

On Equipose, Knowledge, and Speculation: A Unified Theory of Pleading Under the Defend Trade Secrets Act – Jurisdiction, Identification, Misappropriation, and Inevitable Disclosure

William Lynch Schaller
Schaller Law Lectures, LLC

Follow this and additional works at: <https://digitalcommons.law.uga.edu/jipl>



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

Recommended Citation

William L. Schaller, *On Equipose, Knowledge, and Speculation: A Unified Theory of Pleading Under the Defend Trade Secrets Act – Jurisdiction, Identification, Misappropriation, and Inevitable Disclosure*, 27 J. INTELL. PROP. L. 137 ().

Available at: <https://digitalcommons.law.uga.edu/jipl/vol27/iss2/2>

This Article is brought to you for free and open access by Digital Commons @ Georgia Law. It has been accepted for inclusion in Journal of Intellectual Property Law by an authorized editor of Digital Commons @ Georgia Law. [Please share how you have benefited from this access](#) For more information, please contact tstriepe@uga.edu.

On Equipose, Knowledge, and Speculation: A Unified Theory of Pleading Under the Defend Trade Secrets Act – Jurisdiction, Identification, Misappropriation, and Inevitable Disclosure

Cover Page Footnote

William Lynch Schaller is a principal with Schaller Law Lectures, LLC, Oak Brook, Illinois, where he writes and lectures on trade secrets and related matters. From 1982 until his retirement in 2016, Mr. Schaller served as an associate, partner and principal with Baker & McKenzie, LLP (now BakerMcKenzie LLP), Chicago, Illinois, where his practice focused on trade secret and related litigation. Mr. Schaller is a member of the Sedona Conference Working Group on Trade Secrets. Mr. Schaller's views expressed here are not made on behalf, and do not necessarily represent the views, of BakerMcKenzie, the Sedona Conference, or their respective members or clients.

**ON EQUIPOISE, KNOWLEDGE, AND
SPECULATION: A UNIFIED THEORY OF
PLEADING UNDER THE DEFEND TRADE
SECRETS ACT—JURISDICTION, IDENTIFICATION,
MISAPPROPRIATION, AND INEVITABLE
DISCLOSURE**

William Lynch Schaller†©*

“In nature’s infinite book of secrecy a little I can read.”

– WILLIAM SHAKESPEARE, ANTONY AND CLEOPATRA, act 1, sc. 2, lines 8-9

* William Lynch Schaller is a principal with Schaller Law Lectures, LLC, Oak Brook, Illinois, where he writes and lectures on trade secrets and related matters. From 1982 until his retirement in 2016, Mr. Schaller served as an associate, partner and principal with Baker & McKenzie, LLP (now BakerMcKenzie LLP), Chicago, Illinois, where his practice focused on trade secret and related litigation. Mr. Schaller is a member of the Sedona Conference Working Group on Trade Secrets. Mr. Schaller’s views expressed here are not made on behalf, and do not necessarily represent the views, of BakerMcKenzie, the Sedona Conference, or their respective members or clients.

† This article is dedicated to my daughter, Alexandra J. Schaller, B.A., University of Illinois, J.D., Northwestern University, a Chicago lawyer with Loeb & Loeb, a former law clerk to Judge Bill Bauer of the United States Court of Appeals for the Seventh Circuit, and a former articles editor for the Northwestern Journal of Criminal Law and Criminology. No father could be prouder.

© 2020 William Lynch Schaller. All rights reserved.

TABLE OF CONTENTS

I.	DEFINITIONS AND THE RULE OF LENITY	142
II.	RULE 12(B)(1) – JURISDICTION	148
III.	RULE 12(B)(6) – FAILURE TO STATE A CLAIM	150
	A. <i>TWOMBLY</i> , <i>IQBAL</i> AND EQUIPOISE	151
	B. ALLEGING A TRADE SECRET	159
	C. IDENTIFICATION	160
	D. ECONOMIC VALUE	168
	E. REASONABLE SECRECY EFFORTS	177
	F. ALLEGING MISAPPROPRIATION	183
	G. ALLEGING DISCLOSURE OR USE — AND “INEVITABILITY”	187
	H. INEVITABLE DISCLOSURE AND THE DTSA	193
IV.	PLEADING UNDER THE DTSA: A UNIFIED THEORY AND ITS CONSEQUENCES	199
	A. PROPER PLEADING	199
	B. CONSEQUENCES OF IMPROPER PLEADING	203
V.	CONCLUSION	206

I think it's fair to say every business lawyer and every business client knows trade secrets are vital to business success. I think it's also fair to say every business lawyer and every business client knows trade secret law is in flux. Congress' 2016 passage of the Defend Trade Secrets Act (DTSA),¹ a largely general law creating the first federal private right of action for trade secret misappropriation, gives federal courts an opportunity to critically re-examine the field of trade secret regulation. And they'll certainly get their chance: more than 825 DTSA cases were filed in federal district courts in the two years following the DTSA's enactment.² However, few have reached the United States Courts of Appeals and even fewer have resulted in published appellate opinions.³ As our federal appeals courts are fond of reminding us, federal district court opinions are not precedential,⁴ so development of DTSA jurisprudence will likely take years, if not decades, as cases "percolate" through the Courts of Appeals on their way to the Supreme

¹ See 18 U.S.C. §§ 1831-39 (2018).

² See Daniel McGavock, Robert Goldman & Jack Roberts, *An Update on DTSA and Trade Secret Damages*, LAW360 1, 1–2 (June 26, 2018, 12:18 PM), <http://www.crai.com/sites/default/files/publications/An%20Update%20On%20DTSA%20And%20Trade%20Secret%20Damages.pdf> (noting the Northern District of Illinois and the Northern District of California each had 7% of the total DTSA filings during the two-year period, followed by the Central District of California and the Southern District of New York, each with 6%); Travis S. Hunter & Renée M. Mosley, *Better Safe Than Sorry: Experts Should Apportion Damages in Trade Secret Cases*, AMERICAN BAR ASSOCIATION (Nov. 30, 2018), <https://www.americanbar.org/groups/litigation/committees/commercial-business/articles/2018/fall2018-experts-should-apportion-damages-in-trade-secret-cases/> (placing the total number of DTSA filings at 1,104 for the first two years after statute's passage); David S. Levine & Christopher B. Seaman, *The DTSA at One: An Empirical Study of the First Year of Litigation Under the Defend Trade Secrets Act*, 53 WAKE FOREST L. REV. 105 (2018) (careful examination of nearly 500 cases filed in the DTSA's first year).

³ See, e.g., *CMI Roadbuilding, Inc. v. Iowa Parts, Inc.*, 920 F.3d 560, 567 (8th Cir. 2019) (affirming summary judgment on statute of limitations defense barring DTSA and related Iowa state law claims); *DTC Energy Grp., Inc. v. Hirschfeld*, 912 F.3d 1263, 1270 n.3 (10th Cir. 2018) (noting that the DTSA does not create a presumption of irreparable harm for injunction purposes); *Dunster Live, LLC v. Lonestar Logos Mgmt. Co.*, 908 F.3d 948, 950 (5th Cir. 2018) (DTSA's fee-shifting provision inapplicable when claims are voluntarily dismissed without prejudice); *First W. Capital Mgmt., Co. v. Malamed*, 874 F.3d 1136, 1143 (10th Cir. 2017) (violation of the DTSA does not create presumption of irreparable harm); *Waymo LLC v. Uber Techs., Inc.*, 870 F.3d 1342, 1350 (Fed. Cir. 2017) (noting but not deciding federal trade secret law claims); *United States v. Liew*, 856 F.3d 585, 597 (9th Cir. 2017) (noting DTSA amended the Economic Espionage Act's (EEA) definition of "trade secret," but deciding the case under the EEA's prior definition); *United States v. Nosal*, 844 F.3d 1024, 1042 n.15 (9th Cir. 2016) (noting the DTSA's minor change to the EEA's definition of "trade secret").

⁴ See *Hecny Transp., Inc. v. Chu*, 430 F.3d 402, 404 (7th Cir. 2005) (Easterbrook, J.) (stating district court decisions on state law issues "have neither authoritative nor precedential force . . . so we need not analyze them"); *Mueller v. Reich*, 54 F.3d 438, 441 (7th Cir. 1995) (Posner, C.J.) ("[D]istrict court decisions are not authoritative as precedents, even at the district court level."), *vacated on other grounds*, 519 U.S. 1144 (1997) (mem.).

Court.⁵

To be sure, Congress did not write on a blank slate in fashioning the DTSA. All states except New York now have some type of trade secret statute,⁶ and judicial decisions abound both before and after these statutes' passage. Congress seems to have borrowed bits and pieces from these and other sources while adding a few specialty provisions of its own, such as the DTSA's search and seizure section,⁷ its prohibition on injunctions barring employment based on mere knowledge alone,⁸ and its whistleblower and anti-retaliation protections.⁹ Even though the DTSA and virtually all state trade secret statutes are modeled on the Uniform Trade Secrets Act (UTSA), the DTSA does not contain a "uniformity" provision commanding consistency with these state trade secret laws – perhaps because these state laws are themselves inconsistent, or perhaps because the DTSA sits in the midst of a criminal statute and hence triggers the rule of lenity requiring ambiguous criminal statutes to be read narrowly to protect the accused.¹⁰ Either way, the DTSA does not preempt state law,¹¹ so state trade secret and DTSA claims can be paired in federal court under diversity or supplemental

⁵ See *Box v. Planned Parenthood of Indiana and Kentucky, Inc.*, 139 S. Ct. 1780, 1784 (2019) (Thomas, J., concurring) ("Given the potential for abortion to become a tool of eugenic manipulation, the Court will soon need to confront the constitutionality of laws like Indiana's. But because further percolation may assist our review of this issue of first impression, I join the Court in declining to take up the issue now."); William P. Barr, Opinion, *End Nationwide Injunctions*, WALL ST. J., Sept. 6, 2019, at A15 ("When the system works as it should, it encourages what one leading jurist has called 'percolation' – the salutary process by which many lower federal courts offer competing and increasingly refined views on a legal issue before higher courts definitively resolve it.").

⁶ See generally Michael T. Renaud & Nicholas W. Armington, *Massachusetts Adopts Uniform Trade Secrets Act*, NAT'L L. REV. (Sept. 6, 2018), <https://www.natlawreview.com/article/massachusetts-adopts-uniform-trade-secrets-act> (noting Massachusetts became the 49th state to adopt a version of the Uniform Trade Secrets Act); *E.J. Brooks Co. v. Cambridge Sec. Seals*, 105 N.E.3d 301 (N.Y. 2018) (discussing monetary relief under New York trade secret law, which rests on Section 757 of the Restatement of Torts).

⁷ *Id.* at § 1836(b)(2).

⁸ *Id.* at § 1836(b)(3)(A)(i)(I).

⁹ 18 U.S.C. § 1833(b) (1) and (2) (2019). See, e.g., *Christian v. Lannett Co., Inc.*, CV No. 16-963, 2018 WL 1532849 (E.D. Pa. Mar. 29, 2018) (plaintiff's retention of more than 22,000 pages of confidential documents belonging to her employer, disclosed solely to her attorney for use in her discrimination lawsuit against her employer, fell within DTSA's immunity provision, 18 U.S.C. §1833(b)).

¹⁰ See, e.g., *United States v. Davis*, 139 S. Ct. 2319, 2333 (2019) (noting that the rule of lenity "is founded on 'the tenderness of the law for the rights of individuals' to fair notice of the law 'and on the plain principle that the power of punishment is vested in the legislative, not in the judicial department'" (internal citation omitted)).

¹¹ See 18 U.S.C. § 1838 ("Except as provided in section 1833(b), 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, or to affect the otherwise lawful disclosure of information by any Government employee under section 552 of title 5 (commonly known as the Freedom of Information Act).").

jurisdiction principles. As an alternative, if plaintiffs prefer, they can proceed solely on state law theories in state court.¹²

Unfortunately, like the states, Congress has left the hard questions to the courts. Which questions will emerge first is anyone's guess, but I think the beginning is a good place to start: establishing jurisdiction and pleading claims under the DTSA. What should be the consequences of failing to show federal jurisdiction in a DTSA case? Of failing to show a trade secret exists? Of failing to identify it with specificity at the outset? Of failing to show it's been stolen? Of failing to show the theft was knowing? Of failing to show the stolen secret was disclosed or used? Of failing to show the stolen secret was knowingly disclosed or used? In short, who can be sued for what?

These issues may seem elementary, but I suspect they may prove more daunting than many expect. As I discuss in Part I, given their location in a criminal statute, the DTSA's definitions of "trade secret" and "misappropriation" may be given narrower readings than their counterparts in the UTSA.¹³ The Supreme Court has invoked the rule of lenity in other cases involving statutes sharing the same definitions for criminal and civil purposes, and the DTSA fits this description. Narrow statutory construction may also control close jurisdictional questions if the DTSA's jurisdiction grant is challenged under Rule 12(b)(1) in purely local disputes, an issue I discuss with other jurisdictional questions in Part II.¹⁴

The role of Rule 12(b)(6) in DTSA cases is the topic of Part III.¹⁵ I stress there that very few trade secret cases have reached the Courts of Appeals on Rule 12(b)(6) dismissals, so a number of assumptions about proper pleading are open to question, among them whether trade secrets should be alleged with particularity and fully disclosed in sealed appendixes accompanying DTSA complaints. I also examine the implications of the DTSA's "economic value" and "reasonable secrecy measures" requirements from a pleading standpoint. I end Part III with everyone's favorite trade secret *bête noire*, inevitable disclosure. The DTSA seems to expressly bar this controversial doctrine in injunction actions "brought under" the DTSA, and it may operate to bar it for state law injunction claims

¹² See Abraham Y. Skoff, *Tips for Filing a Trade Secret Action After Enactment of the DTSA: Opting for a DTSA Claim in Federal Court Is Not Necessarily the Automatic Choice That Many Thought It Would Be* (July 31, 2017), <https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/practice/2017/tips-for-filing-a-trade-secret-action-after-enactment-of-dtsa/> (arguing that state law and state court advantages may outweigh DTSA and federal court advantages in some cases); Dylan W. Wiseman, *California Plaintiffs May Prefer State Court for Trade Secret Claims* (Dec. 9, 2019), <https://www.buchalter.com/publication/california-plaintiffs-may-prefer-state-court-for-trade-secret-claims/> (discussing advantages of proceeding in California state court under California state trade secret law rather than proceeding in federal court under the DTSA, including lack of jury unanimity in California state court and omission of "readily ascertainable by proper means" from California's state law definition of "trade secret").

¹³ See *infra* notes 21 to 41 and accompanying text.

¹⁴ See *infra* notes 42 to 53 and accompanying text.

¹⁵ See *infra* notes 54 to 245 and accompanying text.

brought together with DTSA claims. But the DTSA might be read as prohibiting inevitable disclosure for all purposes – not just injunctions – if the Courts of Appeals focus on the “knowledge” requirement found in the DTSA’s definition of “misappropriation,” as inevitable disclosure claims arguably dispense with “knowledge” as an element. Here, too, the rule of lenity may turn out to play a prominent role.

Part IV discusses a unified theory of pleading under the DTSA and its consequences.¹⁶ The upshot there is that district courts should demand proper pleading and should mete out sanctions in appropriate cases that fall short of the mark. Part V offers some closing comments to the effect that property is not the only thing that matters.¹⁷ Employee mobility and market innovation count too, and courts should police DTSA pleadings with these competing interests in mind.

