); *see also id.* § 1839(6) (defining "improper means" for acquiring a trade secret).

[120] Evans, *supra* note 12, at 191.

secret[121]—to make the claim viable.[122] Similarly, the complaint must plausibly plead that the defendant committed an act of misappropriation by improperly acquiring, disclosing, or using the alleged trade secret.[123] This can be established, for example, by alleging that the defendant breached a nondisclosure agreement ("NDA")[124] or that he or she downloaded the alleged trade secret information onto a flash drive in violation of company policy for subsequent use in a new job.[125] Finally, above and beyond what is mandated by the pleading requirements, trade secret plaintiffs may elect to include more detailed allegations about the nature of their valuable trade secret information and the defendant's nefarious

[121] *See id.* at 193–94 ("The specific sub-elements to the DTSA trade secret definition require that the trade secret information (1) have independent economic value, actual or potential; (2) not be generally known to another person who would benefit from it; (3) not be readily ascertainable through proper means; and (4) be the subject of reasonable measures to maintain secrecy."); *see also* M.C. Dean, Inc. v. City of Miami Beach, 199 F. Supp. 3d 1349, 1357 (S.D. Fla. 2016) (dismissing the plaintiff's DTSA claim because it "fail[ed] to allege it took reasonable steps to protect the secrecy of the information at issue, thus failing to satisfy the definition of trade secret").

[122] *See, e.g.*, AutoTrakk, LLC v. Auto. Leasing Specialists, Inc., No. 4:16-CV-01981, 2017 WL 2936730, at *6 (M.D. Pa. July 10, 2017) (dismissing the plaintiff's DTSA claim without prejudice because it "pleads insufficient factual material to determine whether . . . a trade secret plausibly existed"); Molon Motor & Coil Corp. v. Nidec Motor Corp., No. 16 C 03545, 2017 WL 1954531, at *4 (N.D. Ill. May 11, 2017) (explaining that the complaint "require[s] some concreteness and specificity" about the trade secrets allegedly misappropriated under the DTSA); *see also* Am. Registry, LLC v. Hanaw, No. 2:13-cv-352-FtM-29UAM, 2013 U.S. Dist. LEXIS 171889, at *9 (M.D. Fla. Dec. 5, 2013) (deeming "broad and generic categories of information" insufficient to provide "notice as to the actual trade secrets misappropriated" in a state law trade secrets case). However, the trade secret "need not be disclosed in [such] detail in a complaint" that it "would result in the public disclosure of the purported trade secret[]." Mission Measurement Corp. v. Blackbaud, Inc., 216 F. Supp. 3d 915, 921 (N.D. Ill. 2016) (quoting AutoMed Techs., Inc. v. Eller, 160 F. Supp. 2d 915, 921 (N.D. Ill. 2001)); *see also* Priority Assist, Inc., v. Stockard & Assocs., No. 4:15-CV-02970, 2016 WL 4479529, at *5 (S.D. Tex. Aug. 24, 2016) (finding that the plaintiffs "specified what is plausibly a trade secret" by identifying broad categories of information, such as "business information, customer lists and agreements, and market share data," allegedly misappropriated by the defendant).

[123] *See* 18 U.S.C.A. § 1839(5) (defining misappropriation of a trade secret); *see also* GeometWatch Corp. v. Hall, No. 1:14-CV-00060-JNP-PMW, 2017 WL 1136946, at *9 (D. Utah Mar. 27, 2017) (dismissing the plaintiff's complaint because it "failed to offer non-conclusory fact-based allegations that support even an inference that any [defendant] improperly used or disclosed [plaintiff]'s trade secrets").

[124] *See, e.g.*, Melville Capital, LLC v. Tenn. Commerce Bank, No. 3:11-CV-00888, 2011 WL 6888476, at *6 (M.D. Tenn. Dec. 29, 2011).

[125] *See, e.g.*, *Molon Motor & Coil Corp.*, 2017 WL 1954531, at *4–5.

conduct to begin persuading the judge regarding the merits of their claim or to induce a favorable pretrial settlement.[126]

We coded the following variables for each complaint. First, we coded the basis for the court's jurisdiction, as asserted by the plaintiff. This included both federal question jurisdiction[127] (which is applicable for all complaints raising a DTSA claim) as well as diversity jurisdiction.[128] We also coded for assertions of supplemental jurisdiction over related state law claims.[129] In addition, we coded for cases where a DTSA claim was originally filed in state court and subsequently removed by the defendant to federal court[130] as well as for cases where the DTSA claim was asserted by a nominal defendant in a counterclaim.[131]

Next, we coded complaints for all other (non-DTSA) causes of action. For federal law,[132] this included claims arising under the Computer Fraud and Abuse Act ("CFAA");[133] patent law;[134] copyright law;[135] the Lanham Act;[136] federal antitrust law;[137] the Racketeer

[126] *See* Elizabeth Fajans & Mary R. Falk, *Untold Stories: Restoring Narrative to Pleading Practice*, 15 J. LEGAL WRITING INST. 3, 11–12, 40–44 (2009) (describing complaints as "tool[s] of tactical advantage" in litigation and asserting that sufficient detail should be included in them to convey the plaintiff's narrative); Anne E. Ralph, *Not the Same Old Story: Using Narrative Theory to Understand and Overcome the Plausibility Pleading Standard*, 26 YALE J.L. & HUMAN. 1, 33 (2014) ("Specific factual detail, whether an individual detail or a multitude of elaborate detail, can have very effective persuasive power."); Koan Mercer, Comment, *"Even in These Days of Notice Pleadings": Factual Pleading Requirements in the Fourth Circuit*, 82 N.C. L. REV. 1167, 1194 n.140 (2004) ("Laying out a factually detailed and persuasive case in the complaint may also serve a negotiation posturing function.").

[127] *See* 28 U.S.C. § 1331 (2012). This was coded as a binary variable [jur_fq].

[128] *See id.* § 1332. This was coded as a binary variable [jur_div]. Numerous cases pleaded diversity jurisdiction as well as federal question jurisdiction.

[129] *See id.* § 1367. This was coded as a binary variable [jur_supp].

[130] *See id.* §§ 1441, 1446. This was coded as a binary variable [remove].

[131] FED. R. CIV. P. 13(a)–(b). This was coded as a binary variable [counterclaim].

[132] All federal law causes of action were initially coded as categorical variables [fedlaw1 to fedlaw3]. From this data, the authors created binary (dummy) variables for the most common causes of action for purposes of data analysis. *See infra* notes 133–39.

[133] 18 U.S.C. § 1030 (2012). This was coded as a binary variable [cfaa].

[134] 35 U.S.C. § 101 (2012). This was coded as a binary variable [patent].

[135] 17 U.S.C. § 101 (2012). This was coded as a binary variable [copyright]. Claims under the Digital Millennium Copyright Act, 17 U.S.C. §§ 1201–1205 (2012), were classified as copyright claims.

[136] 15 U.S.C. §§ 1114, 1125 (2012). This was coded as a binary variable [lanham]. Claims coded as arising under the Lanham Act included trademark infringement (for both registered and unregistered markets), unfair competition, false advertising, false designation of origin, and cybersquatting under the Anticybersquatting Consumer Protection Act, 15 U.S.C. § 1125(d) (2012).

[137] This was coded as a binary variable [antitrust]. This included claims under the Sherman Act, the Clayton Act, and the Federal Trade Commission Act.

Influenced and Corrupt Organizations Act ("RICO");[138] and any other federal law claims that did not fall into one of these categories.[139] Numerous state law claims were coded as well,[140] as the DTSA expressly declined to preempt other causes of action.[141] Specifically, we coded for claims of trade secret misappropriation under state law;[142] breach of contract (including breach of nondisclosure and/or noncompete agreements);[143] breach of the implied covenant (or duty) of good faith and fair dealing;[144] breach of fiduciary duty;[145] unfair competition;[146] conversion;[147] tortious interference with contractual

See Sherman Act, 15 U.S.C. §§ 1–7 (2012) (declaring illegal "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations . . ."); Clayton Act, 15 U.S.C. §§ 12–27, 29 U.S.C. §§ 52–53 (2012) (declaring it unlawful for any person engaged in commerce to discriminate on the basis of price, services, or facilities); Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2012) (empowering the FTC to prevent unfair methods of competition and unfair or deceptive acts in or affecting commerce).

[138] Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961–1968 (2012). The DTSA made trade secret misappropriation a predicate offense for a RICO claim. Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 3(b), 130 Stat. 376, 382 (codified at 18 U.S.C.A. § 1961(1) (West 2018)).

[139] This was coded as a binary variable [otherfed], and a text field was included to describe the claim [otherfednotes].

[140] Like federal law claims, state law causes of action were initially coded as categorical variables [statelaw1 to statelaw9]. From this data, the authors created binary (dummy) variables for the most common causes of action for purposes of data analysis. *See infra* notes 142–53.

[141] *See* 18 U.S.C.A. § 1838 (West 2018) ("Except as provided in section 1833(b) [the whistleblower provision], this chapter shall not be construed to preempt or displace any other remedies, whether civil or criminal, provided by United States Federal, State, commonwealth, possession, or territory law for the misappropriation of a trade secret . . . ."); *see also* Defend Trade Secret Act of 2016, § 2(f), 130 Stat. at 382 ("Nothing in the amendments made by this section shall be construed to modify the rule of construction under section 1838 of title 18, United States Code, or to preempt any other provision of law."). In contrast, the UTSA "displaces conflicting tort, restitutionary, and other law . . . providing civil liability remedies for misappropriation of a trade secret," except for contractual and criminal remedies. UNIF. TRADE SECRETS ACT § 7 (UNIF. LAW COMM'N 1985).

[142] This was coded as a binary variable [statets].

[143] This was coded as a binary variable [contract].

[144] This was coded as a binary variable [goodfaith].

[145] This was coded as a binary variable [duty].

[146] This was coded as a binary variable [unfaircomp]. We classified claims of unfair or deceptive trade practices under state law as a form of unfair competition.