There are many other issues and sub-issues when it comes to trade secrets, of course, but all depend upon the foundational matters of establishing jurisdiction and stating a claim. The DTSA does not directly answer the questions I’ve posed above, so I explore each below as a matter of first principle. My thesis is that DTSA claims should initially be subject to strict scrutiny from a pleading standpoint, so as to protect both competitors and competition. I have generally organized my discussion around two representative district court DTSA decisions, *Plastronics Socket Partners Ltd. v. Highrel Inc.*¹⁸ and *Molon Motor and Coil Corp. v. Nidec Motor Corp.*,¹⁹ to illustrate how pleading should and should not work under the DTSA. My purpose is more to examine than to determine, and to that end I offer illustrative rather than exhaustive case law.²⁰ At times I quote at length from key sources to enhance reader understanding, as I think paraphrasing frequently undercuts analytic clarity. Throughout I emphasize practice and policy in the hope of encouraging business lawyers and their business clients to participate in shaping this critical law.

I. DEFINITIONS AND THE RULE OF LENITY

Too often we overlook the obvious: almost anything can be a trade secret and almost anyone can be sued for stealing it. These far-reaching implications call for care in assessing trade secret claims; competitors don’t like being sued and courts don’t like curbing competition. Making baseless claims, or simply overclaiming, may spell serious trouble for plaintiffs in the form of sanctions or

¹⁶ See *infra* notes 246 to 267 and accompanying text.

¹⁷ See *infra* notes 268 to 272 and accompanying text.

¹⁸ No. CV-18-03201-PHX-SMB, 2019 WL 2054362 (D. Ariz. May 9, 2019).

¹⁹ No. 16 C 03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

²⁰ I’ll skip the more stylish “caselaw.” See Casey C. Sullivan, *Is It Caselaw or Case Law? Twitter, and Everyone Else, Weighs In*, FINDLAW (Nov. 3, 2015, 5:59 PM), <https://blogs.findlaw.com/strategist/2015/11/is-it-caselaw-or-case-law-twitter-and-everyone-else-weighs-in.html> (collecting competing views on the correct nomenclature).

counterclaims,²¹ while well-grounded claims may precipitate prosecution of defendants by federal or state authorities.²² These plainly are dangerous claims,²³ and for everyone's safety I think they should be subjected to procedural rigor from the start.

As to the first point, that anything can be a trade secret, take hospital pricing. A recent Wall Street Journal article reported a strikingly-wide range of prices hospitals charged employers in the same area for treating injured and sick employees: "Prices paid to some hospitals, even in the same city, ranged from double to more than 300% of what Medicare paid, the study published online Thursday found."²⁴ Unsurprisingly, the same article observed: "Prices have long been a closely guarded secret between hospitals and the health insurers that negotiate them."²⁵ So, treating such information as a trade secret makes sense under the

²¹ See, e.g., *Tradesmen Int'l, Inc. v. Black*, 724 F.3d 1004 (7th Cir. 2013) (holding that the Illinois Trade Secrets Act authorized award of attorneys' fees and costs against the plaintiff for wrongfully continuing its trade secret theft action, even assuming the plaintiff was originally justified in bringing the action); Kenneth J. Vanko, *Proving Bad Faith in Trade Secret Cases*, 105 Ill. B. J. 40 (June 2017) (discussing law and strategy for defense recovery of "bad faith" fees under the Illinois Trade Secrets Act, including plaintiff's possible loss of attorney-client privilege under the crime-fraud exception).

²² See, e.g., Heather Somerville & Robert McMillan, *Ex-Google Engineer Faces Federal Charges: Anthony Levandowski Accused of Stealing Information from Google Parent and Taking It to Uber*, WALL ST. J., Aug. 28, 2019, at B1 (reporting 33-count federal indictment of Anthony Levandowski as a result of civil trade secret theft litigation Google/Waymo brought against Uber for hiring Levandowski in connection with self-driving cars); Heather Somerville, *Trade-Secrets Case Seen as Warning*, WALL ST. J., Sept. 4, 2019, at B4 ("The [Levandowski] indictment reflects the Trump administration's priorities, which include the enhanced protection of U.S. intellectual property and more resources to prosecute alleged theft, according to attorneys and federal prosecutors."); Elizabeth Wollman, *Ex-Google Car Project Engineer in Plea Deal*, WALL ST. J., Mar. 20, 2020, at B1 (reporting Levandowski's agreement to plead guilty to a single count of trade secret theft in connection with Google's autonomous vehicle program); 2019 IPEC ANN. REP., at 21–23, 120–26, <https://www.whitehouse.gov/wp-content/uploads/2019/02/IPEC-2018-Annual-Intellectual-Property-Report-to-Congress.pdf> (annual report by the United States Intellectual Property Enforcement Coordinator detailing recent federal prosecutions of trade secret thieves and economic espionage, primarily against Chinese actors, and observing: "The Department of Justice is committed to aggressively investigating and prosecuting individuals and corporations who undermine American competitiveness by stealing what they did not themselves create." *Id.* at 21.); Richard L. Cassin, *South Korea Company Penalized \$360 Million for Plot to Steal DuPont Kevlar Trade Secrets*, THE FCPA BLOG (May 6, 2015, 12:12 PM) <http://www.fcpcbog.com/blog/2015/5/6/south-korea-company-penalized-360-million-for-plot-to-steal.html> (reporting fines and restitution against Kolon Industries).

²³ See, e.g., *In re Muhs*, 923 F.3d 377 (4th Cir. 2019) (discussing trade secret judgment of more than \$20 million and resulting Chapter 7 individual bankruptcy of employee whose conduct triggered the theft claim); Elizabeth Wollman, *Former Google Self-Driving Engineer Files for Bankruptcy: Anthony Levandowski Cites a \$179 Million Legal Judgment in Dispute That Involved Uber*, <https://www.wsj.com> (Mar. 5, 2020) (reporting Anthony Levandowski's bankruptcy filing immediately after Google/Waymo won a \$179 million arbitration award against him for trade secret theft).

²⁴ Melanie Evans, *Employers' Hospital Fees Differ*, WALL ST. J., May 10, 2019, at B3.

²⁵ *Id.*

DTSA's broad definition of "trade secret," found in Section 1839(3):

[T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—

(A) the owner thereof has taken reasonable measures to keep such information secret; and

(B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information;

(4) the term "owner," with respect to a trade secret, means the person or entity in whom or in which rightful legal or equitable title to, or license in, the trade secret is reposed[.]²⁶

I'll return to the hospital example a little later to illustrate the interplay between secrecy measures and independent development, but for the moment, let's focus on who can be sued: virtually anyone who's had access to the owner's secrets and now stands in conflict with the owner.²⁷ Most often this means ex-employees who join or form competitors, but sometimes the accused can be insiders like consultants, accountants, or bankers, or outsiders like suppliers,

²⁶ 18 U.S.C. § 1839 (3)–(4) (2018); *Cf.* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 39 (AM. LAW INST. 1993) ("A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.").

²⁷ Section 1839's express inclusion of licensees avoids the standing problem licensees have faced under state trade secret laws. *See DTM Research, L.L.C. v. AT&T, Corp.*, 245 F.3d 327, 332 (4th Cir. 2001) (authorized possession of secrets supplied standing, even if plaintiff did not "own" them in a fee simple sense); Alex Reese, *Who "Owns" a Trade Secret? Whether Trade Secret Licensees Have Standing to Sue in California*, THE RECORDER (Apr. 2, 2019), <https://www.law.com/therecorder/2019/04/02/who-owns-a-secret-whether-trade-secret-licensees-have-standing-to-sue-in-california/?slreturn=20190504081009> ("The lack of a formal document or process that defines the property interest for trade secret owners has raised a question over who, exactly, has enough 'ownership' of a trade secret to have standing to sue for misappropriation. Yet California courts haven't yet reached this seemingly basic issue.").

distributors or licensees.²⁸ Potential business buyers who see secrets but walk away, only to reemerge shortly thereafter with suspiciously similar products or services, also make prime targets.²⁹ Even lawyers can find themselves in this uncomfortable position.³⁰ Computer hackers, too, are targets, if one can find them and find a place to sue them.³¹ The list is long when it comes to potential wrongdoers because the DTSA in Section 1839(5) broadly defines “misappropriation” to include anyone who knows or has reason to know of improper acquisition of a trade secret:

(5)the term “misappropriation” means—

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

(i) used improper means to acquire knowledge of the trade secret;

²⁸ See *PFS Distrib. Co. v. Raduechel*, 574 F.3d 580 (8th Cir. 2009) (discussing trade secret claim against commercial bank); William Lynch Schaller, *Growing Pains: Intellectual Property Considerations for Illinois Small Businesses Seeking to Expand*, 35 LOY. U. CHI. L.J. 845, 849-71 (2004) (collecting cases); Andrew F. Tuch, *Banker Loyalty in Mergers and Acquisitions*, 94 TEX. L. REV. 1080 (2016) (discussing duties of loyalty and confidentiality of investment banks in the wake of recent Delaware decisions).

²⁹ See, e.g., *Destiny Health, Inc. v. Connecticut Gen. Life Ins. Co.*, 39 N.E.3d 275 (Ill. App. Ct. 2015) (rejecting trade secret claim arising out of Connecticut General’s decision to choose another supplier after first seeing plaintiff’s secrets during deal due diligence).

³⁰ See Robert W. Hillman, *The Property Wars of Law Firms: Of Client Lists, Trade Secrets and the Fiduciary Duties of Law Partners*, 30 FLA. ST. U. L. REV. 767 (2003) (discussing potential trade secret liability in cases between law partners); *Maritrans GP, Inc. v. Pepper, Hamilton & Sheetz*, 602 A.2d 1277, 1280 (Pa. 1992) (affirming fiduciary duty injunction against law firm that had extensive access to Maritrans’ “complete inner-workings . . . along with Maritrans’ long-term objectives, and competitive strategies in a number of areas including the area of labor costs, a particularly sensitive area in terms of effective competition”—and then sought to represent Maritrans’ competitors in labor negotiations).

³¹ See, e.g., Elizabeth A. Rowe, *Rats, Traps, and Trade Secrets*, 57 B.C. L. REV. 381 (2016) (analyzing intersection of trade secrets, cybersecurity and cyber misappropriation by unknown or anonymous offenders); Dave Weinstein, *Hackers Hold Baltimore Hostage*, WALL ST. J., May 31, 2109, at A15 (noting “nameless and faceless criminals” have used ransomware to seize control of Baltimore’s municipal computers, causing an estimated \$18.2 million in damages, and referencing two Iranian hackers “who, beginning in 2015, allegedly unleashed ransomware on more than 200 victims, including municipal governments, state agencies and hospital networks in 43 states,” causing \$30 million in damages).

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake[.]³²

With nothing and no one categorically exempt, we have to look elsewhere for limits. One place worth initial consideration is the rule of lenity. The criminal and civil sections of the federal trade secret statute share the definitions of “trade secret” and “misappropriation” quoted above. This may require courts to narrowly construe the DTSA under the rule of lenity in cases of doubt, as the Supreme Court has held in other contexts.³³ The Supreme Court has shown

³² 18 U.S.C. § 1839(5) (2018).

³³ *See, e.g.*, *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004) (“Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies; *cf.* *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-518 (1992) (plurality opinion) (applying the rule of lenity to a tax statute, in a civil setting, because the statute had criminal applications and thus had to be interpreted consistently with its criminal applications).”); *accord* *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012) (en banc) (“Once we define the phrase [‘exceeds authorized access’] for the purpose of [Computer Fraud and Abuse Act] subsection 1030(a)(4), that definition must apply equally to the rest of the statute pursuant to the ‘standard principle of statutory construction . . . that identical words and phrases within the same statute should normally be given the same meaning.’ *Powerex Corp. v. Reliant Energy Servs., Inc.*, 551 U.S. 224, 232, 127 S. Ct. 2411, 168 L.Ed.2d 112 (2007).”); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (following *Leocal* and *Nosal*, invoking the rule of lenity because the CFAA has both criminal and civil applications, and therefore narrowly construing CFAA “without authorization” and “exceeds authorized access” provisions to exclude violations of restrictions on use, as opposed to violations of restrictions on access); Justin Levine, Note, *A Clash of Canons: Lenity, Chevron, and*

considerable interest in the rule of lenity in recent criminal cases,³⁴ and this sleepy issue could actually turn out to be quite significant in DTSA cases. As I explain later below,³⁵ “inevitable disclosure,” a theory that often applies even when employees unwittingly disclose or use secrets, may be inconsistent with the DTSA’s definition of “misappropriation,” requiring that the defendant “knows or has reason to know” of acquisition through improper means.³⁶ In addition, the DTSA’s definition limits “trade secret” to “financial, business, scientific, technical, economic or engineering information,” in contrast to the UTSA’s definition that potentially covers *all* information that otherwise meets its terms.³⁷ For example, would the DTSA cover details about President Trump’s supposed tryst with adult actress Stormy Daniels or the leaked law firm memos about CBS’ settlement with mainstream actress Eliza Dushku?³⁸ Is it true that others “can obtain economic value from the disclosure or use of [such] information” within the meaning of the DTSA? Would disclosure of such information be exempt from civil or criminal trade secret prosecution under the whistleblower immunity section of the DTSA? Would the DTSA’s whistleblower immunity provision —

the One-Statute, One-Interpretation Rule, 107 GEO. L.J. 1423 (2019) (reviewing *Leocal* and other precedents in the context of conflicting judicial and administrative agency interpretations of statutes having both criminal and civil provisions).

³⁴ See *United States v. Davis*, 139 S. Ct. 2319, 2333 (2019) (noting that the rule of lenity “is ‘perhaps not much less old than’ the task of statutory ‘construction itself’” and that the rule “is founded on ‘the tenderness of the law for the rights of individuals’ to fair notice of the law ‘and on the plain principle that the power of punishment is vested in the legislative, not in the judicial department’”); *Sessions v. Dimaya*, 138 S. Ct. 1204, 1244 (2018) (Thomas, J., dissenting) (noting that “lenity is a tool of statutory construction, which means States can abrogate it—and many have” and that “[l]enity, moreover, applies only to ‘penal’ statutes”).

³⁵ See *infra* Part III(D).

³⁶ See William Lynch Schaller, *Trade Secret Inevitable Disclosure: Substantive, Procedural & Practical Implications of an Evolving Doctrine (Part I)*, 86 J. PAT. & TRADEMARK OFF. SOC’Y 336 (May 2004) (discussing different versions of inevitable disclosure, including “pure” form that requires no bad acts or bad intent and allows injunctions based on inadvertent disclosure alone).