[147] This was coded as a binary variable [conversion].

or business relations;[148] unjust enrichment;[149] fraud;[150] state law computer crime or tort;[151] and civil conspiracy.[152] We also included a catch-all category to cover other state law claims that did not fall into one of these categories.[153]

In addition, we coded all complaints for the type(s) of trade secret information allegedly misappropriated.[154] The DTSA defines "trade secret" expansively as "all forms and types of financial, business, scientific, technical, economic and engineering information," including formulas, methods, processes, and programs that "derive[] independent economic value, actual or potential, from not being generally known, and not being readily ascertainable through proper means . . . by another person who can obtain economic value . . . from the information."[155] Specifically, we coded for technical or scientific information;[156] financial information;[157] marketing information;[158]

[148] This was coded as a binary variable [interfere]. This general category of tort encompasses various claims, including tortious interference with contractual rights, intentional interference with contractual relations, inducement of breach of contract, tortious interference with business relations, and intentional interference with prospective economic advantage.

[149] This was coded as a binary variable [unjustenrich].

[150] This was coded as a binary variable [fraud]. This variable encompassed various fraud-related claims, including fraudulent misrepresentation and fraudulent inducement.

[151] This was coded as a binary variable [statecomp]. According to the National Conference of State Legislatures, all 50 states have enacted computer crime laws, most of which target unauthorized access to computer systems. Some of these laws also address other types of computer-related con, such as spyware, phishing, denial of service attacks, and ransomware. *See Computer Crime Statutes*, NAT'L CONF. ST. LEGISLATURES (Dec. 5, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx.

[152] This was coded as a binary variable [conspiracy].

[153] This was coded as a binary variable [otherstate], and a text field was included to describe the claim [otherstatenotes]. Purely remedial "claims" without an underlying cause of action, such as injunctive relief, were omitted.

[154] Types of trade secret information allegedly misappropriated were initially coded as categorical variables [secret1 to secret8]. From this data, the authors created binary (dummy) variables for each category of trade secret. *See infra* notes 156–64.

[155] 18 U.S.C.A. § 1839(3)(B) (West 2018). The DTSA also requires the owner of a trade secret to take "reasonable precautions to keep such information secret." *Id.* § 1839(3)(A). The definition of trade secrets in the DTSA is similar but not identical to the UTSA; the latter refers to any "information," while the DTSA only covers particular categories of information—namely, "financial, business, scientific, technical, economic and engineering information." *Compare* UNIF. TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985), *with* 18 U.S.C.A. § 1839(3). As a result, some trade secret scholars (including one coauthor) have argued that the DTSA's definition of "trade secret" may be interpreted less expansively than the UTSA's. *See* Sandeen & Seaman, *supra* note 9, at 904–05.

[156] This was coded as a binary variable [technical].

[157] This was coded as a binary variable [financial].

[158] This was coded as a binary variable [marketing].

internal business or strategic plans;[159] customer lists and other customer-related information;[160] secret formulas;[161] computer software;[162] so-called "negative" trade secrets (i.e., information about what not do, such as unsuccessful research experiments);[163] and a catch-all category for any other information that did not fall into one of these categories.[164]

Several additional variables were coded from allegations contained in the complaints.[165] These included the relationship between the parties, such as whether the defendant was a former employee or business partner of the plaintiff;[166] whether at least one defendant was a citizen of a foreign country;[167] whether the case involved a claim of computer hacking;[168] whether one or more

[159] This was coded as a binary variable [busplan].

[160] This was coded as a binary variable [customer].

[161] This was coded as a binary variable [formula].

[162] This was coded as a binary variable [software]. It included any type of computer software, program, or algorithm.

[163] *See* UNIF. TRADE SECRETS ACT § 1 cmt. (UNIF. LAW COMM'N 1985) (explaining that "trade secret" may include "information that has commercial value from a negative viewpoint, for example, the results of lengthy and expensive research which provides that a certain process will *not* work"); *see also* Charles Tait Graves, *The Law of Negative Knowledge: A Critique*, 15 TEX. INTELL. PROP. L.J. 387, 388 (2007) (criticizing the concept of liability for negative know-how because it "is conceptually unworkable and serves mainly as an anticompetitive threat to employee mobility"). This was coded as a binary variable [negative].

[164] This was coded as a binary variable [othersecret], and a text field was included to describe the type of trade secret at issue [othersecretnotes].

[165] In addition to the other variables identified in this paragraph, we also attempted to code for the type(s) of alleged misappropriation—namely, whether the defendant(s) had improperly acquired [acquire], disclosed [disclose], and/or used [use] the alleged trade secrets without the owner's permission. However, we discovered during the coding process that these variables were unable to provide much useful information because many complaints contained boilerplate asserting all these acts of misappropriation. As a result, although they are included in our dataset, we did not perform any data analysis on these variables.

[166] This was initially coded as categorical variables [relations1 to relations4]. From this data, we created several binary (dummy) variables for purposes of data analysis: (1) cases where at least one defendant was a current or former employee of the plaintiff(s) [employee]; (2) cases where at least one defendant was a current or former business partner of the plaintiff(s) [buspartner]; and (3) cases that did not fall into either of these categories (i.e., where there was no apparent prior relationship between the parties described in the complaint) [otherdefs].

[167] This was coded as a binary variable [foreigndef]. In addition, a text field was included to identify foreign defendants' citizenship [country].

[168] This was coded as a binary variable [hacking]. Specifically, we classified a complaint as involving a hacking claim when the plaintiff(s) asserted that the defendant(s) had engaged in economic espionage or accessed the computer system, network, or server of a plaintiff without authorization. Note that claims of access of a computer system, network, or server merely in excess of authorized access—for example, when a current employee, in violation of company policy,

defendants had entered into an NDA or written confidentiality agreement;[169] and whether one or more defendants had entered into a noncompete agreement.[170]

The final category of information coded pertained to interim relief in DTSA cases. This was of particular interest because of the controversial ex parte seizure remedy contained in the DTSA, which was the subject of considerable debate and amendment during the legislative process.[171] We coded for three types of interim relief that can be awarded in federal court for trade secret cases: temporary restraining orders ("TROs");[172] preliminary injunctions;[173] and ex parte seizures.[174] For each variable, coders reviewed the docket sheet in Bloomberg Law to determine if the alleged trade secret owner(s) requested one or more of these forms of relief and, if so, reviewed the district court's decision on the motion.[175]

Notably, we did not code for outcomes of the DTSA cases in our dataset. This was because there were few merits decisions at the one-year anniversary of the DTSA's enactment, as the vast majority of cases were either still pending or had been dismissed prior to judgment (i.e., they were settled).[176] The subsequent outcomes of

accessed trade secret information on the employer's server or downloaded trade secret information to a personal electronic device—were not considered "hacking" claims.

[169] This was coded as a binary variable [nda].

[170] This was coded as a binary variable [noncompete].

[171] *See* Goldman, *Ex Parte Seizures and the Defend Trade Secrets Act*, *supra* note 12, at 284; Valerie Kahn, *The Defend Trade Secrets Act's Seizure Provisions and What They Mean for Employers*, NAT'L L. REV. (May 24, 2016), https://www.natlawreview.com/article/defend-trade-secrets-act-s-seizure-provisions-and-what-they-mean-employers; *see also* Peter J. Toren, *The Defend Trade Secrets Act*, 28 INTELL. PROP. & TECH. L.J. 3, 3, 6 (2016); James Dowd et al., *Federalizing Trade Secret Protection: A Close Look at the Ex Parte Seizure Provision*, CORP. COUNS. (May 23, 2016), http://www.corpcounsel.com/id=1202758416397; *supra* notes 60–63 and accompanying text (describing opposition to the DTSA's ex parte seizure provision and modifications made to it during the legislative process).

[172] *See* FED. R. CIV. P. 65(b) (authorizing TROs). This was coded as a categorical variable [tro].

[173] *See id.* R. 65(a) (authorizing preliminary injunctions). This was coded as a categorical variable [pi].

[174] *See* 18 U.S.C.A. § 1836(b)(2) (West 2018) (authorizing ex parte seizures). This was coded as a categorical variable [exparte].

[175] If a motion was granted in part and denied in part, it was coded as "granted." If a motion was entirely denied prior to the case's termination, it was coded as "denied." If a motion was still pending at the time of the case's dismissal or the end of data collection, it was coded as "no decision."

[176] The authors are aware of only one jury verdict on a DTSA claim during the law's first year. *See* Jury Verdict, Dalmatia Import Group, Inc. v. Foodmatch, Inc., No. 2:16-CV-02767 (E.D. Pa. Feb. 27, 2017) (awarding the plaintiff $500,000 in damages for its claims under the DTSA and the Pennsylvania Uniform Trade Secrets Act).

these cases can be a topic for future empirical research by trade secret scholars.

C. Limitations

Like all empirical research, the methodology used in this study has limitations that could affect the results and implications discussed in the following Parts.[177] Here, we discuss several potential limitations and our efforts to address them.

The first limitation is that our study involves a review of litigation, which is subject to well-known selection bias. "[T]he disputes selected for litigation . . . will constitute neither a random nor a representative sample . . . of all disputes."[178] One reason is the cost of litigation; "[m]any disputes are resolved before a lawsuit is filed" because it is frequently more cost-effective "to settle than to litigate."[179] Trade secret litigation can be quite expensive; a recent survey of IP attorneys found that the median litigation cost for a trade secret case varied from $400,000 (where less than $1 million was at risk) to over $1.6 million (where more than $25 million was at risk).[180] As a result, parties may select other methods, such as alternative dispute resolution ("ADR"), to resolve their grievances.[181] In addition, ADR—which is private—may be desirable to prevent public disclosure of the alleged trade secrets.[182] Furthermore, many trade secret litigants have a preexisting contractual relationship, such as

[177] *See* Heise, *supra* note 102, at 849 ("Data, research design, and statistical methods frequently enforce limits on what can be properly inferred from the results of empirical studies . . . . Notwithstanding these inherent and structural limitations, empirical methodologies are well-positioned to enhance and complement traditional legal scholarship."). Authors of empirical legal research "should discuss limitations on the validity and generalizability of [their] findings." Mitchell, *supra* note 93, at 201, 203.

[178] George L. Priest & Benjamin Klein, *The Selection of Disputes for Litigation*, 13 J. LEGAL STUD. 1, 4 (1984). The Priest-Klein model is focused on empirical studies of outcomes (win rates) in litigation; they define the term "litigate" narrowly as only disputes where "a verdict is rendered." *Id.* at 4–6. This study, in contrast, looks at all federal court cases involving a DTSA claim.

[179] Robert H. Gertner, *Asymmetric Information, Uncertainty, and Selection Bias in Litigation*, 1993 U. CHI. L. SCH. ROUNDTABLE 75, 75, 79 (1993); *see also* Theodore Eisenberg, *Litigation Models and Trial Outcomes in Civil Rights and Prisoner Cases*, 77 GEO. L.J. 1567, 1571 (1989) ("Both sides can save the costs of litigation by settling [a] dispute.").

[180] AM. INTELLECTUAL PROP. LAW ASS'N, 2017 REPORT OF THE ECONOMIC SURVEY, at I-197, I-201 (2017).

[181] *See generally* Steven Shavell, *Alternative Dispute Resolution: An Economic Analysis*, 24 J. LEGAL STUD. 1 (1995) (examining reasons why parties would choose ADR as opposed to trial).

[182] *See* Scott H. Blackman & Rebecca M. McNeill, *Alternative Dispute Resolution in Commercial Intellectual Property Disputes*, 47 AM. U. L. REV. 1709, 1728 (1998) ("By the very nature of the issues involved, usually at least one party in a trade secret dispute is very concerned about maintaining the secrecy of the trade secret or other confidential or proprietary information.").

an employment agreement or business agreement.[183] If the contract provides for resolution of disputes through mandatory arbitration, these cases also typically will not be litigated.[184]

Second, it is possible that, despite our best efforts,[185] we may have failed to identify some cases that raise DTSA claims during the study period. But by conducting broad searches in multiple sources involving different types of information (docket sheets, court filings, and court decisions), we believe that our methodology has captured the vast majority of relevant cases during the study period.

Third, as previously discussed, complaints—which are the data source for the majority of variables in our study—contain only allegations by an interested party, not findings of fact by a neutral decision maker. As a result, the information contained within these documents is obviously designed to support the plaintiff's theory of the case. While there are constraints to prevent litigants from making frivolous or knowingly false claims in their pleadings, such as the Federal Rules of Civil Procedure[186] and the Model Rules of Professional Conduct,[187] unfavorable aspects of the case may be downplayed or omitted. In addition, complaints may be deliberately

[183] *See* Almeling et al., *supra* note 23, at 302 tbl.2 (finding that over 90% of trade secret disputes decided in federal court from 1950 to 2007 involved either a current or former employee or a business partner of the trade secret owner).

[184] *See* Gertner, *supra* note 179, at 77 ("[I]f disputes can only go to arbitration if both parties agree to arbitration, the mere fact that the parties agree to arbitration may reflect important underlying characteristics of the dispute."); *see also* Aviation All. Ins. Risk Retention Grp., Inc. v. Polaris Enter. Grp., Inc., No. CV 17-35-M-DWM, 2017 WL 2799151, at *4 (D. Mont. June 27, 2017) (granting a motion to compel arbitration of a DTSA claim); T&S Brass & Bronze Works, Inc. v. Slanina, No. CV 6:16-03687-MGL, 2017 WL 1734362, at *4, *7 (D.S.C. May 4, 2017) (compelling arbitration of a DTSA claim). Some arbitration agreements permit the trade secret owner to obtain injunctive relief in court while arbitration is pending. *See* Erin O'Hara O'Connor & Christopher R. Drahozal, *The Essential Role of Courts for Supporting Innovation*, 92 TEX. L. REV. 2177, 2196–97 (2014) (discussing contractual franchise agreements that did not contain an arbitration clause or contained a carve-out from arbitration for "injunctive relief to protect[] . . . trade secrets[] and confidential information").

[185] *See supra* notes 94–101 and accompanying text (explaining the methodology used to identify cases involving DTSA claims).

[186] *See* FED. R. CIV. P. 11(b) ("By presenting to the court a pleading, . . . an attorney or unrepresented party certifies that to the best of the person's knowledge, information, and belief, . . . the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law . . . [and] the factual contentions have evidential support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation . . . .").

[187] *See* MODEL RULES OF PROF'L CONDUCT r. 3.1 (AM. BAR. ASS'N 1983) ("A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis [in law and fact] for doing so that is not frivolous . . . ."); *id.* r. 3.3(a)(1) ("A lawyer shall not knowingly[] make a false statement of material fact or law to a tribunal . . . .").

vague or ambiguous about certain issues, such as the identification of trade secret information, for tactical reasons.[188] Furthermore, a handful of publicly accessible complaints have significant redactions[189] that made it difficult or impossible to code some variables.[190]

In addition, we hand coded many variables in the dataset, which is a potential source of error. For example, if the variables are ambiguous or include room for subjectivity, this could result in inconsistent application and negatively impact reproducibility.[191] However, this concern can be mitigated by creating, pilot testing, and implementing written coding instructions that all coders must follow, as was done in this study.[192] In addition, one of the coauthors personally coded half of the cases in the dataset, and the remaining

[188] *See* Charles Tait Graves & Brian D. Range, *Identification of Trade Secret Claims in Litigation: Solutions for a Ubiquitous Dispute*, 5 NW. J. TECH. & INTELL. PROP. 68, 68 (2006) ("Trade secret plaintiffs rarely provide a precise and complete identification of the alleged trade secrets at issue without a court order requiring them to do so. This is a strategy, not an accident. The tactical advantages a plaintiff gains from non-identification are too tempting for a plaintiff to voluntarily provide such identification.").

[189] *See, e.g.*, Complaint, AptarGroup, Inc. v. Kraft Heinz Foods Co., No. 2:17-CV-00521 (W.D. Pa. filed Apr. 21, 2017) (redacting information regarding the plaintiff's alleged confidential information and prior contractual agreements); Complaint, CrowdStrike, Inc. v. NSS Labs, Inc., No. 1:17-CV-00146-GMS (D. Del. Mar. 21, 2017) (redacting information regarding a nondisclosure agreement between the parties); Complaint, First W. Capital Mgmt. Co. v. Malamed, No. 16-cv-1961-WJM-MJW (D. Colo. filed Sept. 30, 2016) (redacting part or all of fourteen paragraphs regarding the defendant's alleged misappropriation of trade secrets and breach of fiduciary duties and employment agreement); Complaint, Congenra Solar, Inc. v. SolarCity Corp., No. 3:16-CV-05481 (N.D. Cal. filed Sept. 26, 2016) (redacting the identification of alleged trade secrets, actions taken by the plaintiff to protect the alleged secrets from disclosure, and the defendants' alleged acts of misappropriation). A similar issue exists regarding the redaction and nondisclosure of government records regarding trade secret information used in public infrastructure. *See* Levine, *supra* note 20.

[190] When a variable could not be coded due to redactions, a missing value was entered and a comment was placed in a text field [notes].

[191] *See generally* Jason Rantanen, *Empirical Analyses of Judicial Opinions: Methodology, Metrics and the Federal Circuit*, 49 CONN. L. REV. 227 (2016) (exploring the use of multiple studies to form a complete understanding of the Federal Circuit's patent law decisions).

[192] In empirical research, written coding instructions are preferred so that all coders apply the same criteria for each coding decision. This promotes consistency in coding, and it also serves as "a check against looking, consciously or not, for confirmation of predetermined positions." Mark A. Hall & Ronald F. Wright, *Systematic Content Analysis of Judicial Opinions*, 96 CALIF. L. REV. 63, 81 (2008); *see also* Lee Epstein & Andrew Martin, *Coding Variables*, *in* 1 ENCYCLOPEDIA OF SOCIAL MEASUREMENT 321, 325 (Kimberly Kempf-Leonard ed., 2005) (explaining that "the overriding goal of a codebook is to minimize human judgment—to leave as little as possible to interpretation"). The authors' coding instructions are available upon request.

cases were coded by law students who were instructed, trained, and supervised by the authors to ensure accuracy.

IV. RESULTS

This Part summarizes the key findings from the study described in the previous section, primarily through descriptive statistics. It first provides some basic information about the cases filed under the DTSA in the first year following its passage. Next, it summarizes a variety of information contained within DTSA pleadings. Finally, it provides some data on interim relief in DTSA cases, including ex parte seizures, TROs, and preliminary injunctions.

A. Case Information

1. Filings

As previously discussed, we identified 486 federal court cases that raised a DTSA claim during the study period.[193] Of these, 15 (3%) are cases originally filed in state court that were removed to federal court by the defendant(s).[194] In addition, 9 (2%) of these cases involve a DTSA claim raised by a defendant as a counterclaim or third-party claim.[195]

Notably, DTSA claims were not linear over the study period.[196] Figure 1 below shows the number of DTSA claims asserted per month. On average, 35 DTSA claims per month were filed from the DTSA's passage through the end of 2016.[197] In contrast, 50 DTSA claims per month were filed during 2017.[198] Possible explanations for this increase in filings include growing awareness of the DTSA since its passage as well as several court decisions holding that improper

[193] *See supra* notes 94–101 and accompanying text (discussing the methodology used to identify cases); *see also* DTSA LITIGATION, *supra* note 93.

[194] *See supra* note 130 and accompanying text (discussing removal); *see also* DTSA LITIGATION, *supra* note 93.

[195] *See supra* note 131 and accompanying text (discussing counterclaims); *see also* DTSA LITIGATION, *supra* note 93.

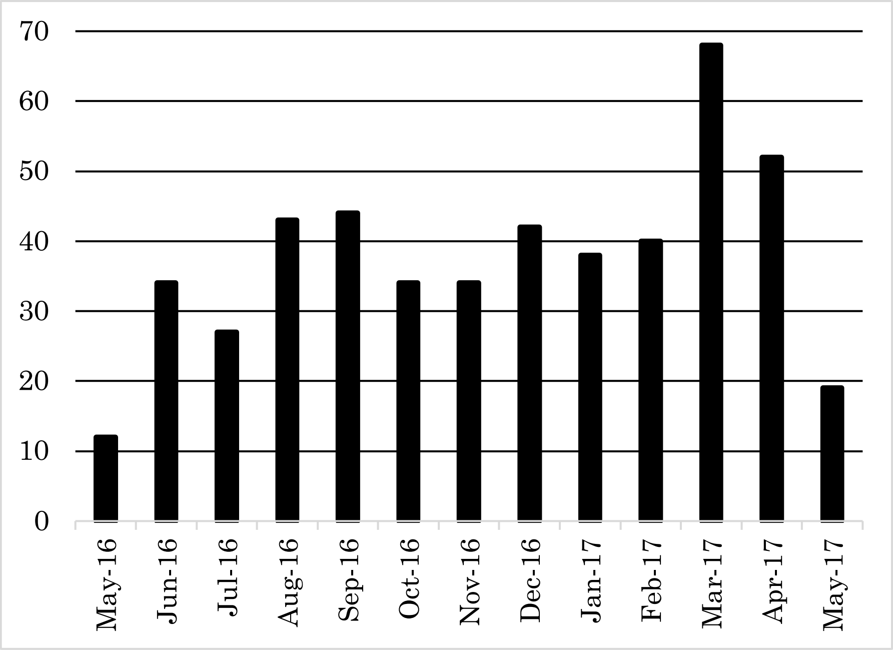
[196] We coded filing dates of DTSA claims based on the first pleading that alleged a cause of action under the DTSA. For most cases, this was the initial complaint. However, a significant number of cases (albeit a minority) first advanced a DTSA claim in an amended complaint; this typically occurred when a DTSA claim was added to a lawsuit that was already pending in federal court at the time of the DTSA's passage.