³⁷ Compare 18 U.S.C. § 1839(4) (2018) with UNIF. TRADE SECRET ACT WITH 1985 AMENDMENTS § 1(4) (UNIF. LAW COMM’N 1985), which provides:

§ 1(4) “Trade secret” means 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 to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and
- (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

³⁸ See Rebecca R. Ruiz, *Stormy Daniels’s Hush Money Lawsuit Is Dismissed by Judge*, N.Y. TIMES (March 7, 2019), <https://www.nytimes.com/2019/03/07/us/politics/trump-stormy-daniels-lawsuit-dismissed.html>; Rachel Abrams & John Koblin, *CBS Paid the Actress Eliza Dushku \$9.5 Million to Settle Harassment Claims*, N.Y. TIMES (Dec. 13, 2018), <https://www.nytimes.com/2018/12/13/business/media/cbs-bull-weatherly-dushku-sexual-harassment.html>.

which by its terms applies to civil or criminal liability only for disclosure of a “trade secret,” a defined term under both federal and state law³⁹ — protect disclosure of such information against non-trade secret claims like breach of fiduciary duty?⁴⁰ I would think the answer to some of these might be “no” if the rule of lenity compels a restricted reading of the term “trade secret.”⁴¹

II. RULE 12(B)(1) – JURISDICTION

Given the distinctly local character of some trade secret disputes, one has to wonder whether a narrow construction might be given to the DTSA’s provision permitting federal jurisdiction only when the misappropriated “trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.”⁴² This language is broader than the jurisdictional phrasing the Second Circuit confined under the rule of lenity in *United States v. Aleynikov*,⁴³ and it appears in the purely civil section of the DTSA, unlike the criminal code language at issue in *Aleynikov*. However, the DTSA’s civil “commerce” and “relatedness” language is identical to the criminal theft “commerce” and “relatedness” jurisdiction language in the EEA,⁴⁴ and Congress tucked the DTSA into the EEA,

³⁹ See William Lynch Schaller, *Illinois Trade Secret Law: The Peculiar Problem of Preemption*, 43 S. ILL. U. L. J. 243 (2019) (discussing variation among state trade secret statutes on whether they preempt all claims relating to competitively significant information or whether they just displace claims meeting the statutorily-defined term “trade secret”).

⁴⁰ Cf. Kristen Rasmussen, *Employer Responds to Qui Tam Suit with Fiduciary Duty Breach Claim Against Whistleblower*, CORPORATE COUNSEL (May 10, 2019), <https://www.law.com/corpcounsel/2019/05/10/employer-responds-to-qui-tam-suit-with-fiduciary-duty-breach-claim-against-whistleblower/?sreturn=20190411053359> (discussing complaint in *Wheeling Hospital, Inc. v. Longo*, 5:19-CV-32 (N.D. W. Va. Mar. 13, 2019) (Stamp, J.), in which hospital-employer alleged that whistleblower-executive breached his fiduciary duties by failing to internally report physician misconduct and by then using that information in an effort to extract a False Claims Act settlement from hospital); Peter S. Menell, *Tailoring a Public Policy Exception to Trade Secret Protection*, 105 CAL. L. REV. 1 (2017) (examining the historic interplay of trade secrecy protection and reporting of illegal activity).

⁴¹ See Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L. J. 829, 858-86 (2017) (discussing rule of lenity and other statutory construction rules that might be used in construing the DTSA).

⁴² 18 U.S.C. § 1836(b)(1) (2018).

⁴³ 676 F.3d 71, 79-82 (2d Cir. 2012) (reversing trade secret theft conviction; company’s internal computer code was not “related to or included in a product that [was] produced for or placed in interstate or foreign commerce” under the narrow construction demanded by the rule of lenity); *United States v. Agrawal*, 726 F.3d 235 (2d Cir. 2013) (reaching jurisdictional result contrary to *Aleynikov* on similar facts, over Judge Pooler’s dissent).

⁴⁴ See 18 U.S.C. §1832(a) (2018) (criminalizing theft of a trade secret “related to a product or service used in or intended for use in interstate or foreign commerce”); Conor Tucker, *The DTSA’s Federalism Problem: Federal Court Jurisdiction Over Trade Secrets*, 28 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1 (2017) (exploring the jurisdictional limits of the DTSA based on a careful parsing of its language and history, and emphasizing that the DTSA does not purport to reach the full extent of Congress’ power to regulate interstate commerce).

thereby bringing us right back to the rule of lenity calling for a narrow construction of terms shared in statutes with criminal and civil provisions. Will the rule of lenity apply to the DTSA's jurisdictional provision, given its location in the civil section of the EEA? Even if the rule of lenity does not apply, will this new language reach, say, a purely local trade secret fight between two Chicago doctors over a list of their Chicago patients?⁴⁵ Will the Supreme Court's new majority hold that such completely local interests fail to "substantially affect interstate commerce" for purposes of DTSA jurisdiction?⁴⁶

A separate jurisdictional tangle concerns inevitable disclosure. I work through this issue under the DTSA in detail much later below in the context of a specific case, *Molon Motor and Coil Corp. v. Nidec Motor Corp.*⁴⁷ For now, it is enough to say that most inevitable disclosure cases are brought as injunction actions to prevent unavoidable leaks by "the man (or woman) who knew too much," yet the DTSA explicitly forbids injunctions based "merely on the information the person knows."⁴⁸ If diversity jurisdiction does not exist and federal court jurisdiction is predicated exclusively on the DTSA, federal courts may lack subject matter jurisdiction in inevitable disclosure cases. Given this pleading configuration, attentive federal courts might disregard or strike inevitable disclosure allegations, block discovery, and then dismiss such DTSA cases pursuant to Rule 12(b)(1) or *sua sponte* as outside their limited jurisdictional authority.⁴⁹

⁴⁵ See *DLMC, Inc. v. Flores*, No. CV 18-00352 DKW-RT, 2019 WL 309754, at *2 (D. Haw. Jan. 23, 2019) (order granting motion to dismiss) (finding lack of interstate commerce connection and dismissing healthcare firm's DTSA action against ex-employee for customer list misappropriation where all involved were from Hawaii); *Aurora Internal Medicine, Ltd. v. Moore*, 2011 IL App (2d) 101042-U (non-precedential order affirming finding that patient list was a trade secret in litigation exclusively among local Illinois doctors); *Prentice Medical Corp. v. Todd*, 495 N.E.2d 1044 (Ill. App. Ct. 1986) (patient list was a trade secret that registered nurse misappropriated from local medical practice); Sara Ghantous, *Making the List: What Does It Take to Make a Patient List a Trade Secret?*, 18 J. MARSHALL REV. INTEL. PROP. L. 83, 86 n.19 (2018) (internal citation omitted) (noting federal jurisdiction language in 18 U.S.C. § 1836(b)(1)).

⁴⁶ *United States v. Lopez*, 514 U.S. 549, 559 (1995). See also Robert J. Pushaw, Jr., *Enforcing Principled Constitutional Limits on Federal Power: A Neo-Federalist Refinement of Justice Cardozo's Jurisprudence*, 60 WM. & MARY L. REV. 937, 962 (2019) ("The Rehnquist and Roberts Courts have been unwilling to overrule this [*Wickard v. Filburn*, 317 U.S. 111 (1942)] precedent, which has stymied their efforts to impose meaningful originalist restrictions on the Commerce Clause."); Martin J. Salvucci, Note, *A Federalist Account of the Law of Trade Secrecy*, 29 STAN. L. & POL'Y REV. 183, 191-99 (2018) (discussing jurisdictional implications of the DTSA's "commerce" and "relatedness" requirements).

⁴⁷ No. 16-C-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

⁴⁸ 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2018).

⁴⁹ See, e.g., *Gov't Employees Ins. Co. v. Nealey*, 262 F. Supp. 3d 153, 172, 173 (E.D. Pa. 2017) (noting federal court's duty to *sua sponte* consider its jurisdiction, discussing legislative history of DTSA jurisdiction provision, and holding: "GEICO's complaint does not allege any nexus between interstate or foreign commerce and the alleged trade secrets contained within the Antonacci affidavit. This deficiency, in itself, warrants dismissal of plaintiffs' DTSA claim.").

Timing presents another, though more modest, jurisdictional issue. The DTSA expressly states it applies only to claims arising on or after its effective date, May 11, 2016, or begun before and continuing after that date.⁵⁰ This raises a question: Does a claim “arise” when the theft takes place, or is a new claim triggered each time a defendant discloses or uses the stolen secret? The DTSA’s three-year statute of limitations, found in Section 1836(d), states that “[f]or purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation,”⁵¹ but by its terms, this language is limited to “this subsection.” Some courts have held that continued use after the DTSA’s enactment implicates the DTSA, even when the original misappropriation occurred before May 11, 2016.⁵² *Molon Motor*, which I discuss more fully below in connection with “identification,” “misappropriation” and “knowledge,” went so far as to extend the trade secret “inevitable disclosure” doctrine to find continuous use after the DTSA’s effective date.⁵³ This jurisdictional timing problem will fade as new acts of misappropriation take place well after the DTSA’s passage, but in these first few years a limited subset of pending cases may turn on it.

III. RULE 12(B)(6) – FAILURE TO STATE A CLAIM

The pro-defendant policy animating the rule of lenity should carry over to assessment of DTSA claims at the threshold stage of a Rule 12(b)(6) motion to dismiss. While courts use varying formulations to describe trade secret claim elements,⁵⁴ whether under the DTSA or state law, all amount to requiring (1) a

⁵⁰ Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376, 381-82 (2016) (“(e) EFFECTIVE DATE.—The amendments made by this section shall apply with respect to any misappropriation of a trade secret (as defined in section 1839 of title 18, United States Code, as amended by this section) for which any act occurs on or after the date of the enactment of this Act.”).

⁵¹ 18 U.S.C. § 1836(d) (2018). *Cf.* *Allied Erecting & Dismantling Co. v. Genesis Equipment & Mfg., Inc.*, 805 F.3d 701, 705 (6th Cir. 2015) (applying Ohio law) (trade secret claim against a given defendant arises only once, at the time of misappropriation, subject to the discovery rule).

⁵² *See, e.g.,* *Teva Pharm. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 674-75 (E.D. Pa. 2018) (observing that “one who acquired and used a trade secret before enactment of the DTSA and continues to use it after enactment is liable”); *Yeiser Research & Dev. LLC v. Teknor Apex Co.*, 281 F. Supp. 3d 1021, 1057 (S.D. Cal. 2017) (DTSA applies to the misappropriation of trade secrets before its enactment date “as long as the misappropriation continues to occur after the enactment date”).

⁵³ *Molon Motor and Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531 at *7 (N.D. Ill. May 11, 2017) (motor design and quality control trade secrets allegedly misappropriated in June 2013 would not necessarily become stale quickly, and thus it was plausible defendant would continue to use them after the DTSA’s effective date in May 2016).

⁵⁴ *See, e.g.,* *Raytheon Co. v. Indigo Systems Corp.*, 895 F.3d 1333, 1339 (Fed. Cir. 2018) (applying California law) (“Raytheon was required to prove, among other things: (1) it owned a trade secret; and (2) Indigo misappropriated the trade secret, either by acquisition, use, or disclosure.”); *Sargent Fletcher, Inc. v. Able Corp.*, 110 Cal. App. 4th 1658, 1665 (2003) (“Under the UTSA, a prima facie claim for misappropriation of trade secrets requires the plaintiff

trade secret, (2) misappropriation, and (3) actual use or disclosure, or at least threatened use or disclosure.⁵⁵ Courts have occasionally pared down the elements to just two or have even dispensed with explicit elements altogether, as in *Plastronics Socket Partners Ltd. v. Highrel Inc.*,⁵⁶ where the district court framed the Arizona state law test as having two parts – “(1) the existence of a trade secret and (2) actual or threatened misappropriation” – and then implicitly applied the same two-part test to the DTSA claims without announcing a distinct federal standard. Regardless of how the elements are expressed, the Supreme Court’s decisions in *Bell Atlantic Corp. v. Twombly*⁵⁷ and *Ascroft v. Iqbal*⁵⁸ hold that to withstand a Rule 12(b)(6) motion to dismiss, a complaint must offer sufficient factual matter to state a claim that is “plausible on its face.”⁵⁹ But what does this really mean in the trade secret context?⁶⁰

A. TWOMBLY, IQBAL AND EQUIPOISE

Actually, it should mean a lot. I can capture the concern in a single word: equipoise. In law, as in medicine, equipoise is defined as an equal balance of interests.⁶¹ Simply put, to avoid losing, a plaintiff must allege some fact which, if believed, makes it more likely than not a wrong has been committed.⁶² Conduct as consistent with innocence as with guilt — a tie — is not enough; it leaves

to demonstrate: (1) the plaintiff owned a trade secret, (2) the defendant acquired, disclosed, or used the plaintiff’s trade secret through improper means, and (3) the defendant’s actions damaged the plaintiff.”).

⁵⁵ See, e.g., *Learning Curve Toys, Inc. v. PlayWood Toys, Inc.*, 342 F.3d 714, 728 (7th Cir. 2003) (applying Illinois Trade Secrets Act).

⁵⁶ No. CV-18-03201-PHX-SMB, 2019 WL 2054362 at *2 (D. Ariz. May 9, 2019).

⁵⁷ 550 U.S. 544 (2007).

⁵⁸ 556 U.S. 662 (2009).

⁵⁹ *Iqbal*, 556 U.S. at 678.

⁶⁰ See Daniel A. Epstein, *How Probable Is “Plausible”?*, 86 U. CHI. L. REV. ONLINE 34 (2018) (offering a theoretical model assigning probabilities and expected values to Rule 12(b)(6) motions to dismiss under *Twombly* and *Iqbal*); Bradley Lipton, Comment, *Trade Secret Law and the Changing Role of Judge and Jury*, 120 YALE L.J. 955 (2011) (arguing *Twombly* and *Iqbal* suggest stricter scrutiny of trade secret claims at the summary judgment stage, but overlooking the more direct impact of those Supreme Court cases on Rule 12(b)(6) attacks on trade secret claims).

⁶¹ See, e.g., Burt I. Huang, *The Equipoise Effect*, 116 COLUM. L. REV. 1595 (2016) (discussing equipoise in the legal remedies context); Chad Cook & Charles Sheets, *Clinical Equipoise and Personal Equipoise: Two Necessary Ingredients for Reducing Bias in Manual Therapy Trials*, 19 J. MANUAL & MANIPULATIVE THERAPY 55 (2011) (“Clinical and personal equipoise exists when a clinician has no good basis for a choice between two or more care options or when one is truly uncertain about the overall benefit or harm offered by the treatment to his/her patient.”).

⁶² Cf. *Director, Office of Workers’ Comp. Programs v. Greenwich Collieries*, 512 U.S. 267, 272 (1994) (“Burden of proof was frequently used to refer to what we now call the burden of persuasion—the notion that if the evidence is evenly balanced, the party that bears the burden of persuasion must lose.”).

the parties in equipoise.⁶³ Indeed, the Supreme Court in *Twombly* and *Iqbal* actually put it in these terms: “Where a complaint pleads facts that are ‘merely consistent with’ a defendant’s liability, it ‘stops short of the line between possibility and plausibility of ‘entitlement to relief.’”⁶⁴

A great many trade secret cases fit this description all too painfully, since virtually all trade secret cases involve someone with past access to secrets embarking on a course that could conceivably, but not necessarily, result in unauthorized use or disclosure of those secrets. Without something more, without some “trigger” fact, the parties stand in equipoise and a lawsuit is not justified.⁶⁵ In such cases, to borrow from the Seventh Circuit’s famous trade secret opinion in *PepsiCo, Inc. v. Redmond*, “[a]ll that is alleged, at bottom, is that defendants could misuse plaintiff’s secrets, and plaintiffs fear they will. This is not enough. It may be that little more is needed, but falling a little short is still falling short.”⁶⁶

Although the Supreme Court did not use the word, equipoise was very much on the Court’s mind in *Twombly*, an antitrust case involving parallel conduct of competitors. Indeed, this context prompted the Court’s most famous passages in *Twombly*:

In applying these general standards to a § 1 claim, we hold that stating such a claim requires a complaint with enough factual matter (taken as true) to suggest that an agreement was made. Asking for plausible grounds to infer an agreement does not impose a probability requirement at the pleading stage; it simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of illegal agreement. And, of course, a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable, and “that a recovery is very remote and unlikely.” [*Id.*] In identifying facts that are suggestive enough to render a § 1 conspiracy plausible, we have the benefit of the prior rulings and considered views of leading commentators, already quoted, that lawful parallel conduct fails to be-speak unlawful agreement. It makes sense to say, therefore, that an allegation of parallel conduct and a bare assertion of conspiracy will not suffice. Without more, parallel conduct does not suggest conspiracy, and a conclusory allegation of

⁶³ *Cf.* *United States v. Hoffman*, 901 F.3d 523 (5th Cir. 2018)(in criminal cases the “equipoise rule” means no rational factfinder could find guilt beyond a reasonable doubt), *cert. denied*, 139 S. Ct. 2615 (2019).

⁶⁴ *Iqbal*, 556 U.S. at 678 (quoting *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 557 (2007)).

⁶⁵ See William Lynch Schaller, Russell Beck & Randall E. Kahnke, *Trade Secret “Triggers”: What Facts Warrant Litigation?*, 19 SEDONA CONF. J. 625, 660 (2018) (explaining equipoise under *Twombly* and *Iqbal* in the trade secret misappropriation context).

⁶⁶ *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1268-69 (7th Cir. 1995) (quoting *Teradyne, Inc. v. Clear Commc’ns Corp.*, 707 F. Supp. 353, 357 (N.D. Ill. 1989)).

agreement at some unidentified point does not supply facts adequate to show illegality. Hence, when allegations of parallel conduct are set out in order to make a § 1 claim, they must be placed in a context that raises a suggestion of a preceding agreement, not merely parallel conduct that could just as well be independent action.

The need at the pleading stage for allegations plausibly suggesting (not merely consistent with) agreement reflects the threshold requirement of Rule 8(a)(2) that the “plain statement” possess enough heft to “sho[w] that the pleader is entitled to relief.” A statement of parallel conduct, even conduct consciously undertaken, needs some setting suggesting the agreement necessary to make out a § 1 claim; without that further circumstance pointing toward a meeting of the minds, an account of a defendant’s commercial efforts stays in neutral territory. An allegation of parallel conduct is thus much like a naked assertion of conspiracy in a § 1 complaint: it gets the complaint close to stating a claim, but without some further factual enhancement it stops short of the line between possibility and plausibility of “entitle[ment] to relief.” Cf. *DM Research, Inc. v. College of Am. Pathologists*, 170 F.3d 53, 56 (1st Cir.] 1999) (“[T]erms like ‘conspiracy,’ or even ‘agreement,’ are border-line: they might well be sufficient in conjunction with a more specific allegation—for example, identifying a written agreement or even a basis for inferring a tacit agreement, . . . but a court is not required to accept such terms as a sufficient basis for a complaint”).

We alluded to the practical significance of the Rule 8 entitlement requirement in *Dura Pharmaceuticals, Inc. v. Broudo*, 544 U.S. 336 (2005), when we explained that something beyond the mere possibility of loss causation must be alleged, lest a plaintiff with “a largely groundless claim” be allowed to “take up the time of a number of other people, with the right to do so representing an *in terrorem* increment of the settlement value.” *Id.*, at 347 (quoting *Blue Chip Stamps v. Manor Drug Stores*, 421 U.S. 723, 741 (1975)). So, when the allegations in a complaint, however true, could not raise a claim of entitlement to relief, “this basic deficiency should . . . be exposed at the point of minimum expenditure of time and money by the parties and the court.” 5 Wright & Miller § 1216, at 233-234 (quoting *Daves v. Hawaiian Dredging Co.*, 114 F. Supp. 643, 645 ([D. Hawaii] 1953)); see also *Dura*, *supra*, at 346; *Asabi Glass Co. v. Pentech Pharmaceuticals, Inc.*, 289 F. Supp. 2d 986, 995 ([N.D.] Ill. 2003) (Posner, J., sitting

by designation) (“[S]ome threshold of plausibility must be crossed at the outset before a patent antitrust case should be permitted to go into its inevitably costly and protracted discovery phase.”).⁶⁷

Federal court trade secret misappropriation pleading presents complexities comparable to those plaguing antitrust pleading under *Twombly*. First, direct proof is in short supply in both settings. Second, conspiracies are common if not the norm in both situations. Third, the line between fair and unfair competition is often barely discernable in both. Fourth, both generate enormous expense because of legal, factual, and discovery complications and thus produce more than their fair share of *in terrorem* settlement value.⁶⁸ These difficulties, however, do not excuse improper pleading in trade secret cases any more than they excuse it in antitrust cases. If anything, a powerful argument can be made that strict adherence to *Twombly* is even more important in trade secret cases because thousands of people jump ship to competitors every day, prompting hundreds of trade secret lawsuits each year⁶⁹ — a number that has increased significantly with the passage of the DTSA.⁷⁰ By comparison, antitrust violations and

⁶⁷ *Twombly*, 550 U.S. at 556-58 (footnotes omitted); cf. *Comcast Corp. v. Nat’l Assoc. African American-Owned Media*, 140 S. Ct. 1009, 1014 (2020) (examining “but for” tort causation requirement as an element of 42 U.S.C. § 1981 claims: “[T]o determine what the plaintiff must plausibly allege at the outset of a lawsuit, we usually ask what the plaintiff must prove in the trial at its end.”).

⁶⁸ See, e.g., *SKF USA Inc. v. Bjerknæs*, Nos. 08 C 4709, 09 C 2232, 2011 WL 4501395 (N.D. Ill. Sept. 27, 2011) (awarding plaintiff over \$1 million in fees under the Illinois Trade Secrets Act based on 2,700 hours billed for successful injunction work against ex-employee, even though plaintiff only won compensatory damages of \$41,068 and punitive damages of \$40,000, and even though plaintiff rejected multiple settlement offers higher than plaintiff’s ultimate monetary recovery); James H. Pooley, *The Uniform Trade Secrets Act: California Civil Code 3426*, 1 SANTA CLARA HIGH TECH L.J. 193, 203 (1985) (“Trade secret litigation is very expensive and disruptive, especially for the start-up technology company which must struggle to achieve credibility with customers, employees and sources of financing. As a result, trade secret lawsuits are very effective in the hands of unscrupulous plaintiffs who would pursue a claim not to achieve protection of a legitimate trade secret, but simply to harass and possibly destroy a new competitor.”).

⁶⁹ See David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum, & Jill Weader, *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 69 (2010) (study finding almost 60% of trade secret cases involved departing employees and more than 30% involved divorcing business owners).

⁷⁰ See Rachel Bailey, *Lex Machina: Trade Secret Litigation Report 2018* at 3, Lex Machina (July 2018), https://www.gordonrees.com/Templates/media/files/pdf/Trade_Secret_Litigation_Report_2018.pdf (“Trade Secret case filings in federal district court were steady at around 900 cases per year until 2017, when filings increased sharply by over 30% over the previous year. A significant factor for this increase is likely the passing of the Defend Trade Secrets Act [.]”).

antitrust litigation, though profoundly important, are far less common.⁷¹ The case for *Twombly* vigilance in trade secret cases is all the more compelling when one considers that most departing employees and divorcing business owners have only modest means to fund litigation defense costs compared to the far deeper pockets of antitrust defendants.

Unfortunately, with the exception of statutes of limitations questions, federal appeals courts have seldom published opinions exploring trade secret pleading issues under *Twombly/Iqbal*,⁷² and they have yet to do so in the DTSA context.⁷³ One of the few, indeed the only one I can find on general pleading issues, *ABB Turbo Systems AG v. TurboUSA, Inc.*,⁷⁴ was a pre-DTSA case under Florida law involving a misappropriation scam spanning twenty years. Defendant Hans Franken left plaintiff ABB in 1986 to found rival firm TurboNed, and later founded sister firm TurboUSA in the 1990s. According to the complaint, “[f]or more than twenty years, from 1986 until the sale of TurboNed to a third party in 2009, Hans Franken and employees of TurboNed paid at least one ABB employee for confidential information related to ABB parts, servicing, and pricing.”⁷⁵ The stolen ABB information was later passed along to TurboUSA, and in 2008 TurboUSA hired another former ABB employee who had stolen still more ABB trade secrets before quitting.⁷⁶ TurboNed employees thereafter

⁷¹ See *Civil Antitrust Litigation Continues to Decline*, TRAC REPORTS (June 2019), <https://trac.syr.edu/tracreports/civil/563/> (reporting 567 federal court antitrust suits in 2018, with a projected decline to 536 suits in 2019). In rare instances trade secret misappropriation and antitrust claims can even intersect, as in *Premier Comp Solutions LLC v. UPMC*, 377 F. Supp. 3d 506, 538 (W.D. Pa. 2019) (misappropriation of trade secrets did not constitute per se violation of the Sherman Act).

⁷² See, e.g., *Tension Envelope Corp. v. JBM Envelope Co.*, 876 F.3d 1112, 1122–23 (8th Cir. 2017) (applying Missouri law) (affirming Rule 12(b)(6) dismissal of trade secret claims and holding that the “identity of [Tension’s] customers and their unique requirements” were not protectable trade secrets, with no discussion of *Twombly* or *Iqbal*).

⁷³ See *Coda Dev. S.R.O. v. Goodyear Tire & Rubber Co.*, 916 F.3d 1350, 1351 (Fed. Cir. 2019) (applying Ohio law) (trade secret misappropriation statute of limitations dismissal determination from face of complaint reversed); *Brand Coupon Network, LLC v. Catalina Mktg. Corp.*, 748 F.3d 631 (5th Cir. 2014) (applying Louisiana law) (noting that the district court’s dismissal of plaintiff’s trade secret claim, on statute of limitations grounds, was not appealed by plaintiff); *Cygnus Telecomms. Tech., LLC v. Telesys Comms., LLC*, 536 F.3d 1343, 1344 (Fed. Cir. 2008) (applying Minnesota law) (affirming Rule 12(b)(6) dismissal of trade secret claim based on statute of limitations defense apparent from face of complaint); Michelle Evans, *Plausibility Under the Defend Trade Secrets Act*, 16 J. MARSHALL REV. INTELL. PROP. L. 188 (2017) (citing no federal appellate cases discussing Rule 12(b)(6) dismissal of trade secret claims); Ronald T. Coleman, Jr., *Pleading Plausible Trade-Secret Claims under Twombly and Iqbal*, AMERICAN BAR ASSOCIATION (May 20, 2014), <https://www.americanbar.org/groups/litigation/committees/intellectual-property/articles/2014/pleading-plausible-trade-secret-claims-under-twombly-iqbal/> (citing no federal appellate cases discussing Rule 12(b)(6) dismissal of trade secret claims).

⁷⁴ 774 F.3d 979 (Fed. Cir. 2014).

⁷⁵ *Id.* at 982.

⁷⁶ *Id.* at 983.

“altered confidential ABB documents in their possession to obscure references to ABB, in part to conceal the source of the information, in connection with the sale of TurboNed to a new owner in 2009.”⁷⁷ TurboNed and TurboUSA were named as defendants since they were under Hans Franken’s control at all relevant times, and Hans’ son Willem, TurboUSA’s manager, was joined as a defendant as well. The district court dismissed the complaint, ruling that ABB was on sufficient inquiry notice to trigger the statute of limitations barring ABB’s claims and (somewhat inconsistently) that ABB could not have used reasonable secrecy efforts given ABB’s failure to discover the theft scheme for decades.

The Federal Circuit reversed, holding that both the statute of limitations defense and the reasonableness of ABB’s alleged secrecy measures could not be definitively determined on a *Twombly* Rule 12(b)(6) motion. On the limitations question, the Court of Appeals thought defendants’ secret payments and acquisition concealment efforts spoke for themselves, and “nothing in the amended complaint ma[de] clear that the trade secrets were the kind that would readily reveal themselves in the marketplace conduct of the users of the information.”⁷⁸ These circumstances went beyond “conclusory” and “factually neutral” to make ABB’s lack of actual or constructive discovery affirmatively plausible for *Twombly* purposes, the Federal Circuit held, although it stressed that ABB didn’t even have to satisfy *Twombly* to survive the limitations dismissal motion: “It is enough that ABB’s amended complaint certainly does not state facts making apparent that ABB actually or constructively discovered the alleged misappropriations by June 2009.”⁷⁹

The reasonableness of ABB’s secrecy measures was equally easy to resolve. After listing the measures ABB alleged,⁸⁰ the appeals court noted that the complaint stage is not well-suited for determining what secrecy steps are reasonable in a given context.⁸¹ It then rejected the district court’s rationale that it was “highly unlikely” ABB was “actually restricting physical and electronic access to the information and taking other protective measures” in light of the repeated

⁷⁷ *Id.* at 982.

⁷⁸ *Id.* at 985-86.

⁷⁹ *Id.* at 986.

⁸⁰ *Id.* at 986 (ABB’s secrecy measures “include[ed] imposing confidentiality and nondisclosure obligations on ABB employees that have access to ABB’s Turbocharger Trade Secrets, marking documents constituting ABB’s Turbocharger Trade Secrets with confidentiality designations and/or other indicia prohibiting the reproduction or dissemination of such documents or information to third parties, [and] restricting physical and electronic access by third parties to ABB’s Turbocharger Trade Secrets”)(internal citation omitted)(alteration in original).

⁸¹ *Id.* at 986-87 (citing *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179 (7th Cir. 1991) (Posner, J.) (“[O]nly in an extreme case can what is a ‘reasonable’ precaution be determined on a motion for summary judgment, because the answer depends on a balancing of costs and benefits that will vary from case to case and so require estimation and measurement by persons knowledgeable in the particular field of endeavor involved.”)(alteration in original)).

thefts:

Protections may be legally adequate to confer legal status as secrets, but still not perfectly prevent misappropriation. Indeed, trade-secret law is premised on that possibility; there would be no actionable misappropriation otherwise. Moreover, once the protections are overcome by those engaged in misappropriation, detectability turns on the acts of the miscreants, such as their furtiveness and concealment efforts. But those acts have no particular bearing on whether the actions of the secret owner in seeking to protect against disclosure were adequate. The sheer number and scope of misappropriations, considered apart from detectability, may well have a logical bearing on assessing the reasonableness of protective measures. But that presents a classic factual question turning on the details of the misappropriations. It cannot be answered by judicial assessment at the complaint stage in this case.