[197] DTSA claims filed in May 2016 were prorated over the remainder of the month because the DTSA's passage occurred on May 11, 2016. *See* DTSA LITIGATION, *supra* note 93.

[198] DTSA claims filed in May 2017 were prorated over the first part of the month, as the study period ended on May 11, 2017. *See id.*

conduct occurring prior to the DTSA's passage might be actionable under the DTSA if it was part of a continuing misappropriation.[199]

FIGURE 1: DTSA CLAIMS BY MONTH



It is also interesting to compare DTSA filings to patent cases, as both patents and trade secrecy are intended to promote innovation, albeit

[199] *See, e.g.*, Brand Energy & Infrastructure Servs., Inc. v. Irex Contracting Grp., No. CV 16-2499, 2017 WL 1105648, at *4 (E.D. Pa. Mar. 24, 2017) (denying a motion to dismiss because the plaintiff's complaint alleged, as part of a continuing misappropriation, that the defendant "used" the plaintiff's trade secrets after the DTSA's enactment); Adams Arms, LLC v. Unified Weapons Sys., Inc., No. 8:16-CV-01503-T-33AEP, 2016 WL 5391394, at *6 (M.D. Fla. Sept. 27, 2016) (denying a motion to dismiss and holding that the plaintiff could pursue a claim based on the disclosure of trade secret misappropriation occurring after the DTSA's passage, even if the trade secret information was improperly acquired prior to the DTSA); Syntel Sterling Best Shores Mauritius Ltd. v. Trizetto Grp., Inc., 15-cv-211 (LGS) (RLE), 2016 WL 5338550, at *6 (S.D.N.Y. Sept. 23, 2016) (finding viable a continuing misappropriation claim that began preenactment because the DTSA defines misappropriation as the "disclosure or use of a trade secret" and the complaint alleged that the defendants "continue[d] to use" the trade secrets after the DTSA was enacted).

in different ways.[200] Over 4,500 patent cases were filed in 2016,[201] which is nearly ten times greater than the number of DTSA claims filed over our one-year study period. However, this is something of an apples-to-oranges comparison, as the America Invents Act of 2011 ("AIA") sharply limited multidefendant patent cases.[202]

2. Districts

The top districts for DTSA claims are listed in Table 1 below. Nearly all of the top districts for DTSA claims include major metropolitan areas that are home to high-technology hubs and/or major corporate headquarters: the Northern District of Illinois (Chicago); the Northern District of California (San Francisco and Silicon Valley); the Central District of California (Los Angeles); the Southern and Eastern Districts of New York (New York City); the Eastern District of Virginia (suburban D.C.); and the Eastern District of Pennsylvania (Philadelphia). Also noteworthy is the overall distribution of cases: no individual district has more than 10% of all DTSA claims, and 67 out of 90 district courts (74%) have at least one DTSA claim.[203]

[200] *See* Brenda M. Simon & Ted Sichelman, *Data-Generating Patents*, 111 NW. U. L. REV. 377, 382–83 (2017) ("Patent and trade secret law share the same goal of promoting innovation."); *see also* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 484–85 (1970).

[201] BRIAN C. HOWARD & JASON MAPLES, LEX MACHINA, PATENT LITIGATION YEAR IN REVIEW 2016, at 1 (2017), http://www.raklaw.com/wp-content/uploads/2017/05/LexMachina-2016-Patent-Litigation-Year-in-Review-1-1.pdf.

[202] Leahy-Smith America Invents Act, Pub. L. No. 112-29, § 19(d)(1), 125 Stat. 284, 332–33 (2011) (codified at 35 U.S.C. § 299 (2012)); David O. Taylor, *Patent Misjoinder*, 88 N.Y.U. L. REV. 652, 671 (2013) ("When compared to the treatment of [Fed. R. Civ. P.] 20 . . . , the AIA makes it more difficult to join accused infringers in patent infringement cases . . . ."); *see also* Christopher Cotropia et al., *Unpacking Patent Assertion Entities (PAEs)*, 99 MINN. L. REV. 649, 676–78 (2013) (reporting that the number of patent cases filed more than doubled after the AIA's passage but the total number of defendants stayed relatively constant).

[203] This calculation excludes district courts in U.S. territories and the Commonwealth of Puerto Rico as well as the two federal trial courts with specialized jurisdiction (the U.S. Court of Federal Claims and the U.S. Court of International Trade). *See* DTSA LITIGATION, *supra* note 93.

TABLE 1: TOP DISTRICTS FOR DTSA CLAIMS (MINIMUM 10 CASES)

District	**Cases**	**%**
Northern District of Illinois	43	9%
Northern District of California	38	8%
Central District of California	30	6%
Southern District of New York	29	6%
Eastern District of Virginia	16	3%
Eastern District of Pennsylvania	15	3%
Southern District of Florida	15	3%
District of Colorado	13	3%
District of Massachusetts	12	2%
District of Utah	12	2%
Eastern District of New York	11	2%
District of New Jersey	11	2%
District of Delaware	10	2%
District of Oregon	10	2%
Eastern District of Michigan	10	2%
Southern District of California	10	2%
Western District of Pennsylvania	10	2%

In comparison, unlike DTSA claims, patent litigation is highly concentrated in a handful of districts, with the top two fora—the Eastern District of Texas and the District of Delaware—receiving nearly half of all patent cases filed in 2016.[204] In contrast, these two districts have relatively few DTSA claims—the District of Delaware had only 2% of all DTSA litigation (10 cases) during the study period, while the Eastern District had approximately 1% (7 cases).[205]

3. *Nature of Suit Codes*

Another significant issue is the nature of suit code designated by plaintiffs for cases containing a DTSA claim.[206] Unlike patent, copyright, and trademark cases, there is no separate NOS code for DTSA cases.[207] Table 2 below shows the most common NOS code used for cases in the dataset.

[204] According to one study, in 2016 the Eastern District of Texas saw 1662 patent cases filed (37% of all patent cases) and the District of Delaware saw 455 cases filed (10%). HOWARD & MAPLES, *supra* note 201, at 4.

[205] DTSA LITIGATION, *supra* note 93.

[206] *See supra* note 95 and accompanying text (explaining NOS codes).

[207] *Id.* at 30.

TABLE 2: DTSA CLAIMS BY NATURE OF SUIT CODE

Nature of Suit Code	**Type of Claim**	**Cases (%)**
190	Contract (Other)	26%
470	RICO	2%
820	Copyright	7%
830	Patent	6%
840	Trademark	8%
890	Other Statutory Actions	45%
Various	Other	4%

The most common NOS code (890)—used in nearly half of all DTSA cases (45%)—is a catch-all designation for statutory actions that do not clearly fall into another category, while the second-most common NOS code (190) is for non-specific contract-based claims (26%).[208] Other frequently used NOS codes include copyright (820) (7% of cases), patent (830) (6% of cases), and trademark (840) (8% of cases).[209] To assist future empirical research in trade secret disputes, we recommend that the Administrative Office of the U.S. Courts create a new NOS code for DTSA litigation.

B. Pleadings

As previously described, each pleading asserting a DTSA claim was coded for a variety of information.[210] The key findings from this data are reported below.

1. Jurisdiction

One group of variables coded was the asserted bases for subject matter jurisdiction in federal court.[211] The vast majority, or 96%, of all cases with a DTSA claim expressly asserted that jurisdiction existed based on the existence of a federal question.[212] Also, 44% of cases asserted federal jurisdiction based on diversity of citizenship of

[208] DTSA LITIGATION, *supra* note 93.

[209] *Id.*

[210] *See supra* notes 102–10, 127–75 and accompanying text.

[211] *See supra* notes 127–29 and accompanying text.

[212] 28 U.S.C. § 1331 (2012). As previously noted, a small percentage of DTSA claims were raised as counterclaims. Under the well-pleaded complaint rule, federal question jurisdiction under § 1331 cannot be based on a counterclaim. *See* Louisville & Nashville R.R. Co. v. Mottley, 211 U.S. 149, 152 (1908); *see also* Christopher A. Cotropia, *Counterclaims, The Well-Pleaded Complaint, and Federal Jurisdiction*, 33 HOFSTRA L. REV. 1, 2 (2004) ("[F]ederal law counterclaims cannot form the sole basis for federal question jurisdiction."); DTSA LITIGATION, *supra* note 93.

the litigants.[213] In addition, supplemental jurisdiction over related state law claims was alleged in 78% of cases.[214]

Interestingly, 128 cases in the dataset (26%) appear to lack federal court jurisdiction absent the DTSA because the plaintiff neither asserted any other federal law claim nor alleged diversity of citizenship.[215] The remaining 358 cases (74%) would have been properly filed in federal court even without the DTSA.[216] This suggests that the DTSA has expanded access to federal court for some trade secret disputes that previously would have been litigated in state court, albeit modestly.[217]

2. *Other Federal Law Claims*

Nearly half of all pleadings in the dataset (45%, or 220 out of 486 cases) asserted one or more other claims arising under federal law in addition to a DTSA claim.[218] As shown in Table 3 below, the most common non-DTSA federal law claim was the CFAA (20%, 95 cases),[219] followed by claims under the Lanham Act (15%, 73 cases).[220] A number of cases involve other IP claims, including patent (6%, 30 cases)[221] and copyright (8%, 39 cases).[222] Less common were claims brought under the federal RICO statute (2%, 11 cases)[223] and federal antitrust law (less than 1%, 2 cases).[224] Finally, 13 cases contain other federal claims that do not fall into one of these categories.[225]

[213] 28 U.S.C. § 1332(a), (c); DTSA LITIGATION, *supra* note 93.