ABB's specific factual allegations of protective measures are enough to survive a motion to dismiss. To be sure, *Twombly* and *Iqbal* indicate that, in separating conclusions from facts and deciding whether the alleged facts make affirmatively plausible the asserted basis of liability, *Twombly*, 550 U.S. at 557 n.5 . . . courts deciding a motion to dismiss for insufficient pleading may consider the strength of alternative explanations of the alleged facts. *See Twombly*, 550 U.S. at 567-68. . . (claim of parallel business conduct not enough to support conspiracy claim where no facts alleged that suggested reason something other than individual self-interest); *Iqbal*, 556 U.S. at 681-82 . . . (claim of discriminatory policy insufficient where no official communications or other facts alleged beyond allegation of disproportionate effect on Arab Muslim men from investigation of 9/11 attacks carried out by Arab Muslim men). But such consideration is limited, because the court's role is only to determine if the factual allegations go beyond being "merely consistent with" liability to "plausibly suggest[ing]" liability. *Twombly*, 550 U.S. at 557 . . . Making that distinction requires a "context-specific" assessment of the particular complaint, *Iqbal*, 556 U.S. at 679, . . . made with the recognition that "a well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of the facts alleged is improbable," *Twombly*, 550 U.S. at 556, . . . In this

case, for the reasons given, the factual allegations meet the pleading standard regarding protection of the alleged trade secrets.⁸²

I am particularly interested in two issues raised on appeal but not addressed by the district court: (1) whether ABB alleged sufficient facts to show its secrets had “economic value” and (2) whether ABB alleged sufficient facts to show defendants TurboUSA and Willem Franken (as opposed to defendants TurboNed and Hans Franken) had the “knowledge of the misappropriations required for liability,”⁸³ a reference to the “knew or had reason to know” standard set forth in the “misappropriation” definition found in the UTSA (and now found in the DTSA). The Federal Circuit noted but did not comment on ABB’s “economic value” allegations, which claimed its secrets were not susceptible to reverse engineering and were the subject of significant investment for creation and protection, but the Court of Appeals did comment on ABB’s “knowledge” allegations, which suggested Hans Franken exerted control over TurboUSA (and presumably over his son Willem). Without deciding the sufficiency of the pleadings on this knowledge issue, the Federal Circuit noted:

[T]he importance of a “context-specific” application of Rule 8, *Iqbal*, 556 U.S. at 679, . . . and the particular need to apply the plausibility standard with a recognition that direct evidence of some facts—such as guilty knowledge, in some cases—may be distinctively in the defendant’s possession, requiring that the threshold standard of plausibility be applied to more circumstantial evidence. See *Matrixx Initiatives, Inc. v. Siracusano*, [563 U.S. 27, 49 & n.15] (2011) (holding, even under a special statutory heightened pleading standard requiring a “strong inference” of scienter, that plaintiff’s claim could not be dismissed where it pleaded facts “sufficient to render the inference of scienter at least as compelling as the inference” of innocent conduct; and stating that determining guilty knowledge requires courts to review “all the allegations holistically” (quotation marks and citation omitted)); *Lamm v. State Street Bank & Trust*, 749 F.3d 938, 945 (11th Cir. 2014) (finding insufficient pleading in a particular case after noting: “We are also mindful of the challenge a plaintiff faces in establishing a defendant’s mental state without the benefit of discovery.”); Honorable Mark R. Kravitz, *Report of the Civil Rules Advisory Committee* 53 (May 2, 2011) (“How much fact is required to support a reasonable inference of liability varies with context, and in many types of action can be rather scant.”); *McCauley v.*

⁸² *Id.* at 987-88.

⁸³ *Id.* at 988.

City of Chicago, 671 F.3d 611, 619 n.2 (7th Cir. 2011) (highlighting commentary).⁸⁴

I dwell on *ABB Turbo Systems* because it's the only appellate precedent we have to measure trade secret allegations under *Twombly* and *Iqbal*. As I show below, *ABB Turbo Systems* foreshadowed a number of important trade secret pleading issues under the DTSA, not least “reasonable [secrecy] measures” and “economic value” when alleging a trade secret, and “knew or had reason to know” when alleging misappropriation.⁸⁵ The *ABB Turbo Systems* framework should be kept in mind as we work through *Plastronics* and *Molon Motor*, two pleading cases I give close consideration below.

B. ALLEGING A TRADE SECRET

Plastronics focused exclusively on the first element, the existence of a trade secret, so it is a good place to start, even though it did not cite *ABB Turbo Systems*. The scenario was standard: two employees, one of whom was *Plastronics*' Chief Technology Officer, quit to form a rival.⁸⁶ Although establishing a protectable trade secret in a complaint should be routine, plaintiff in *Plastronics* failed to sufficiently identify the secret at issue and struggled to allege the statutory element of “economic value” embedded in both the Arizona and DTSA definitions of “trade secret.”⁸⁷ The *Plastronics* court ruled that plaintiff's complaint at least needed to identify the secrets in issue by category or by reference to documents containing them. The court also rejected plaintiff's bare recital of the statutory definition of economic value; no facts were alleged to show how or why *Plastronics*' vague information had independent economic value by virtue of not being generally known in the industry. However, the court did uphold plaintiff's “reasonable secrecy measures” allegations based solely on the ex-employees' confidentiality agreements with *Plastronics*.⁸⁸ The *Plastronics* court's rulings at first blush seem to be consistent with the notice-pleading purpose of Rule 8(a) and the issue-narrowing function of Rule 12(b)(6) as glossed by *Twombly* and *Iqbal*,⁸⁹ but these rulings deserve a closer look.

⁸⁴ *Id.* at 988-89.

⁸⁵ 18 U.S.C. § 1839(3)(A)–(B), (5)(B)(ii) (2018).

⁸⁶ *Plastronics Socket Partners Limited v. Highrel Inc.*, No. CV-18-03201-PHX-SMB, 2019 WL 2054362 at *1 (D. Ariz. May 9, 2019).

⁸⁷ *Id.* at *2-*4 (citing ARIZ. REV. STAT. ANN. § 44-401(4)(b); 18 U.S.C. § 1839(3)(B) (2018)).

⁸⁸ *Id.* at *4.

⁸⁹ See Rebecca Love Kourlis, Jordan M. Singer, & Natalie Knowlton, *Reinvigorating Pleadings*, 87 DENVER U.L. REV. 245, 262 (2010) (“From our perspective, the degree of departure from prior caselaw—and even whether the ‘plausibility’ standard [in *Twombly* and *Iqbal*] is the right one—is less important than the unmistakable message of both cases that the issue-narrowing function of current pretrial procedure is broken. The Court's announcement of a ‘plausibility’ standard for pleadings was an overt admission that the long-held assumption that discovery could compensate for the loss of issue-narrowing at the pleadings stage is simply not true for

C. IDENTIFICATION

Every case must start somewhere, and the place to start is with the one thing plaintiff knows: its secrets. Indeed, the existence of a trade secret is an indispensable element of every trade secret claim.⁹⁰ Every trade secret complaint, therefore, should specifically identify the secret(s) the plaintiff initially claims to be in issue, even if additional secrets turn out to have been stolen. This provides a fixed target for trade secret discovery.⁹¹ But insisting on pleading trade secret identity with specificity does more: it prevents plaintiff from using vaguely described secrets as a means to bully competitors through baseless litigation and lays down a marker to measure plaintiff's shifting descriptions of its secrets for sanction purposes.⁹² After all, as part of its reasonable secrecy measures, the owner should have been cataloging its secrets⁹³ and monitoring their use long before a lawsuit,⁹⁴ and simple fairness dictates that employees and other

at least some types of cases.”); Yoichiro Hamabe, *Functions of Rule 12(b)(6) in the Federal Rules of Civil Procedure: A Categorization Approach*, 15 CAMPBELL L. REV. 119, 127 (1993) (lamenting notice-pleading regime before *Twombly* and *Iqbal* and arguing, presciently, that Rule 12(b)(6) can eliminate or narrow “issues concerning substantive law or sufficiency of the complaint which would promote a resolution on the merits, or disposing of an unmeritorious claim”).

⁹⁰ See Julie A. Henderson, *The Specifically Defined Trade Secret: An Approach to Protection*, 27 SANTA CLARA L. REV. 537, 550 (1987) (“In the context of trade secret litigation, proof of the existence of a trade secret has been characterized as the ‘sine qua non’ of a misappropriation claim.”) (quoting MELVIN JAGER, TRADE SECRETS LAW §5.02 (1985)).

⁹¹ See, e.g., *Imax Corp. v. Cinema Tech., Inc.*, 152 F.3d 1161, 1164-68 (9th Cir. 1998) (summary judgment decision discussing without deciding Imax’s need to identify its projector system’s “dimensions and tolerances” trade secrets with particularity under California law, as set forth in Cal. Civ. Code §3426.1(d)); *Combined Metals of Chi. Ltd. P’ship v. Airtek, Inc.*, 985 F.Supp. 827, 832 (N.D. Ill. 1997) (ruling that disputes concerning scope of trade secret would not be tolerated beyond pleading stage).

⁹² See *DeRubeis v. Witten Tech., Inc.*, 244 F.R.D. 676, 680 (N.D. Ga. 2007) (“[I]f discovery on the defendant’s trade secrets were automatically permitted, lawsuits might regularly be filed as ‘fishing expeditions’ to discover the trade secrets of a competitor.”) (quoting Kevin R. Casey, *Identification of Trade Secrets during Discovery: Timing and Specificity*, 24 AIPLA Q.J. 191, 204 (1996)); *Cypress Semiconductor Corp. v. Maxim Integrated Products, Inc.*, 236 Cal. App. 4th 243, 255 (2015) (confronted with trade secret identification discovery concerning its alleged in-house list of employees working on touchscreen technology, plaintiff Cypress voluntarily dismissed its misappropriation complaint; court nevertheless sanctioned Cypress with a fee award of over \$180,000, rejecting Cypress’ appeal as “a kind of carnival fun house in which the facts of the case are distorted into grotesque and nearly unrecognizable shapes”).

⁹³ See R. Mark Halligan, *The Next Revolution in Intellectual Property Law: Automated Trade Secret Asset Management*, LANDSLIDE, May/June 2019, at 10–12 (discussing automation options for recording and maintaining secrets).

⁹⁴ See *GE Betz, Inc. v. Moffitt-Johnston*, 885 F.3d 318, 322 (5th Cir. 2018) (“GE installs monitoring software on the computers of all GE employees, which captures and logs certain actions taken, including emails sent and files copied to external hard drives. According to a report generated by the software on Moffitt-Johnston’s computer (the DLP report), on September 24, 2012, days after she announced her resignation, someone using Moffitt-Johnston’s computer downloaded over 27,000 files to an external hard drive . . . Subsequently, on October 9, 2012, another download was attempted to the same external hard drive but was blocked

authorized users should have been put on notice as to concrete, identifiable information they were not permitted to copy or take with them for their own purposes as part of their general skill and knowledge.⁹⁵ As Professor Deepa Varadarajan has observed:

[C]lear communication or notice about one's claim to property is important because it helps facilitate trade, minimizes conflict over resources, and prevents wasted labor by others.

....

... In trade secret law, these concerns take on an additional dimension because insufficient notice about the boundaries of trade secrets can impact employee mobility and freedom. If employees cannot discern the boundaries of trade secret-protected

by exit controls that had been installed on Moffitt-Johnston's computer in the interim . . . Additionally, according to the DLP report, in the days prior to her departure, Moffitt-Johnston sent GE files via email to herself at outside email addresses.”); *United States v. Aleynikov*, 785 F. Supp. 2d 46, 51 (S.D.N.Y. 2011) (“Goldman Sachs has implemented many security measures to maintain the secrecy of its high frequency trading system. In order to protect the firm’s computer systems from intrusion, the firm maintains a fire-wall. It monitors its employees’ use of internet sites and also blocks access to certain websites. A banner that appears whenever employees log in to their computers advises them of prohibited uses of the internet and accepted behaviors. Access to Goldman Sachs’ buildings is restricted to employees with proper identification cards; access to firm computers is also restricted. Only those few employees with administrative access, including Aleynikov at the time of his employment with the firm, are permitted to use USB flash drives.”).

⁹⁵ See *GlobalTap LLC v. Elkay Mfg. Co.*, No. 13 C 632, 2015 WL 94235 at *6 (N.D. Ill. Jan. 5, 2015) (rejecting witness testimony that “every word” of a 101-page document was a trade secret; to be a protectable trade secret, an idea or concept must be “concrete”); *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 902-03 (Minn. 1983) (“ECC’s [secrecy] efforts were especially inadequate because of the nonintuitive nature of ECC’s claimed secrets here. The dimensions, etc., of ECC’s motors are not trade secrets in as obvious a way as a ‘secret formula’ might be. ECC should have let its employees know in no uncertain terms that those features were secret. Instead, ECC treated its information as if it were not secret. None of its technical documents were marked ‘Confidential,’ and drawings, dimensions and parts were sent to customers and vendors without special marking. Employee access to documents was not restricted. ECC never issued a policy statement outlining what it considered to be secret.”); Camilla A. Hrady, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C.L. Rev. 2409 (2019) (examining cases and arguing on historical and public policy grounds that the general skill and knowledge defense should be given sweeping effect in employee cases, in order to protect employee mobility); Kurt M. Saunders & Nina Golden, *Skill or Secret? – The Line Between Trade Secrets and Employee General Skills and Knowledge*, 15 N.Y.U. J. L. & BUS. 61, 75-84 (2018) (discussing different approaches courts have taken in distinguishing trade secrets from employee general skill and knowledge). But see Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 525 (2010) (discussing UTSA drafters’ decision to omit a “tangibility” condition from the “economic value” requirement in the UTSA definition of “trade secret”).

information ex ante, they may be overly cautious to move jobs and start new entrepreneurial endeavors, taking their existing skills and knowledge with them.⁹⁶

These circumstances demand particularity in pleading, but at the federal level there is no specific statute or rule addressing trade secret identification requirements for pleading or discovery. The DTSA itself is silent on the issue. The Supreme Court has never considered the issue from a pleading standpoint, and the Courts of Appeals also appear not to have analyzed identification as a matter of pure pleading. As a result, federal district courts have been sporadic at best in calling for identification pleading.⁹⁷ *Combined Metals of Chicago Ltd. Partnership v. Airtek*,⁹⁸ a Northern District of Illinois case decided before *Twombly* and *Iqbal*, is representative. Airtek hired Combined Metals to fabricate catalytic converters pursuant to Airtek's proprietary designs and blueprints for tooling. Combined Metals began making converters for other firms, prompting Airtek to bring trade secret theft and other counterclaims. On a Rule 12(b)(6) motion to dismiss, Combined Metals argued Airtek had failed to sufficiently allege its precise trade secrets in issue. The district court rejected Airtek's "notice pleading" response as well as Airtek's reliance on *Conley v. Gibson*⁹⁹ before noting that Airtek appeared to be identifying two trade secrets – "the die and the knowledge of producing the catalytic converter shells."¹⁰⁰ The district court then recounted its own unhappy experience with insufficient identification one year before in *Thermodyne Food Service Products, Inc. v. McDonald's Corp.*,¹⁰¹ where defense confusion arose at summary judgment when the plaintiff redefined its claimed secrets. Citing no appellate authority on trade secret identification pleading, the *Airtek* court ruled:

Airtek will be held to those trade secrets, *i.e.*, it will not be permitted to change or narrow them as the case progresses. If there is a more specific technology underlying the die or the knowledge of producing the catalytic converter shells that Airtek desires to claim as a trade secret, Airtek better put Combined Metals on notice of such technology now (by filing an amended

⁹⁶ Deepa Varadarjan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 382, 385-86 (2017).

⁹⁷ See, e.g., *AutoMed Techs., Inc. v. Eller*, 160 F. Supp. 2d 915, 925 (N.D. Ill. 2001) (noting plaintiff promised to identify its trade secrets with more particularity in its amended complaint, and then finding plaintiff's "general allegations of software, designs and research" to be "insufficient," without citing any law).

⁹⁸ 985 F. Supp. 827 (N.D. Ill. 1997).

⁹⁹ See *id.* at 831; *id.* at 829 (citing *Conley v. Gibson*, 355 U.S. 41, 45-46 (1957)).

¹⁰⁰ *Id.* at 832.

¹⁰¹ 940 F. Supp. 1300, 1304-05 (N.D. Ill. 1996).

counterclaim) or forfeit the right to claim such technology as a trade secret at a later time in this case.¹⁰²

Some states have provided more definitive guidance on trade secret identification for pleading purposes. California, a fact-pleading jurisdiction, has long imposed a reasonable “particularity” pleading standard in trade secret cases, starting with the famous decision in *Diodes, Inc. v. Franzen*.¹⁰³ There, Stump and Franzen, both directors and officers of Diodes, refused to divulge their secret research and departed to form a rival semiconductor firm. Uncertain as to what research Stump and Franzen had been doing, Diodes in its third amended complaint was only able to vaguely allege that they had developed a “secret process” having something to do with manufacturing diodes. The California Court of Appeal held this was not sufficient to meet California’s fact-pleading standards:

Before a defendant is compelled to respond to a complaint based upon claimed misappropriation or misuse of a trade secret and to embark on discovery which may be both prolonged and expensive, the complainant should describe the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies.¹⁰⁴

Diodes eventually led the California legislature to pass a California Civil Code of Procedure provision requiring the party alleging misappropriation to identify its trade secrets with reasonable particularity before commencing discovery.¹⁰⁵ This statute, as one might expect, has resulted in battles over whether plaintiff has made too little disclosure or whether defendant has demanded too much.¹⁰⁶

¹⁰² *Combined Metals*, 985 F. Supp. at 832.

¹⁰³ 260 Cal. App. 2d 244 (1968). See also *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 522 (9th Cir. 1993) (applying California law and citing *Diodes*) (“[A] plaintiff who seeks relief for misappropriation of trade secrets must identify the trade secrets and carry the burden of showing that they exist.”).

¹⁰⁴ *Diodes*, 260 Cal. App. 2d at 253.

¹⁰⁵ Cal. Code Civ. Proc. § 2019.210 (“[B]efore commencing discovery relating to a trade secret, the party alleging the misappropriation shall identify the trade secret with reasonable particularity. . . .”); Pooley, *supra* note 68, at 203, 215 (discussing legislative history of the California Code of Civil Procedure “reasonable particularity” section and its tie to *Diodes*).

¹⁰⁶ *Perlan Therapeutics, Inc. v. Superior Court*, 178 Cal. App. 4th 1333, 1350 (2009) (“Perlan is not entitled to include broad, ‘catch-all’ language as a tactic to preserve an unrestricted, unilateral right to subsequently amend its trade secret statement. If Perlan does not know what its own trade secrets are, it has no basis for suggesting defendants misappropriated them. Nor is Perlan entitled to hide its trade secrets in ‘plain sight’ by including surplusage and voluminous attachments in its trade secret statement. If, through discovery, Perlan uncovers

It has also prompted federal court decisions debating whether this disclosure requirement constitutes substantive law, implicating *Erie* in California diversity jurisdiction cases.¹⁰⁷ Other states, by statute or judicial decision, have imposed similar particularity disclosure requirements on plaintiffs, either in complaints or at least before discovery commences,¹⁰⁸ with Massachusetts the latest to act on both fronts.¹⁰⁹ The net effect of these scattered state and federal district court

information suggesting defendants misappropriated additional trade secrets, it may have good cause to amend its trade secret statement under appropriate circumstances.” (footnotes omitted); *Brescia v. Angelin*, 172 Cal. App. 4th 133, 143 (2009) (“Absent a showing that the details alone, without further explanation, are inadequate to permit the defendant to discern the boundaries of the trade secret so as to prepare available defenses, or to permit the court to understand the identification so as to craft discovery, the trade secret claimant need not particularize how the alleged secret differs from matters already known to skilled persons in the field.”); *Advanced Modular Sputtering, Inc. v. Superior Court*, 132 Cal. App. 4th 826, 834 (2005) (“‘Reasonable particularity’ mandated by section 2019.210 does not mean that the party alleging misappropriation has to define every minute detail of its claimed trade secret at the outset of the litigation. Nor does it require a discovery referee or trial court to conduct a miniature trial on the merits of a misappropriation claim before discovery may commence . . . The degree of ‘particularity’ that is ‘reasonable’ will differ, depending on the alleged trade secrets at issue in each case. Where, as here, the alleged trade secrets consist of incremental variations on, or advances in the state of the art in a highly specialized technical field, a more exacting level of particularity may be required to distinguish the alleged trade secrets from matters already known to persons skilled in that field.”).

¹⁰⁷ *Compare* *Funcat Leisure Craft, Inc. v. Johnson Outdoors, Inc.*, No. S-06-0533 GEB GGH, 2007 WL 273949 (E.D. Cal. Jan. 29, 2007) (ruling that Section 2019.210 is procedural and hence not binding in federal court under *Erie*) with *Comput. Econ., Inc. v. Gartner Grp., Inc.*, 50 F. Supp. 2d 980 (S.D. Cal. 1999) (holding Section 2019.210 constituted substantive state law applicable to federal court diversity jurisdiction proceedings under *Erie*) and *E.J. Gallo Winery v. Instituut Voor Landbouw-En Visserijonderzoek*, No. 1:17-cv-00808-DAD-EPG, 2018 WL 3062160, at *2-*4 (E.D. Cal. June 18, 2018) (collecting conflicting cases on *Erie* treatment of Section 2019.210 and then following Section 2019.210 under the court’s inherent authority to sequence discovery).

¹⁰⁸ *SmithKline Beecham Pharms. Co v. Merck & Co.*, 766 A.2d 442, 447 (Del. 2000) (“In cases involving trade secrets, the plaintiff is required to disclose, before obtaining discovery of confidential proprietary information of its adversary, the trade secrets it claims were misappropriated . . . The plaintiff must disclose the allegedly misappropriated trade secrets with reasonable particularity.” (citation omitted)); *MSCI Inc. v. Jacob*, 36 Misc. 3d 211, 213-14 (N.Y. Sup. Ct. 2012) (adopting reasonable particularity standard for discovery purposes: “[T]he court is persuaded that the law requires that a trade secret plaintiff identify trade secrets with reasonable particularity early in the case . . . Only by distinguishing between the general knowledge in their field and their trade secrets will the court be capable of setting the parameters of discovery and will defendants be able to prepare their defense.”)(citation omitted); *Krawiec v. Manly*, 811 S.E.2d 542, 548 (N.C. 2018) (following *SmithKline Beecham* and adopting reasonable particularity for pleading a trade secret); *ECT Int’l, Inc. v. Zwerlein*, 597 N.W.2d 479, 482 (Wis. Ct. App. 1999) (endorsing *Diodes* pleading “particularity” standard for assessing trade secret complaints).

¹⁰⁹ *See* MASS. GEN. LAWS ch. 93, § 42D(b) (2018) (“In an action . . . alleging trade secrets misappropriation a party must state with reasonable particularity the circumstances thereof, including the nature of the trade secrets and the basis for their protection. Before commencing discovery related to an alleged trade secret, the party alleging misappropriation shall identify

standards has been to require modest identification in complaints followed by more searching identification inquiries during discovery. Since state and federal trade secret identification law has thus far favored discovery over complaints, since no federal statute or rule speaks to trade secret identification, and since federal notice pleading could hardly have been more lax until *Twombly* and *Iqbal*, it is unsurprising that the very capable commentators who have weighed in on aspects of identification have given relatively short shrift to the federal court pleading issue, focusing instead on state and federal court discovery.¹¹⁰ I confess I've been guilty of the same sin.¹¹¹

As matters stand, with so few trade secret cases reaching the federal Courts of Appeals on pleading questions, it is easy to assume that a “short and plain statement” for purposes of Rule 8(a) means general pleading standards in federal court “require plausibility as opposed to particularity.”¹¹² Or, in what amounts to only a small improvement, a court might say Rule 8(a) calls for something like the brief trade secret description the *Plastronics* court suggested, with the details left for the discovery process. I think both approaches miss the Supreme Court’s “context-specific” emphasis in *Iqbal*. The North Carolina Supreme Court, construing North Carolina Rule of Civil Procedure 8 on notice pleading in *Kraniec v. Manly*, adopted the rule federal courts *should* follow: “To plead misappropriation

the trade secret with sufficient particularity under the circumstances of the case to allow the court to determine the appropriate parameters of discovery and to enable reasonably other parties to prepare their defense.”)

¹¹⁰ DAVID W. QUINTO & STUART H. SINGER, *TRADE SECRETS: LAW AND PRACTICE*, ch. 2, at 83-87 (Oxford 2009) (in Chapter 2 describing the “reasonable particularity” pleading standard as “relatively minimal” and citing only one case, *Diodes*, but then cautioning in Chapter 3 that “[t]he argument that a plaintiff should always identify its allegedly misappropriated trade secrets with reasonable particularity at the outset may gain support from the Supreme Court decision in *Bell Atlantic Corp. v. Twombly*”); Casey, *supra* note 92, at 245-53 (discussing federal court notice pleading under *Conley* and state court particularity standard under *Diodes*, but offering no pleading particularity decision other than *Diodes* and writing long before *Twombly* and *Iqbal*); 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, 480-81 (2017) (discussing only one identification pleading case, *Diodes*, without discussing potential impact of *Twombly* and *Iqbal*); 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, 79-80 (2006) (devoting a single paragraph to identification pleading while citing *Diodes* and a handful of pleading cases, but writing before *Twombly* and *Iqbal*); Pooley, *supra* note 68, at 203 (mentioning *Diodes* in two-paragraph discussion of the provision that ultimately was codified as §2019.210, but focusing exclusively on California state law and writing long before *Twombly* and *Iqbal*).

¹¹¹ See William Lynch Schaller, *Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiff's Perspective*, 29 REV. LITIG. 729, 772-73, 801 (2010) (discussing whether *Twombly* and *Iqbal* might herald “greater factual specificity for [pleading] federal court [trade secret] cases” and later collecting Seventh Circuit and other trade secret identification discovery cases, but offering no explicit identification pleading discussion).

¹¹² *Physician's Surrogacy, Inc. v. German*, No. 17cv0718-MMA (WVG), 2018 WL 638229, at *5 n.4 (S.D. Cal. Jan. 31, 2018) (rejecting California-style “particularity” pleading for DTSA cases).

of trade secrets, a plaintiff must identify a trade secret with sufficient particularity so as to enable a defendant to delineate that which he is accused of misappropriating and a court to determine whether misappropriation has or is threatened to occur.”¹¹³

Assuming Congress leaves the DTSA as is for the foreseeable future, federal courts should at least adopt a reasonable particularity pleading standard, whether by local rule, by appellate decision, or by amendment to the Federal Rules of Civil Procedure.¹¹⁴ I would go further and require plaintiffs to file their secrets under seal simultaneously with the complaint. This is what the plaintiff did in *Molon Motor*, for example, so it certainly can be done, albeit with leave of court.¹¹⁵ The DTSA generally authorizes courts to make whatever orders are necessary to protect secrets¹¹⁶ and provides a specific example for court custody of secrets impounded under a search and seizure order.¹¹⁷ In fact, the DTSA expressly alludes to complaints being filed under seal in its whistleblower immunity section.¹¹⁸ Rule 26(c) of the Federal Rules of Civil Procedure, of course, also has long empowered courts to enter protective orders to shield trade secrets from unnecessary disclosure.¹¹⁹ And in the absence of any specific statute or rule,

¹¹³ *Krawiec*, 811 S.E.2d at 547–48 (quoting *Washburn v. Yadkin Valley Bank & Trust Co.*, 660 S.E.2d 577, 585 (N.C. Ct. App. 2008)).

¹¹⁴ Indeed, some federal Courts of Appeals have read *Twombly* and *Iqbal* to require factual particularity of a sort in other contexts. *See, e.g.*, *Doe v. Columbia College Chi.*, 933 F.3d 849, 854 (7th Cir. 2019) (stating in a Title IX case: “A plaintiff must plead particularized factual content, not conclusory allegations, that allows the court to plausibly infer the defendant is liable for the alleged misconduct.”) (citation omitted); Bethany A. Corbin, *Riding the Wave or Drowning?: An Analysis of Gender Bias and Twombly/Iqbal in Title IX Accused Student Lawsuits*, 85 *FORDHAM L. REV.* 2665 (2017) (discussing whether *Twombly* and *Iqbal* are being applied correctly in the Title IX context).

¹¹⁵ *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531, at *4 (N.D. Ill. May 11, 2017) (“Nidec acknowledges that, in a sealed appendix to the Third Amended Complaint, Molon has added details – file names and summaries – of the alleged stolen trade secrets.”); *cf.* *CleanFish, LLC v. Sims*, No. 19-CV-03663-HSG, 2020 WL 1274991, at *9 (N.D. Cal. Mar. 17, 2020) (on Rule 12(b)(6) motion to dismiss in case brought under DTSA and California law, court refused to wade through alleged trade secrets “further identified in [plaintiff’s] Motion to Seal,” on the ground that the court “cannot consider extrinsic evidence outside the [complaint] at the motion to dismiss stage”).

¹¹⁶ *See* 18 U.S.C. §1836(b)(3)(A)(ii) (2018) (“In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may grant an injunction if determined appropriate by the court, requiring affirmative actions to be taken to protect the trade secret.”).

¹¹⁷ *See* 18 U.S.C. §1836(b)(2)(D).

¹¹⁸ *See* 18 U.S.C. § 1833(b)(1)(B) (2018) (an individual shall not be criminally or civilly liable under any federal or state law for disclosing a trade secret “in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal”).

¹¹⁹ *See* FED. R. CIV. P. 26(c)(1), 26(c)(1)(G) (“The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following . . . requiring that a trade secret or other confidential research, development, or commercial information not be revealed or be revealed only in a specified way.”).

federal courts possess inherent authority “to manage their own affairs so as to achieve the orderly and expeditious disposition of cases”¹²⁰ — authority that includes sealing a complaint or its relevant exhibits upon a proper “good cause” showing of trade secret necessity.¹²¹ All of these address the often-expressed concern that requiring specificity in complaints runs the risk of public disclosure and hence destruction of secrets.¹²²

When I speak of attaching plaintiff’s secrets to the complaint (under seal, of course), I mean attaching the actual secret defendant was supposedly shown and supposedly stole. This is, in essence if not in fact, a chain of custody requirement.¹²³ We live in an age of heightened corporate security and careful computer monitoring; employers practically brag about their ability to track employee computer activity down to the keystroke, to analyze data about their employees, and to predict an employee’s every move.¹²⁴ Blockchain technology is rapidly gaining popularity, too, with its ability to validate and track transactions in a reliable and indeed self-authenticating manner;¹²⁵ it’s only a question of time until this technology is adapted for internal trade secret recordkeeping purposes.¹²⁶ In these

¹²⁰ *Dietz v. Bouldin*, 136 S. Ct. 1885, 1891 (2016) (quoting *Link v. Wabash R.R. Co.*, 370 U.S. 626, 630-31 (1962)).

¹²¹ *See* *Sherwin Williams Co. v. Courtesy Oldsmobile Cadillac, Inc.*, No. 1:15-cv-01137 MJS, 2015 WL 8665601 at *2 (E.D. Cal. Dec. 14, 2015) (denying motion to seal supply agreement exhibit because plaintiff merely made “conclusory arguments” and “blanket” claims that supply agreement contained trade secrets).

¹²² *See, e.g.,* *Mission Measurement Corp. v. Blackbaud, Inc.*, 216 F. Supp. 3d 915, 921 (N.D. Ill. 2016) (denying Rule 12(b)(6) trade secret identification motion in DTSA case, ruling that “[a]t the pleading stage, plaintiffs need only describe the information and efforts to maintain confidentiality of the information in general terms” and that “trade secrets need not be disclosed in detail in a complaint alleging misappropriation for the simple reason that such a requirement would result in public disclosure of the purported trade secrets”) (alteration in original) (internal quotations omitted).