[214] 28 U.S.C. § 1367. Notably, some cases with DTSA claims included state law claims but failed to formally plead supplemental jurisdiction under § 1367. *See* DTSA LITIGATION, *supra* note 93.

[215] DTSA LITIGATION, *supra* note 93.

[216] *Id.*

[217] *Cf.* Seaman, *supra* note 12, at 368–70 (explaining that many trade secret cases could be litigated in federal court prior to the DTSA).

[218] DTSA LITIGATION, *supra* note 93.

[219] *See supra* note 133; *see also* DTSA LITIGATION, *supra* note 93.

[220] *See supra* note 136; *see also* DTSA LITIGATION, *supra* note 93.

[221] *See supra* note 134; *see also* DTSA LITIGATION, *supra* note 93.

[222] *See supra* note 135; *see also* DTSA LITIGATION, *supra* note 93.

[223] *See supra* note 138; *see also* DTSA LITIGATION, *supra* note 93.

[224] *See supra* note 137; *see also* DTSA LITIGATION, *supra* note 93.

[225] *See supra* note 139. This includes claims under the Stored Communications Act, 18 U.S.C. §§ 2701–2702 (2012); the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–2522 (2012); and the Declaratory Judgment Act, 28 U.S.C. §§ 2201–2202 (2012). *See also* DTSA LITIGATION, *supra* note 93.

TABLE 3: NON-DTSA FEDERAL LAW CLAIMS

Claim	Cases	%
Computer Fraud and Abuse Act	95	20%
Lanham Act	73	15%
Copyright	39	8%
Patent	30	6%
Civil RICO	11	2%
Antitrust	2	<1%
Other federal law claims	13	3%

3. *State Law Claims*

In addition, nearly all cases with a DTSA claim also asserted one or more related state law causes of action.[226] Unlike the UTSA, which expressly "displaces conflicting tort, restitutionary, and other . . . civil remedies for misappropriation of a trade secret" (with certain exceptions, such as contractual remedies and criminal violations),[227] the DTSA does not preempt other federal or state law claims.[228] These state law claims asserted are listed in Table 4 below.

TABLE 4: STATE LAW CLAIMS

Claim	Cases	%
State trade secret misappropriation	408	84%
Breach of contract	341	70%
Tortious interference	259	53%
Unfair competition	200	41%
Breach of fiduciary duty	196	40%
Conversion	153	31%
Unjust enrichment	108	22%
Civil conspiracy	82	17%
Breach of implied covenant of good faith	48	10%
Fraud	45	9%
State computer crimes/torts	41	8%
Other state law claims	152	31%

[226] Specifically, parties in 480 out of 486 cases in the dataset (99%) asserted one or more state law claims in the relevant pleading.

[227] UNIF. TRADE SECRETS ACT § 7 (UNIF. LAW COMM'N 1985). Some states modified or declined to adopt this portion of the UTSA. *See* Richard F. Dole, Jr., *Preemption of Other State Law by the Uniform Trade Secrets Act*, 17 SMU SCI. & TECH. L. REV. 95, 99 (2014). For instance, Iowa, New Mexico, and Nebraska did not enact section 7 of the UTSA, and, as a result, there is no preemption of state law claims related to the misappropriation of a trade secret in those states. *See* IOWA CODE §§ 550.1–.7 (2018); NEB. REV. STAT. §§ 87-501 to -507 (2018); N.M. STAT. ANN. §§ 57-3A-1 to -7 (2018); *see also* 205 Corp. v. Brandow, 517 N.W.2d 548, 551–52 (Iowa 1994).

[228] *See supra* note 141. The whistleblower provision of the DTSA is an exception. *See supra* notes 69, 141 and accompanying text.

Unsurprisingly, the most frequently raised state law claim was trade secret misappropriation, which was raised 84% of the time (408 out of 486 cases).[229] Contract-related claims were common as well. Breach of contract was alleged in 70% of pleadings (341 cases),[230] and the quasi-contractual claim of unjust enrichment (22%, 108 cases)[231] and breach of the implied covenant (or duty) of good faith and fair dealing (10%, 48 cases)[232] were also repeatedly raised by trade secret owners. In addition, tortious interference with contractual or business relations was asserted in slightly over half of all DTSA disputes (53%, 259 cases). Other common tort-related claims were unfair competition (41%, 200 cases); breach of a fiduciary duty, such as the duty of loyalty (40%, 196 cases); conversion (31%, 153 cases); civil conspiracy (17%, 82 cases); and fraud (9%, 45 cases). An additional 8% of pleadings (41 cases) asserted a violation of a state computer crime statute.[233] Finally, other state law causes of action not listed above were raised 31% of the time (152 cases).[234]

4. *Type of Trade Secret Information Allegedly Misappropriated*

We also studied the type of trade secret information that was allegedly misappropriated. As previously discussed, trade secret information is defined expansively under both state law and the DTSA.[235] As one leading treatises has explained, "[V]irtually any subject matter of information can be a trade secret" if the statutory

[229] DTSA LITIGATION, *supra* note 93.

[230] *Id.*

[231] *See supra* note 149; *see also* RESTATEMENT (THIRD) OF RESTITUTION AND UNJUST ENRICHMENT § 1 (AM. LAW INST. 2011) ("A person who is unjustly enriched at the expense of another is subject to liability in restitution."); Douglas Laycock, *Restoring Restitution to the Canon*, 110 MICH. L. REV. 929, 931 (2012) (explaining that "[q]uasi-contract [is] the nineteenth-century name for the common law's response to cases of what we would now call unjust enrichment"); DTSA LITIGATION, *supra* note 93.

[232] *See supra* note 144; *see also* RESTATEMENT (SECOND) OF CONTRACTS § 205 (AM. LAW INST. 1981) ("Every contract imposes upon each party a duty of good faith and fair dealing in its performance and its enforcement."); DTSA LITIGATION, *supra* note 93.

[233] *See supra* note 151; *see also* Christine LiCalzi, *Computer Crimes*, 54 AM. CRIM. L. REV. 1025, 1063 (2017) ("Every state has enacted some form of computer-specific criminal legislation."); DTSA LITIGATION, *supra* note 93.

[234] *See supra* note 153; *see also* DTSA LITIGATION, *supra* note 93. Other state law claims included the following: accounting, aiding and abetting, declaratory judgment, defamation, false advertising, inducement of breach of contract, injunctive relief, intentional and/or negligent nondisclosure, misappropriation of confidential or proprietary information, negligence, promissory estoppel, quantum meruit, replevin, specific performance, trademark infringement under state or common law, trespass to chattels, usurpation of business opportunity, and violation of state franchise law.

[235] *See supra* note 155 and accompanying text.

requirements are met.[236] Accordingly, we created several broad categories of trade secret information and attempted to classify each allegedly misappropriated trade secret into one of these categories.[237] Table 5 below summarizes our findings on this issue.

TABLE 5: ALLEGEDLY MISAPPROPRIATED TRADE SECRETS

Trade Secret	Cases	%
Customer list/information	284	58%
Business information (including financial data, marketing information, and business plans)	280	58%
Technical information	189	39%
Software/algorithm	105	22%
Formula	37	8%
"Negative" knowledge/know-how	6	1%

The leading categories of allegedly misappropriated trade secret information were customer lists and other customer information (58%, 284 cases) and business information (58%, 280 cases).[238] Alleged misappropriation of technical information was somewhat less frequent, occurring in nearly 40% of DTSA claims (189 cases).[239] But in general, these results are similar to earlier studies of trade secret litigation under state law, which found that customer lists, internal business information, and technical knowledge were the most widely misappropriated types of trade secrets.[240] Less common were allegations of misappropriation of computer software/algorithms (22%, 105 cases)[241] and so-called "negative" trade secrets (1%, 6

[236] MICHAEL A. EPSTEIN, EPSTEIN ON INTELLECTUAL PROPERTY LAW § 1.02(F) (5th ed. 2008 & Supp. 2017).

[237] *See supra* notes 156–64 and accompanying text. Many pleadings alleged that more than one type of trade secret had been misappropriated.

[238] Because there was a high degree of overlap in assertions of misappropriation regarding trade secrets that involved financial data, marketing information and plans, and business plans, and because it was sometimes difficult to clearly distinguish between these categories (for example, financial information and/or marketing strategies included in a business plan), we combined these variables for purposes of reporting. *See supra* notes 157–59 and accompanying text; *see also* DTSA LITIGATION, *supra* note 93.

[239] DTSA LITIGATION, *supra* note 93.

[240] *See* Almeling et al., *supra* note 23, at 304 tbl.3 (studying trade secret cases decided in federal court in 2008 and finding that technical information and know-how were at issue in 35% of the cases, internal business information was at issue in 35% of the cases, and customer lists were at issue in 31% of the cases); Almeling et al., *supra* note 25, at 72 tbl.3 (studying trade secret cases decided in state court from 1995 to 2009 and finding that customers lists were at issue in 52% of the cases, internal business information was at issue in 42% of the cases, and technical information and know-how were at issue in 27% of the cases).

[241] This figure, however, does represent an increase from prior studies. *See* Almeling et al., *supra* note 23, at 304 tbl.3 (finding that software or computer

cases).[242] Interestingly, despite numerous popular accounts depicting secret formulas, such as the recipe for Coca-Cola, as the paradigm of a trade secret,[243] few DTSA claims asserted misappropriation of such information (8%, 37 cases).[244]

5. Relationship between Trade Secret Owner and Alleged Misappropriator(s)

Another issue is the relationship, if any, between the owner of the alleged trade secret and the alleged misappropriator(s). Previous studies have found that the vast majority of trade secret litigation under state law involves "someone the trade secret owner knew—either an employee or a business partner."[245] This remains true in litigation under the DTSA. Approximately two-thirds of all DTSA disputes involve a current or former employee of the alleged trade secret owner (66%, 323 cases),[246] while 26% involve a current or former business partner (128 cases).[247] Only 10% of DTSA claims (50 cases) involve parties who lack a prior relationship.[248]

6. Misappropriation by Foreign Defendants

As previously explained, the DTSA's sponsors repeatedly cited high-profile incidents of alleged trade secret misappropriation by

programs were at issue in 10% of trade secret cases in federal court in 2008); Almeling et al., *supra* note 25, at 72 tbl.3 (finding that software or computer programs were at issue in 6% of trade secret cases in state court from 1995 to 2009); DTSA LITIGATION, *supra* note 93.