¹²³ *See, e.g.,* *Melendez-Diaz v. Massachusetts*, 557 U.S. 306, 311 n.1 (2009) (discussing chain of custody as a Confrontation Clause requirement in criminal cases); Jared S. Hopkins & Stacy St. Clair, *Mysterious Bag in Patrick Kane Case Was a Hoax, DA Says*, *Chicago Tribune* (Sept. 25, 2015 3:58 PM), <https://www.chicagotribune.com/news/breaking/ct-patrick-kane-investigation-20150925-story.html> (reporting on “rape kit” hoax against famous Chicago Blackhawks hockey player Patrick Kane: “At a news conference on Friday, Erie County District Attorney Frank Sedita III said the bag was given to the accuser’s mother when she accompanied her daughter to a local hospital to have a rape kit done on Aug. 2. She was the last known person to have the bag, he said. Sedita methodically walked reporters through a detailed timeline and surveillance video, showing the chain of custody of the rape kit. Video recordings, Sedita said, showed the kit was put in a box and never placed in [the] bag.”).

¹²⁴ *See* Sarah Krouse, *The New Ways Your Boss Is Spying on You*, *WALL ST. J.*, July 20, 2019, at B1.

¹²⁵ *See* Jason Tashea, *Best Evidence*, 105 A.B.A. J. 22 (2019) (reporting on new laws in Arizona, Delaware, Ohio and Vermont, and noting blockchain may constitute self-authenticating evidence under Rule 902 of the Federal Rules of Evidence).

¹²⁶ *See* Christina M. Jordan, *Navigating Discovery with Blockchain Technology*, 44 *LITIG. NEWS* 2 (2019) (“Because the ledger is an ongoing, validated, and secure log of all transactions recorded, blockchain can be useful for transactions involving proof and chain of title and

circumstances, a diligent trade secret owner should know exactly what its secrets are, should know exactly who was given access to them, should know exactly when they were accessed, and through proper pre-litigation investigation, should know exactly which trade secrets it thinks were stolen and why. In other words, trade secret identification at the time of authorized access should present a question of law for Rule 12(b)(6) purposes; either the secret was sufficiently identified at access or it was not.¹²⁷ The complaint can easily tell this tale by attaching the secret exactly as disclosed and by attaching computer logs detailing the time and place of disclosure.

Trade secret theft is a serious crime. Such an accusation can instantly derail a new employee's career or tank a pending business deal. No one should need to guess about what was allegedly taken in these and other settings involving controversies crucial to our free market economy. Ending such uncertainty at the outset should be the very purpose of "notice" pleading. In my view, *Twombly* and *Iqbal* command it in trade secret cases.¹²⁸

D. ECONOMIC VALUE

Aside from knowing what its secrets are, plaintiff should also know why its secrets would be valuable to others in the trade. As suggested in *ABB Turbo Systems*, a brief description of the time and effort it took to create them and why they provide a competitive edge should be enough to withstand attacks under *Twombly* and *Iqbal*.¹²⁹ *Plastronics* was somewhat unusual in that plaintiff merely made boilerplate economic value allegations. Assuming most plaintiffs will offer at least some facts on this topic, few trade secret cases should be subject to

ownership of property. These features also make blockchain effective for providing current and accurate audit trails and identifying parties to transactions.”).

¹²⁷ See *Genentech, Inc. v. JHL Biotech, Inc.*, No. C 18-06582, 2019 WL 1045911, at * 8 (N.D. Cal. Mar. 1, 2019) (in DTSA case, granting Rule 12(b)(6) motion to dismiss, in part, and ordering plaintiff Genentech to provide a detailed description of who it shared its trade secret documents with, emphasizing that “he who seeks equity must do equity”).

¹²⁸ See *Javo Beverage Co., Inc. v. California Extraction Ventures, Inc.*, No. 19-CV-1859-CAB-WVG, 2020 WL 886527, at *1 (S.D. Cal. Feb. 24, 2020)(waiting until preliminary injunction stage before determining that plaintiff's asserted trade secrets differed substantially from defendants' patent disclosures; accordingly, court denied preliminary injunction seeking “to prohibit Defendants from further using Javo's trade secrets and other confidential information in connection with: CEV's process or selling any products derived from such information; raising money from investors; filing any new patent applications; and taking any steps to license or grant to third parties any rights in any issued patents or pending patent applications claiming priority to the 497 Provisional application.”).

¹²⁹ *Cf. MAI Sys. Corp. v. Peak Comput., Inc.*, 991 F.2d 511, 521 (9th Cir. 1993) (ruling on summary judgment appeal: “MAI contends its Customer Database is a valuable collection of data assembled over many years that allows MAI to tailor its service contracts and pricing to the unique needs of its customers and constitutes a trade secret. We agree that the Customer Database qualifies as a trade secret. The Customer Database has potential economic value because it allows a competitor like Peak to direct its sales efforts to those potential customers that are already using the MAI computer system.”).

challenge on economic value grounds at the Rule 12(b)(6) stage — unless the “secret” information has no value because it’s in the public domain,¹³⁰ or, perhaps, because it amounts to general skill and knowledge.¹³¹ In effect, such a motion to dismiss would ask the court to take judicial notice of industry or common knowledge. If it’s in a book, published by the government or the company itself,¹³² available on the internet, or perhaps just common sense, I suppose the court could do so,¹³³ and I suspect this angle of attack will sharpen as online

¹³⁰ See *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1002 (1984) (“Information that is public knowledge or that is generally known in an industry cannot be a trade secret.”); *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974) (“The Court has also articulated another policy of the patent law: that which is in the public domain cannot be removed therefrom by action of the States.”); *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279, 1298 (11th Cir. 2018) (affirming Rule 56 summary judgment that suppliers’ identities were not secret: “[T]he identities of Yellowfin’s suppliers are typically well known—indeed, ‘the photos in the record show that many [of the suppliers] prominently brand their products.’” (alteration in original) (citation omitted)); *Accent Packaging, Inc. v. Leggett & Platt, Inc.*, 707 F.3d 1318 (Fed. Cir. 2013) (affirming Rule 12(b)(6) dismissal of trade secret claims based on public disclosure in United States patents); *Ultimax Cement Mfg. Corp. v. CTS Cement Mfg. Corp.*, 587 F.3d 1339, 1356 (Fed. Cir. 2009) (affirming Rule 56 summary judgment on trade secret claims based on public disclosure in Japanese patent); *Capricorn Mgm’t Sys., Inc. v. Gov’t Employees Ins. Co.*, 15 CV 2926 (DRH)(SIL), 2020 WL 1242616, at *9 (E.D.N.Y. Mar. 16, 2020) (ruling, on summary judgment, that unredacted source code deposits on file with Copyright Office were “public” and hence not entitled to trade secret status).

¹³¹ *Cf. Comput. Care v. Serv. Sys. Enter., Inc.*, 982 F.2d 1063 (7th Cir. 1992) (the idea of sending service-reminder letters to customers was well known and in the public domain); *Sys. Dev. Serv’s., Inc. v. Haarmann*, 907 N.E.2d 63, 74 (Ill. App. Ct. 2009) (customer list consisting of nothing more than names, addresses and telephone numbers lacked sufficient secrecy to be a trade secret under the Illinois Trade Secrets Act); *Serv. Ctr’s. of Chi., Inc. v. Minogue*, 535 N.E.2d 1132, 1136–37 (Ill. App. Ct. 1989) (plaintiff’s “rules of thumb” used in pricing medical records storage space were not protected under the Illinois Trade Secrets Act; plaintiff failed to show they were not generally known in the industry or not part of defendant-employee’s general skill and knowledge); *Cent. Bldg. & Cleaning Co. v. Vodnansky*, 406 N.E.2d 32, 35 (Ill. App. Ct. 1980) (tuckpointing and restoration firm’s bid estimation method was not a trade secret; employee “learned to estimate through his day-to-day experience and training on the job”).

¹³² See, e.g., *CouponCabin, Inc. v. PriceTrace, LLC*, No. 18 C 7525, 2019 WL 1572448, at *3 (N.D. Ill. Apr. 11, 2019) (denying DTSA trade secret protection because plaintiff’s complaint admitted its website and coupon codes were “generally accessible” to the public).

¹³³ See *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009) (in determining plausibility, the court must “draw on its judicial experience and common sense”); *Rowe v. Gibson*, 798 F.3d 622 (7th Cir. 2015) (majority opinion by Judge Posner taking judicial notice of medical subjects based on court’s own internet search, prompting a vigorous partial dissent by Judge Hamilton); Henry S. Noyes, *The Rise of the Common Law of Federal Pleading: Iqbal, Twombly and the Application of Judicial Experience*, 56 VILL. L. REV. 857, 871-89 (2012) (discussing judicial experience and common sense within the meaning of *Twombly* and *Iqbal*); Coleen M. Barger, *Challenging Judicial Notice of Facts on the Internet Under Federal Rule of Evidence 201*, 48 U.S.F. L. REV. 43 (2013) (exploring the limits of judicial notice via the internet); Debra Cassens Weiss, *May Judges Search the Internet for Facts? ABA Ethics Opinion Sees Problems*, ABA JOURNAL (Dec. 8, 2017, 7:02 AM) http://www.abajournal.com/news/article/may_judges_search_the_internet_for_facts_aba_ethics_opinion_sees_ethics_pro (discussing ABA Formal Opinion 478

information expands.¹³⁴ Otherwise this opposition should await proof.¹³⁵

However, pleading “economic value” may be complicated by the “identification” standard federal courts ultimately adopt. The California state court decision in *Diodes* and the North Carolina state court decision in *Krawiec*, for example, carry very different implications for pleading “economic value.” With its emphasis on “sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those who are skilled in the trade,” *Diodes* in effect requires plaintiff to plead and prove a negative to show economic value — what others in the trade don’t know.¹³⁶ The *Krawiec* formulation, by contrast, merely demands that plaintiff identify the misappropriated secret with sufficient particularity to enable a meaningful defense. It does not explicitly inject the *Diodes* “general knowledge/special knowledge” inquiry into the pleading stage.

and cautioning against judicial notice of adjudicative facts—i.e., facts that are either not generally known or subject to reasonable dispute); Cheryl D. Stein, *Judicial Notice: A Useful Tool to Consider*, ABA JOURNAL (May 20, 2019), <https://www.americanbar.org/groups/litigation/committees/criminal/articles/2019/spring2019-judicial-notice-a-useful-tool-to-consider/> (May 20, 2019) (“An adjudicative fact can be judicially noticed if it ‘is not subject to reasonable dispute.’ FED. R. EVID. 201(b). There are two categories of these facts: (1) those that are ‘generally known within the trial court’s territorial jurisdiction’ and (2) those that ‘can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned.’ *Id.*”).

¹³⁴ See, e.g., Colin T. Reardon, Note, *Pleading in the Information Age*, 85 N.Y.U. L. REV. 2170, 2183–87 (2010) (arguing that *Twombly* and *Iqbal* challenges should become increasingly common as the internet makes public information more readily available to plaintiffs and defendants); Dave Michaels & Alexander Osipovich, *VC Firm Battles Crypto Crackdown*, WALL ST. J., Sept. 3, 2019, at B5 (quoting Netscape founder and well-known investor Marc Andreessen as saying the internet has evolved into the world’s information hub and an engine for commerce).

¹³⁵ See, e.g., *Chastleton Corp. v. Sinclair*, 264 U.S. 543, 548–49 (1924) (Holmes, J.) (the Court could take judicial knowledge of the fact that no housing shortage justifying District of Columbia wartime rent controls continued to exist in 1924, but remand was necessary to decide whether a sufficient emergency existed during 1922 in the immediate aftermath of World War I); *Cedars-Sinai Medical Center v. Quest Diagnostics, Inc.*, No. CV 17-5169-GW, 2018 WL 2558388 (C.D. Cal. Feb. 27, 2018) (denying Rule 12(b)(6) motion to dismiss in DTSA case on the ground that the court could not say Cedars-Sinai’s patent filings had publicly disclosed everything about its trade secrets; expert testimony was necessary to determine scope of Cedars-Sinai’s public disclosures).

¹³⁶ See, e.g., *CleanFish, LLC v. Sims*, No. 19-CV-03663-HSG, 2020 WL 1274991, at *9 (N.D. Cal. Mar. 17, 2020) (granting Rule 12(b)(6) motion to dismiss in case brought under DTSA and California law: conclusory allegations of trade secrets concerning “niche clientele of end-run buyers” were “indistinguishable from matters of general knowledge within the parties’ industry”); *Pellerin v. Honeywell, Inc.* 877 F. Supp. 2d 983, 988 (S.D. Cal. 2012) (complaint must describe “the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons who are skilled in the trade, and to permit the defendant to ascertain at least the boundaries within which the secret lies”); Victor de Gyarfas, *Pleading a Claim for Misappropriation of Trade Secrets in California: A Problem of Particularity*, FOLEY & LARDNER LLP (Feb. 27, 2018), <https://www-foley.com/en/insights/publications/2018/02/pleading-a-claim-for-misappropriation-of-trade-sec> (collecting cases).

Like the UTSA, and like the common law and Restatement of Torts before the UTSA, the DTSA in its definition of “trade secret” plainly prohibits protection of generally known or readily ascertainable information; no one questions this. But this does not speak to the issue of who has to plead and prove what. To me, this should be a matter of relative convenience. I suppose courts could force plaintiffs to canvass the known universe in an effort to prove what is not there,¹³⁷ but I think this gets the inquiry exactly backwards. If defendants can “readily ascertain” (as the DTSA puts it) secrets from the public domain or from comparable, non-confidential sources, it would be far easier to simply require defendants to produce source evidence as exhibits to their Rule 12(b)(6) motions to dismiss.¹³⁸ Courts and parties can then focus their attention on the public source evidence with minimal expense and delay. In other words, I would place the initial burden of production on the defendant, with respect to public domain or industry knowledge, even though I would leave the ultimate burden of persuasion on the plaintiff, as with reverse engineering and independent development.¹³⁹ *Krawiec* is consistent with this pleading approach; *Diodes* is not.

I am aware of no case requiring plaintiffs to explicitly negate reverse

¹³⁷ Based on his confirmation hearing experience, I would think Justice Kavanaugh would have little interest in forcing anyone to “prove a negative.” See Theodore Dalrymple, *A Gladitorial Soap Opera: The Kavanaugh Hearings, Through the Eyes of a British Psychiatrist*, CITY JOURNAL, (Winter 2019), <https://www.city-journal.org/brett-kavanaugh-hearings> (“Kavanaugh was in the impossible position of trying to prove a negative, when the only way of doing so would have been to establish conclusively that he spent the entire period in, say, the Amazon jungle. The allegations against him did not meet the civil, much less the criminal, standard of proof; and if everyone seeking high office had to prove his innocence beyond reasonable doubt of any accusation leveled by anyone against him, we should soon have no holders, or even seekers, of high office.”).

¹³⁸ See *Putnam Res. v. Patemen*, 958 F.2d 448, 461 (1st Cir. 1992) (“If the rule were otherwise, every similarly situated suitor would be left in an epistemological quandary, required, in effect, to do the impossible, that is, to prove a negative by direct evidence.”); JEFF KOSSEFF, *THE TWENTY-SIX WORDS THAT CREATED THE INTERNET* 218 (Cornell Univ. Press Ithaca & London, 2019) (cross-examination of TheDirty.com operator Nik Richie on how defamation victim Sarah Jones would be able to disprove his website’s assertion that she had sex with every member of the Cincinnati Bengals as a team cheerleader: “How do you prove you didn’t have sex with every Bengal football player?” [Jones’s lawyer Eric] Deters asked. ‘I don’t know,’ Richie replied.”).