[242] *See supra* note 163 (explaining negative trade secrets); *see also* DTSA LITIGATION, *supra* note 93.

[243] *See, e.g.*, Liam Stack, *A Secret Blend of 11 Herbs and Spices Slips Out, but Is It the Colonel's?*, N.Y. TIMES, Aug. 27, 2016, at A13 (describing how the formula for KFC's fried chicken, which the company describes as "one of the biggest trade secrets in the world," was allegedly disclosed to a reporter); *Vault of the Secret Formula*, WORLD OF COCA-COLA, https://www.worldofcoca-cola.com/explore/explore-inside/explore-vault-secret-formula/ (last visited Apr. 10, 2018) (describing the "vault where the legendary secret formula for Coca-Cola is secured"); *What's Inside WD-40? Superlube's Secret Sauce*, WIRED (Apr. 20, 2009, 12:00 PM), https://www.wired.com/2009/04/st-whatsinside-6/ (describing some of the contents of WD-40 lubricant, the recipe for which is "a closely guarded trade secret").

[244] DTSA LITIGATION, *supra* note 93.

[245] Almeling et al., *supra* note 23, at 294; *see also id.* at 302 tbl.2 (studying trade secret claims in federal court in 2008 and finding that 59% involved an employee or former employee of the trade secret owner, while 31% involved a business partner); Almeling et al., *supra* note 25, at 69 tbl.2 (studying trade secret claims in state court from 1995 to 2009 and finding that 77% involved an employee or former employee of the trade secret owner, while 20% involved a business partner).

[246] DTSA LITIGATION, *supra* note 93.

[247] *Id.*

[248] *Id.* Totals exceed 100% because 15 cases involve both a current or former employee *and* a business partner of the alleged trade secret owner.

foreign entities and governments as a reason that federal civil trade secret legislation was needed.[249] However, our study finds that few foreigners were named as defendants in DTSA claims. Out of 486 cases in our dataset, only 29 (6%) alleged that a foreign citizen or national had committed trade secret misappropriation.[250] China is the most represented country for foreign defendants, but only in 7 cases—in other words, less than 2% of all DTSA claims.[251] Only 1 case named a Russian citizen as a defendant.[252] Foreign citizens or nationals from the following countries were also named as defendants: Canada (5 cases), Singapore (3 cases), France (2 cases), India (2 cases), Taiwan (2 cases), Colombia (1 case), the Cayman Islands (1 case), Germany (1 case), Japan (1 case), Jordan (1 case), Mauritius (1 case), Sweden (1 case), and the United Kingdom (1 case).[253]

7. *Cyberespionage*

In addition, the DTSA's sponsors argued, at least initially, that the DTSA was needed to help combat the growing problem of cyberespionage.[254] However, the vast majority of trade secret misappropriation claims under the DTSA do not allege hacking. Only 9% of DTSA suits (42 cases) assert that one or more defendants accessed the trade secret owner's computer network without authorization.[255] In addition, most hacking claims involve domestic rather than foreign defendants; only 4 cases assert that a foreign citizen plotted to steal trade secrets through cyberespionage.[256]

[249] *See supra* notes 44–45, 50 and accompanying text.

[250] DTSA LITIGATION, *supra* note 93. In our dataset, 451 cases (93%) involve only U.S. defendants. In an additional 5 cases (1%), the citizenship of one or more defendants is unclear from the pleadings. *Id.*

[251] *Id.*

[252] *See* Complaint at 1, OOO Brunswick Rail Mgmt. v. Sultanov, No. 5:17-cv-00017-NC (N.D. Cal. filed Jan. 4, 2017) (naming a dual citizen of the United States and the Russian Federation as a defendant).

[253] DTSA LITIGATION, *supra* note 93. One case involves two related foreign defendants. *See* Amended Complaint at 2, Poly-Med, Inc. v. Novus Sci. Pte. Ltd., No. 8:15-cv-01964-JMC, (D.S.C. filed Nov. 29, 2016) (naming a Singaporean corporation and a Swedish corporation that are part of the same firm—Novus Scientific—as defendants).

[254] *See supra* note 46 and accompanying text; *see also* H.R. REP. NO. 114-529, at 3 (2016) (discussing "the increased digitization of critical data" that is "highly susceptible to theft"); S. REP. NO. 114-220, at 2 (2016) ("Protecting trade secrets has become increasingly difficult given ever-evolving technological advancements. Thieves are using increasingly sophisticated methods to steal trade secrets and the growing use of technology and cyberspace has made trade secret theft detection particularly difficult.").

[255] *See supra* note 168 and accompanying text (defining hacking); *see also* DTSA LITIGATION, *supra* note 93.

[256] *See generally* Complaint, KCG Ams. LLC v. Zhang, No. 5:17-cv-01953-EJD (N.D. Cal. filed Apr. 7, 2017) (alleging that the defendant, a Chinese

8. *Nondisclosure Agreements*

Finally, we looked at one important measure frequently used by companies to protect their trade secret information against accidental or intentional disclosure—a nondisclosure agreement.[257] 72% of all DTSA claims (350 out of 486 cases) assert that one or more alleged misappropriators were subject to an NDA.[258] In particular, 81% of current and former employees (262 out of 323 cases) who allegedly misappropriated a trade secret had agreed to an NDA, according to these pleadings—a difference that is statistically significant when compared to nonemployee defendants.[259]

C. *Interim Relief*

This section summarizes the data on interim relief in DTSA cases, including motions and court decisions on TROs and preliminary injunctions under Federal Rule of Civil Procedure 65,[260] as well as ex parte seizures under the DTSA.[261]

national, obtained other employees' user names and passwords and logged into their desktops without authorization to copy the alleged trade secret information); Complaint, River City Media, LLC. v. Kromtech All. Corp., No. 2:17-cv-00105-SAB (E.D. Wash. filed Mar. 21, 2017) (asserting that the defendants, including a German corporation, "perpetrated a coordinated, months-long cyberattack" against the plaintiffs); Complaint, Vape Soc'y Supply Corp. v. Zeiadeh, No. 8:16-cv-01971-JCG (C.D. Cal. filed Oct. 29, 2016) (asserting that a Jordanian national accessed one of the plaintiff's computers without authorization in violation of the CFAA, changed passwords, altered access controls for the plaintiff's website, and destroyed data); Complaint, Effex Capital, LLC v. Wilson, No. 1:16-cv-05438-ALC (S.D.N.Y. filed July 7, 2016) (alleging that the defendant, a U.K. citizen, violated the CFAA and a state computer crimes statute by accessing trade secret information without authorization or by exceeding authorized access on his final day of employment); DTSA LITIGATION, *supra* note 93.

[257] *See* Almeling et al., *supra* note 25, at 81 ("Confidentiality agreements with employees are the reasonable measure that courts cite most often in both federal and state [trade secret] cases."); Evans, *supra* note 12, at 198 ("In federal case law interpreting state UTSAs, the obligation of confidentiality appears to be the most important consideration for determining whether the trade secret owner used reasonable efforts to protect its trade secret . . . ."); Mareesa A. Frederick & Clara N. Jiménez, *Are the Crown Jewels Really Safe? Considerations for Building a Strong Trade Secret Portfolio in Today's Market*, LANDSLIDE, Mar./Apr. 2017, at 14, 17 (2017) ("Because employees create and work with trade secret information on a daily basis, they play a pivotal role in ensuring this information stays protected. As such, companies should require employees to sign confidentiality or nondisclosure agreements as part of their employment agreement.").

[258] DTSA LITIGATION, *supra* note 93.

[259] $p < 0.001$. DTSA LITIGATION, *supra* note 93.

[260] *See* FED. R. CIV. P. 65(a) (governing preliminary injunctions); *id.* R. 65(b) (governing TROs).

[261] *See* 18 U.S.C.A. § 1836(b)(2) (West 2018) (authorizing ex parte seizures).

1. *Temporary Restraining Orders*

A temporary restraining order may be granted by a court when a plaintiff is "faced with the possibility that irreparable injury will occur before a hearing for a preliminary injunction . . . can be held."[262] TROs thus are intended to "preserv[e] the status quo . . . just so long as is necessary to hold a hearing."[263] A TRO may be granted on an ex parte basis without notice to the other party only if the moving party can demonstrate "immediate and irreparable injury, loss or damage" and the party's attorney certifies why notice should not be required.[264] By rule, a TRO may not exceed fourteen days unless the court has good cause to extend it or the adverse party consents.[265] While uncommon, "courts appear to grant TROs . . . in trade secret litigation more frequently than in any other area of intellectual property law," in part because the public disclosure of trade secret information destroys its value.[266]

For the 486 cases in our dataset, 34% (164 cases) involve a motion seeking a TRO. TROs were granted in 72 of these cases and were denied in 52 cases. There was no decision in the remaining 40 cases. In short, TROs were granted 58% of the time (72 of 124 cases) the court reached a decision.

2. *Preliminary Injunctions*

A preliminary injunction is a form of equitable relief "that is issued to protect [a] plaintiff from irreparable injury and to preserve the court's power to render a meaningful decision after a trial on the merits."[267] A preliminary injunction is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief."[268] To obtain a preliminary injunction, the plaintiff must prove that it "is likely to succeed on the merits, that [it] is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in [the plaintiff's] favor, and that an injunction is in the public interest."[269] In trade secret cases, the threat of a trade secret's disclosure may establish the necessary irreparable harm.[270]

[262] CHARLES ALAN WRIGHT ET AL., 11A FEDERAL PRACTICE & PROCEDURE § 2951 (3d ed. 2017).

[263] Granny Goose Foods, Inc. v. Brotherhood of Teamsters & Auto Truck Drivers Local No. 70, 415 U.S. 423, 440 (1974).

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

[265] *Id.* R. 65(b)(2).

[266] TERRENCE P. ROSS, INTELLECTUAL PROPERTY LAW: DAMAGES AND REMEDIES § 11.06, at 68 (2004).

[267] WRIGHT ET AL., *supra* note 262, § 2947.

[268] Winter v. Nat. Res. Defense Council, Inc., 555 U.S. 7, 22 (2008).

[269] *Id.* at 20.

[270] *See, e.g.*, Campbell Soup Co. v. ConAgra, Inc., 977 F.2d 86, 92 (3d Cir. 1992); *see also* JAGER, *supra* note 34, § 7:5 ("In the typical trade secret case, the

For the 486 cases in our dataset, 45% (220 cases) involve a motion seeking a preliminary injunction. A preliminary injunction was granted in 86 cases and was denied in 62 cases. There was no decision in the remaining 72 cases. In short, preliminary injunctions were granted 58% of the time (86 of 148 cases) when the court reached a decision. This grant rate is substantially higher than that reported in the Almeling et al. study of pre-DTSA trade secret litigation in federal court, which found that trade secrets owners received a preliminary injunction or TRO less than 40% of the time.[271]

3. *Ex Parte Seizures*

As previously explained, the DTSA added a new remedy not previously available in trade secret litigation: a court order for the seizure of property containing trade secret information granted on an ex parte basis. During the legislative process, Congress added numerous requirements for obtaining this relief, including showing that "immediate and irreparable injury will occur if such seizure is not ordered,"[272] demonstrating a likelihood of success on the merits of the trade secret claim,[273] and establishing that a TRO or preliminary injunction "would be inadequate to achieve" effective relief "because the party to which the order would be issued would evade, avoid, or otherwise not comply with the order."[274]

Despite (or perhaps, because of) receiving extensive attention during the DTSA's enactment, the statutory ex parte seizure remedy has been a little-used provision by trade secret plaintiffs. Out of 486 cases in the dataset, only 2% (10 cases) involve a motion for an ex parte seizure. In only two cases was an ex parte seizure granted.[275] Courts denied a seizure in seven other cases, and there was no decision in the remaining case.

irreparable harm alleged by the trade secret owner is the threatened disclosure of trade secrets by ex-employees to a new employer.").

[271] *See* Almeling et al., *supra* note 23, at 314 tbls.11 & 12 (finding that TROs and PIs were granted in 44 cases but were denied in 67 cases; data aggregated between tables). This difference is statistically significant at $p < .01$.

[272] Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, § 2(a), 130 Stat. 376, 376 (codified at 18 U.S.C.A. § 1836(b)(2)(A)(ii)(II) (West 2018)). The authors were among the drafters of letters to Congress that sought to draw attention to the risk of abuse attendant to the originally drafted ex parte seizure provisions. *See supra* notes 60–61 and accompanying text.

[273] 18 U.S.C.A. § 1836(b)(2)(A)(ii)(IV).

[274] *Id.* § 1836(b)(2)(A)(ii)(I).

[275] Seizure Order, Mission Capital Advisors LLC v. Romaka, No. 1:16-CV-05878-LLS (S.D.N.Y. July 29, 2016); Order, AVX Corp. v. Kim, 6:17-CV-00624-MGL (D.S.C. Mar. 3, 2017). The authors are aware of one additional case where an ex parte seizure has been granted under the DTSA; however, the complaint was filed outside the time of study, so it is not included in our dataset. *See* Order, Blue Star Land Servs. LLC v. Coleman, No. 5:17-CV-00931-R (W.D. Okla. Aug. 31, 2017).

V. IMPLICATIONS

Because this study represents only the first year of litigation under the DTSA, all possible implications may not be evident. Nonetheless, the results from our study have several potentially important implications for trade secret and IP law, as well as innovation policy more generally.

First, claims under the DTSA appear in many cases to overlap with state trade secrets law as well as with other federal and state law causes of action that encompass some or all of the same alleged misconduct.[276] This lends empirical support to the claims of some IP scholars that trade secret law is merely a collection of norms protected by other legal doctrines, such as contract, fraud, and agency law,[277] a proposition which remains hotly debated.[278] Moreover, it suggests that the DTSA is operating in a manner consistent with its sponsors' stated goal of allowing greater access to federal courts for trade secret plaintiffs.[279]

In addition, overlapping state and federal trade secret claims have the potential to create issues of inconsistency and lack of uniformity in areas where the DTSA and UTSA diverge.[280] As one commentator framed the issue, "now that we have a federal statute, *what law are federal district courts going to use in order to interpret the text and flesh out the doctrines of the DTSA?*"[281] While it is

[276] *See supra* Subpart IV.B.2–3.

[277] *See* Bone, *supra* note 29, at 245 (arguing that trade secrecy law should be governed by contract principles); *see also* Lemley, *supra* note 29, at 312 ("Courts, lawyers, scholars, and treatise writers argue over whether trade secrets are a creature of contract, of tort, of property, or even of criminal law."); Risch, *supra* note 29, at 3 (noting that trade secrets are "the most important and most litigated form of intellectual property," yet many scholars maintain that "there is no law of trade secrets").

[278] *See* Lemley, *supra* note 29, at 353 (arguing that "[t]rade secrets are IP rights" and that this understanding provides "a way to think about how those rights are designed, a way that has significant implications for how trade secret law . . . interacts with other laws"); Levine, *supra* note 20, at 147 (noting the pervasiveness of trade secret law, as commentators and courts historically have considered the application of trade secret law amongst various disciplines, "whether [it is] considered a function of property, tort, unfair trade competition, or contract").

[279] *See supra* Subpart IV.B.1.

[280] *See* Sandeen & Seaman, *supra* note 9, at 833 ("While many assume that the principles governing trade secrecy articulated in the UTSA . . . will continue to apply to the DTSA, this is not a foregone conclusion for the simple reason that federal courts are not bound to interpret the DTSA in accordance with the UTSA."); Professors' 2015 Letter, *supra* note 59, at 7 ("The DTSA would undermine th[e] high degree of uniformity [pervading trade secret law] by creating new differences with existing state law and by requiring the development of a new body of federal jurisprudence.").

[281] Camilla Alexandra Hrdy, *Sandeen and Seaman: Toward a Federal Jurisprudence of Trade Secret Law*, WRITTEN DESCRIPTION (Sept. 6, 2016),

reasonable to expect courts to look to existing state trade secret law for guidance, the unique aspects of the DTSA, from the ex parte seizure provision[282] to the ambiguous status of the inevitable disclosure doctrine,[283] suggest that trade secret law may be in for a bumpy ride.

More broadly, our findings suggest that further research into the relationship between trade secret law and other forms of IP protection, such as federal patent, copyright, and trademark law, is warranted, as a notable number of cases in the dataset involve multiple types of IP rights.[284] As discussed earlier, there is limited empirical and scholarly writing on trade secrecy.[285] Comparative literature on trade secrecy across national boundaries is even sparser.[286] The DTSA, rendering trade secret law on par with other federal IP laws, should now be easier to study comparatively.

As for venue, many DTSA cases are filed in major metropolitan areas with clusters of highly innovative industries.[287] In contrast to patent litigation—which is heavily concentrated in two smaller, more rural districts (the Eastern District of Texas and the District of Delaware)[288]—litigation under the DTSA is more broadly distributed. This result suggests that trade secrecy remains of particular interest

http://writtendescription.blogspot.com/2016/09/sandeen-and-seaman-toward-federal.html (discussing Sandeen & Seaman, *supra* note 9).

[282] *See supra* notes 60, 68 and accompanying text.

[283] *See supra* notes 61, 84 and accompanying text.

[284] *See supra* Subpart IV.B.2. As explained by Levine and Sichelman, to the extent that one seeks theoretical analysis of the relationship between trade secrets and other formal appropriation mechanisms, there exists almost no comparison of trade secrecy to methods other than patents, like copyright. *See generally* Levine & Sichelman, *supra* note 7.

[285] *See supra* Subpart II.C.

[286] For one recent paper comparing trade secrecy protection between countries, see Douglas C. Lippoldt & Mark F. Schultz, *Uncovering Trade Secrets – An Empirical Assessment of Economic Implications for Protection for Undisclosed Data* (OECD, Trade Policy Paper No. 167, 2014), https://www.oecd-ilibrary.org/uncovering-trade-secrets-an-empirical-assessment-of-economic-implications-of-protection-for-undisclosed-data_5jxzl5w3j3s6.pdf?itemId=%2Fcontent%2Fpaper%2F5jxzl5w3j3s6-en&mimeType=pdf.

[287] *See supra* Subpart IV.A.2. *See generally* COMPTIA, CYBERSTATES 2016 (2016), https://www.comptia.org/docs/default-source/advocacydocs/cyberstates/comptia-cyberstates-2016-vfinal-v2.pdf?sfvrsn=2 (offering a state-by-state summary of employment in information technology).

[288] *See supra* note 204 and accompanying text; *see also* Matthew Sag, *IP Litigation in U.S. District Courts: 1994–2014*, 101 IOWA L. REV. 1065, 1088 (2016) (noting the "astonishing rise" of patent cases in the Eastern District of Texas and the District of Delaware). *See generally* Brian Love & James Yoon, *Predictably Expensive: A Critical Look at Patent Litigation in the Eastern District of Texas*, 20 STAN. TECH. L. REV. 1 (2017) (comparing U.S. patent litigation across districts to consider the Eastern District of Texas's popularity with patent plaintiffs).

to innovative industries, which comports with prior research,[289] and we expect that interest to grow as the DTSA becomes more established and understood.

Regarding the claims themselves, the large number of DTSA cases against former employees—many of whom are also subject to noncompete agreements[290]—raises the question of whether trade secret misappropriation claims may hinder the mobility of highly skilled employees and thus potentially affect entrepreneurship and innovation more generally.[291] To the extent that the DTSA amplifies mobility of labor issues, particularly in claims that are later found to lack merit, the DTSA could have a negative effect on information diffusion. This is an issue that warrants further examination in future studies.

Importantly, the fact that few DTSA cases involve claims of computer hacking suggests that the law is not as valuable of a weapon against cyberespionage as the law's sponsors had at one time hoped.[292] While it is, again, too early to conclude that the DTSA is ineffective against cyberespionage, this result does comport with the sponsors' shift during the legislative process toward pointing to other

[289] *See* Hurmelinna-Laukkanen & Puumalainen, *supra* note 89 (finding a positive relationship between seeking short-term value, the use of lead-time, and secrecy); Zaby, *supra* note 86, at 159 (emphasizing that if "the winner of a R&D race decides to patent his invention, he loses his technological lead and consequently all firms face the same probability of success subsequently").

[290] *See supra* note 170 and accompanying text (describing coding for noncompete agreements). We found that nearly half (47%, 153 of 323 cases) of DTSA claims involving current or former employees also alleged that the employee was or is subject to a noncompete agreement.

[291] *See* COUNCIL OF ECON. ADVISORS, LABOR MARKET MONOPSONY: TRENDS, CONSEQUENCES, AND POLICY RESPONSES 5–6, 8–9, 14–15 (2016), https://obamawhitehouse.archives.gov/sites/default/files/page/files/20161025_monopsony_labor_mrkt_cea.pdf (discussing the potential benefits and drawbacks of noncompete agreements); *see also* Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 791 (2015) ("Noncompete agreements are now required in almost every industry and position, stymieing job mobility and information flows."). *But see* Jonathan Barnett & Ted M. Sichelman, *Revisiting Labor Mobility in Innovation Markets* 7 (USC Ctr. for Law & Social Sci., Research Paper No. 16-13, 2016) https://ssrn.com/abstract=2758854 (suggesting that "enforcing noncompetes limits the mobility of R&D personnel, which may hinder the efficient allocation of talent across firms" but finding that "the conventional analysis of noncompetes and other restraints on employee mobility cannot support a definitive position against or in favor of enforcing these agreements"). *See generally* Matt Marx & Lee Fleming, *Non-Compete Agreements: Barriers to Entry . . . and Exit?*, 12 INNOVATION POL'Y & ECON. 39 (2012) (suggesting that noncompete agreements can affect the level and sources of entrepreneurial activity).

[292] *See supra* Subpart IV.B.7; *see also* Levine, *supra* note 12, at 329 (asserting that the DTSA "solves a problem that has not been proven to exist, while creating new or exacerbating existing problems and failing to address cyberespionage directly").

rationales for adopting the DTSA.[293] To the extent that there are early lessons regarding cyberespionage from this study, it lends support to the argument that a more fruitful statutory course of combatting such activity may lie in reforming the CFAA,[294] which has been the subject of wide criticism.[295] Especially since it is not being used heavily to combat cyberespionage, the DTSA may serve as a distraction from considering real solutions to the serious cyberespionage problem facing American industry.

Furthermore, the widespread availability of interim relief for trade secret owners under Federal Rule of Civil Procedure 65—nearly a quarter of all trade secret plaintiffs were awarded a TRO, a preliminary injunction, or both[296]—has rendered the DTSA's ex parte seizure provision largely superfluous. Some commentators have asserted that the relative lack of ex parte seizures so far demonstrates that concerns raised by law professors and others about this provision were overblown.[297] But these claims overlook the fact that numerous safeguards were added during the legislative process to protect against abusive ex parte seizures, including clarifying that they could only be awarded in "extraordinary circumstances," suggesting the

[293] *See* Levine, *supra* note 55 (stating that the rationale of the DTSA shifted from cyberespionage to "the rise of trade secret theft by rogue employees and the need for uniformity in trade secret law").

[294] *See* Levine, *supra* note 12, at 329; Levine & Sandeen, *supra* note 12, at 259–60.

[295] *See* Jamie Williams, *Our Fight to Rein in the CFAA: 2016 in Review*, ELEC. FRONTIER FOUND. (Dec. 28, 2016), https://www.eff.org/deeplinks/2016/12/our-fight-rein-cfaa-2016-review ("The law's notoriously vague language has confused courts, chilled security research, and given overzealous prosecutors broad discretion to bring criminal charges for behavior that in no way qualifies as breaking into a computer. And it's out of touch with how we use computers today."); Josephine Wolff, *The Hacking Law That Can't Hack It*, SLATE (Sept. 27, 2017, 11:15 AM), http://www.slate.com/articles/technology/future_tense/2016/09/the_computer_fraud_and_abuse_act_turns_30_years_old.html (criticizing the CFAA).

[296] *See supra* Subparts IV.C.1–2 (finding that preliminary relief was granted in 121 out of 486 cases). Courts granted both a TRO and a preliminary injunction in 37 cases. *See* DTSA LITIGATION, *supra* note 93.

[297] *See, e.g.*, Jessica Engler, *Insights and Lessons: The Defend Trade Secrets Act at Year One*, IN-HOUSE DEF. Q., Fall 2017, at 20, 21 ("[F]ears that the *ex parte* seizure provision would be misused seem to be mostly assuaged."); Paul M. Mersino, *The DTSA's Ex Parte Seizure Order: The "Ex" Stands for "Extraordinary,"* TECH. & MARKET. L. BLOG (Feb. 2, 2017), http://blog.ericgoldman.org/archives/2017/02/the-dtsas-ex-parte-seizure-order-the-ex-stands-for-extraordinary-guest-blog-post.htm ("Based on a review of all known cases, . . . [i]t appears that *ex parte* seizures have not been abused, as some feared."); *see also* Pooley, *supra* note 12, at 1056 (asserting that law professors' concerns about the ex parte seizure provisions were "ungrounded and exaggerated").

possibility that Congress took these concerns about potential abuse seriously.[298]

Finally, as federal courts work through these cases for the first time, their collective interpretation of the scope of trade secret law will undoubtedly impact how states interpret their own trade secret laws. Given relatively "fresh" eyes on the law, we envision conflicts that may lead to altered contours of trade secret law, cybersecurity practice, and information law more broadly. We also expect to see increasingly nuanced opinions out of federal courts, which should aid in our overall understanding of trade secret law and information sharing today.

For example, deepening the understanding of trade secret law at the federal level might allow courts, over time, to take a more granular view of the Freedom of Information Act ("FOIA") trade secret exemption.[299] The FOIA trade secret exemption has been liberally applied by courts and is generally found to exempt wide swaths of information from public disclosure, even after litigation challenges.[300] There has been a judicial and legislative thumb on the scale in favor of protecting trade secrets from public disclosure, even in situations where the public might have a strong interest in the information, like code in voting machines[301] and the chemical formula of liquids used in hydraulic fracturing.[302] It is conceivable that

[298] Sandeen & Seaman, *supra* note 9, at 851 & n.126 (citing 18 U.S.C.A. § 1836(b)(2)(A)(i) (West 2018)).

[299] *See* 5 U.S.C. § 552(b)(4) (2012) (exempting from FOIA "matters that are . . . trade secrets and commercial or financial information obtained from a person and privileged or confidential").

[300] *See* Levine, *supra* note 20, at 137–38 (noting the tension between the interests of the *public* and *commerce*—"[s]ecrecy, and its attendant goals of pecuniary gain and commercial competition, conflict with the methods and purpose of transparent and accountable democratic governance"); *see also* David S. Levine, *The People's Trade Secrets?*, 18 MICH. TELECOMM. & TECH. L. REV. 61, 64 (2011) (arguing that the government should not have the power to define information about public expenditures as a trade secret).

[301] *See* Levine, *supra* note 20, at 138 (arguing that the conflict between secrecy and transparency and accountability "is crystallized in the private distribution of voting machines").

[302] *See* David S. Levine & Mary L. Lyndon, Law Professors' Second Alaska Oil and Conservation Commission Trade Secrets Letter (Oct. 14, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2363099; Vanessa Schipani, *The Facts on Fracking Chemical Disclosure*, FACTCHECK.ORG (Apr. 7, 2017), http://www.factcheck.org/2017/04/facts-fracking-chemical-disclosure/ (noting that a federal judge struck down a fracking rule promulgated by the Bureau of Land Management in 2015 that was intended to protect groundwater and would have required companies to "report some of the chemicals they used during fracking operations on federal and tribal lands in all 50 states"). *See generally* David S. Levine, *Confidentiality Creep and Opportunistic Privacy*, 20 TULANE J. TECH. & INTELL. PROP. 11 (2017) (discussing, in the context of the alleged Russian interference in the 2016 U.S. presidential election via social media, the arguable need for public access to the algorithmic code (i.e., software)

greater federal court exposure to trade secret law may allow courts to more thoroughly examine blanket trade secret exemption arguments and whether the information at issue actually qualifies as a trade secret.[303] On the other hand, it is also possible the DTSA's legislative history evincing a strong public policy in favor of trade secret protection[304] will make courts less likely to overturn an administrative entity's decision to exempt such information from disclosure. To that end, it would be helpful for future scholars to track citations in FOIA judicial and administrative decisions to DTSA cases and their impact, if any, on outcomes.

In sum, this Article's focus on an empirical assessment of DTSA litigation is only the beginning of DTSA-related studies. For example, beyond the scope of this Article are the internal discussions and decisions that lead trade secret owners to decide whether to file litigation under the DTSA or not. Other variables that might be studied include (1) the type of plaintiff (e.g., large/publicly traded firm, small business, or individual), (2) the sector or industry where the trade secret is used, (3) the frequency of whistleblower defense claims, and (4) the outcomes of DTSA cases. Nonetheless, by understanding how the DTSA is being utilized in court in its first year, we can collectively begin the process of critically evaluating the impact of this major addition to IP law.

VI. Conclusion

The DTSA represents one of the most significant changes to the landscape of IP law in decades. Through an original dataset that examines cases filed in the law's first year, this Article provides numerous findings regarding the DTSA's early impact on trade secret law and litigation. It also suggests some implications from this data, including the potential need for additional legislation more directly aimed at cyberespionage, the possibility of a lack of uniformity due to overlapping federal and state law claims covering trade secret misappropriation, and the potential negative impact of the law on labor mobility and information diffusion. In short, while it will not be the final word on the DTSA, this Article provides a preliminary assessment of the law's potential strengths, drawbacks, and limitations, upon which to build.

used by Facebook in order to understand how much information was actually shared and how to prevent such interference in the future).

[303] *See* Levine, *supra* note 300, at 101–02 (explaining that courts rarely, if ever, question a trade secret designation in the face of a FOIA exemption challenge).

[304] *See, e.g.*, S. Rep. No. 114-220, at 1–3 (2016) (noting the detrimental impact trade secret theft has on Americans' quality of life and how the DTSA will "incentivize future innovation while protecting and encouraging the creation of American jobs").