¹³⁹ Cf. *Dir., Office of Workers’ Comp. Programs v. Greenwich Collieries*, 512 U.S. 267, 272-76 (1994) (discussing historical development of burden of proof and burden of production in interpreting a federal statute that used the phrase “burden of proof”); *Moore v. Kulicke & Soffa Indus., Inc.*, 318 F. 3d 561, 569-72 (3d Cir. 2003) (applying Pennsylvania law) (defendant has the burden of production on independent development, but plaintiff has the ultimate burden of proof since plaintiff must prove wrongful “use” of a trade secret); *Sargent Fletcher, Inc. v. Able Corp.*, 110 Cal. App. 4th 1658, 1669 (2003) (“It is the plaintiff’s burden to show improper use as a part of its prima facie case. Proof that defendant’s use resulted from independent derivation or reverse engineering is evidence that there was no improper use on its part. The defendant does not have a ‘burden of proof’ to make that showing. But it acts at its peril if it fails to present evidence that rebuts the plaintiffs showing. In some cases, its failure to do so may require judgment in plaintiff’s favor.”) (citation omitted).

engineering or independent development (or any other legitimate means of acquisition) as a matter of pleading,¹⁴⁰ so I will keep my focus here on the public domain defense. Under the “property” conception of trade secret law, the public domain eliminates the alleged “trade secret” (just as reverse engineering and independent development eliminate the alleged “misappropriation”), thereby defeating a trade secret misappropriation claim. More precisely, under this theory it does not matter whether the defendant *actually* obtained the secret legitimately, so long as the defendant *could have* obtained it legitimately, in this instance from the public domain.¹⁴¹ As an example, consider *Ultimax Cement Manufacturing Corp. v. CTS Cement Manufacturing Corp.*,¹⁴² a Federal Circuit case applying the California “property” approach to trade secret law in response to a public domain defense. Affirming summary judgment for the defense, the Court of Appeals observed:

Ultimax argues that the court erred in dismissing the trade secret claims. According to Ultimax, a secret’s availability from a published source is not a defense to trade secret theft under California law unless CTS also obtained the secret from the published source, which CTS did not do. Instead, Ultimax argues, CTS illegally obtained the secret from Ultimax. Ultimax adds that, contrary to CTS’s argument, the secret was not disclosed in the 684 patent . . .

Under California law, a trade secret must “(1) [d]erive[] independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) [be] the subject of efforts that are reasonable under the circumstances to maintain its secrecy.” Cal. Civ. Code § 3426.1(d). Thus, a trade secret must not have already been “generally known to the public.” “Public disclosure, that is the absence of secrecy, is fatal to the existence of a trade secret.” *In re Providian Credit Card Cases*, 96 Cal.App.4th 292, 304. . . (2002). Further, “[i]t is well established that disclosure of a trade secret in a patent places the information comprising the secret into the public domain. Once the

¹⁴⁰ Unlike the UTSA, the DTSA includes a catch-all exclusion of “any other lawful means of acquisition” in its definition of “improper means.” See 18 U.S.C. § 1839(6)(b) (2018) (improper means “does not include reverse engineering, independent derivation, or any other lawful means of acquisition”).

¹⁴¹ The same would also be true for reverse engineering and independent development under the property principle. See, e.g., *Moore*, 318 F.3d at 570-71 (applying Pennsylvania law) (discussing “property” view of trade secrets adopted by the Pennsylvania Supreme Court: “The Court held that under Pennsylvania law, there is no trade secret if, ‘at the time of disclosure or use by a misappropriator, the allegedly secret information could have been ascertained by inspection of sold articles or by reverse engineering.’”) (internal citation omitted).

¹⁴² 587 F.3d 1339, 1355 (Fed. Cir. 2009) (applying California law).

information is in the public domain and the element of secrecy is gone, the trade secret is extinguished and the patentee's only protection is that afforded under the patent law." *Stutz Motor Car of Am. v. Reebok Int'l*, 909 F. Supp. 1353, 1359 (C.D.Cal.1995) (quotation marks, citations, and footnote omitted); see also *Forcier v. Microsoft Corp.*, 123 F.Supp.2d 520, 528 (N.D.Cal.2000).

Ultimax's argument focuses on how CTS obtained the alleged secret information, attempting to rebut a possible defense to a trade secret claim, but that is irrelevant if there is no secret. Here, Ultimax has not shown that it had a secret. Information disclosed in a patent, even a foreign one, is "generally known to the public," especially the relevant public in the cement industry. Indeed, one of the primary purposes of patent systems is to disclose inventions to the public. See *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1379 (Fed.Cir.2006) (finding a foreign patent, like a U.S. patent, "publicly accessible" because "one skilled in the art exercising reasonable diligence" could find it and it was "classified and indexed" in the foreign patent office). We therefore affirm the district court's grant of summary judgment with respect to Plaintiffs' trade secret claims, as Ultimax cannot prove the existence of a secret.¹⁴³

There is another way to look at this problem: the "breach of confidence" theory.¹⁴⁴ On this view the important issue is the defendant's conduct: actual theft is not excused based on what the defendant *could have* done but did not do.¹⁴⁵ In *E.I. DuPont de Nemours Powder Co. v. Masland*,¹⁴⁶ Justice Holmes offered the most famous (and most pointed) expression of the breach of confidence theory:

The case has been considered as presenting a conflict between a right of property and a right to make a full defen[s]e, and it is said that if the disclosure is forbidden to one who denies that there is a trade secret, the merits of his defen[s]e are adjudged

¹⁴³ *Id.* at 1355-56.

¹⁴⁴ Other, less persuasive approaches that try to capture the investment incentive and wrongdoer deterrence policies behind trade secret law include contract, commercial morality, and privacy. See generally Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets As IP Rights*, 61 STAN. L. REV. 311 (2008) (surveying and exploring trade secret theories).

¹⁴⁵ See *Group One, Ltd. v. Hallmark Cards, Inc.*, 254 F.3d 1041, 1050-51 (Fed. Cir. 2001) (collecting cases); *American Can Co. v. Mansukhani*, 728 F.2d 818, 820 (7th Cir. 1984) (collecting cases).

¹⁴⁶ 244 U.S. 100 (1917).

against him before he has a chance to be heard or to prove his case. We approach the question somewhat differently. The word property as applied to trade-marks and trade secrets is an unanalyzed expression of certain secondary consequences of the primary fact that the law makes some rudimentary requirements of good faith. *Whether the plaintiffs have any valuable secret or not, the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied but the confidence cannot be.* Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them. These have given place to hostility, and the first thing to be made sure of is that the defendant shall not fraudulently abuse the trust reposed in him. It is the usual incident of confidential relations. If there is any disadvantage in the fact that he knew the plaintiffs' secrets he must take the burden with the good.¹⁴⁷

Is *Masland* still good law?¹⁴⁸ *Erie* buried federal common law secrecy, but the DTSA may have resurrected it, and with it, *Masland*.¹⁴⁹ If so, defendants who

¹⁴⁷ *Id.* at 102 (emphasis added). Justice Holmes said much the same thing in an earlier trade secret case, *Board of Trade of the City of Chicago v. Christie Grain & Stock Co.*, 198 U.S. 236, 250–51 (1905): “In the first place, apart from special objections, the plaintiff’s collection of quotations is entitled to the protection of the law. It stands like a trade secret. The plaintiff has the right to keep the work which it has done, or paid for doing, to itself. The fact that others might do similar work, if they might, does not authorize them to steal the plaintiffs.” *Cf. Bleistein v. Donaldson Lithographing Co.*, 188 U.S. 239, 249, 250 (1903) (noting the plaintiff does not lose its rights by communicating the result to persons, even if many, in confidential relations to itself, under a contract not to make it public, and strangers to the trust will be restrained from getting at the knowledge by inducing a breach of trust and using knowledge obtained by such a breach).

¹⁴⁸ See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 497-98 (1974) (quoting the famous *Masland* “breach of confidence” passage in full and then observing—somewhat confusingly—that “[a] suit to redress theft of a trade secret is grounded in tort damages for breach of a contract”); Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 *HAMLIN L. REV.* 493, 515-20 (2010) (recounting history of UTSA drafting efforts and how the Supreme Court’s *Kewanee* decision, holding that federal patent law does not preempt state trade secret law, cleared the way for completion and approval of the initial version of the UTSA in 1979).

¹⁴⁹ See *TianRui Grp. Co. v. Int’l Trade Comm’n*, 661 F.3d 1322 (Fed. Cir. 2011) (pre-DTSA decision creating federal trade secret common law for International Trade Commission cases); Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret*, 32 *BERKELEY TECH. L.J.* 829, 867 (2017) (“As the history of U.S. trade secret law reveals, there is a rich body of common law related to trade secrets dating back nearly two centuries, making the common law’s application to the DTSA plausible.”) (footnotes omitted); Caleb Nelson, *The Legitimacy of (Some) Federal Common Law*, 101 *V.A. L. REV.* 1, 45 (2015) (“The idea that judges create the common law out of whole cloth also has ripple effects on the interpretation of federal statutes that borrow terms from the common law.”); Jay Tidmarsh & Brian J. Murray, *A Theory of Federal Common Law*, 100 *Nw. U. L. REV.* 585 (2006) (discussing federal common

wish to invoke the public domain defense may find themselves unable to challenge “economic value” allegations on Rule 12(b)(6) motions because, limited to the face of the complaint and judicially noticeable facts, they will be unable to show they actually acquired secrets from the public domain. They may instead have to wait until summary judgment, only to face “breach of confidence” headwinds there, too, if they in fact copied material but wish to defend based on what

they “could have” found in the public domain. On the other hand, if the property view prevails — as it did for Fifth Amendment “takings” purposes in *Ruckelshaus v. Monsanto Co.*¹⁵⁰ — plaintiffs can and should suffer sanctions for claiming trading secret status with respect to public domain information,¹⁵¹ no matter what the defendants may or may not have done.¹⁵² Such obvious deficiencies are the very essence of bad faith.¹⁵³

How should we resolve this tension in DTSA cases? The UTSA features aspects of both theories: the “property” view can be seen in the “economic value” clause found in Section 1.4 (on display in *Ultimax Cement*) and in the “head start” injunction limitation found in Section 2(a) (a result of the famous *Shellmar-Conmar-Winston* debate),¹⁵⁴ while the “breach of confidence” theory dominates the “misappropriation” definition set forth in Section 1.2 (discussed at length below). The DTSA is a curious mix of these elements; it takes “economic value” and “misappropriation” almost *verbatim* from the UTSA, but it drops the explicit “head start” injunction limitation and adds significant restrictions on injunctions against employees based on their mere knowledge alone.¹⁵⁵ On balance, this

law outside of *Erie*); Richard L. Revesz, *Restatements and the Federal Common Law*, AMERICAN LAW INSTITUTE (Sept. 27, 2016) <https://www.ali.org/news/articles/restatements-and-federal-common-law/>; RESTATEMENT (THIRD) OF UNFAIR COMPETITION §39(AM. LAW INST. 1995), <https://pdfs.semanticscholar.org/3745/dba7a672e7beac1dd52143136f85d5747519.pdf> (discussing potential role of Restatements in shaping federal common law).

¹⁵⁰ 467 U.S. 986, 1000-04 (1984).

¹⁵¹ See *BDT Products, Inc. v. Lexmark Int'l, Inc.*, 602 F.3d 742 (6th Cir. 2010) (applying Kentucky law) (discussing Rule 11 sanctions for misappropriation of trade secrets that had been publicly disclosed long before the litigation).

¹⁵² See *Rockwell Graphic Systems, Inc. v. DEV Industries, Inc.*, 925 F.2d 174, 179 (7th Cir. 1991) (Posner, J.) (“The remedial significance of such [reasonable secrecy] efforts lies in the fact that if the plaintiff has allowed his trade secret to fall into the public domain, he would enjoy a windfall if permitted to recover damages merely because the defendant took the secret from him, rather than from the public domain as it could have done with impunity . . . It would be like punishing a person for stealing property that he believes is owned by another but that actually is abandoned property.”) (citations omitted).

¹⁵³ See Charles Tait Graves, *Bad Faith and the Public Domain: Requiring a Pre-Lawsuit Investigation of Potential Trade Secret Claims*, 8 VA. J.L. & TECH. 12 (2003) (discussing public domain proof via internet searches and expert opinions).

¹⁵⁴ See William Lynch Schaller, *Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiff's Perspective*, 29 REV. LITIG. 729, 813 (2010).

¹⁵⁵ See *Synergetics, Inc. v. Hurst*, 477 F.3d 949, 961 (8th Cir. 2007) (applying Missouri law) (“A defendant should be enjoined only for the time it would take to produce and market the

amalgam seems to side with the “property” approach, mainly because the DTSA’s “economic value” reference to “not generally known” points away from

what a particular defendant knows in favor of what others in the industry generally know or can find in the public domain. The rule of lenity buttresses this pro-defendant view by demanding in all DTSA cases a strict construction of “trade secret” in general and “economic value” (and “not generally known”) in particular, as does to a lesser extent the DTSA’s explicit restriction in employee cases on injunctions tied solely to employee knowledge. If I am correct in thinking “identification” can and should come to the fore in light of *Twombly* and *Iqbal*, the “property” theory takes on added force, as the threshold inquiry will focus on what was taken rather than — as in *Masland* — the defendant’s conduct.

For the hardy souls who have made it this far, I finally return to the hospital pricing example I mentioned earlier, just after I quoted the DTSA’s definition of “trade secret.”¹⁵⁶ The Wall Street Journal article I quoted on hospital pricing as a “closely guarded secret” went on to report that area employers, in an effort “to curb rising costs,” had banded together to share data about what their local hospitals were secretly charging them.¹⁵⁷ The same article noted the “Trump administration is considering a requirement for hospitals and doctors to reveal negotiated prices.”¹⁵⁸ If published at the behest of government, such secrets would fall into the public domain, of course; but what if such pricing was widely shared among employers and hospitals knew it? On these facts, a hospital might have a very hard time alleging its pricing was “not generally known,” and a contrary allegation might even be subject to a Rule 12(b)(6) challenge. How? Consider the Rule 12(b)(6) standard the Second Circuit offered in *Cortec Industries, Inc. v. Sum Holding L.P.*: “Plaintiffs’ failure to include matters of which as pleaders they had notice and which were integral to their claim — and that they apparently most wanted to avoid — may not serve as a means of forestalling the district court’s decision on the motion.”¹⁵⁹

competitive product, absent the misappropriation.”); *Wyeth v. Natural Biologics, Inc.*, 395 F.3d 897, 898 (8th Cir. 2005) (applying Minnesota law) (affirming permanent injunction without time limitation to protect trade secret: “Wyeth’s trade secret process for producing bulk natural conjugated estrogens used in the development of Premarin, the only hormone replacement therapy drug on the market derived from a natural source.”); Richard F. Dole, Jr., *Permanent Injunctive Relief for Trade Secret Misappropriation Without an Express Limit Upon Its Duration: The Uniform Trade Secrets Act Reconsidered*, 17 B.U.J. SCI. & TECH. L. 173, 190 (2011) (surveying statutes and cases following and departing from the UTSA’s “head start” limitation on permanent injunctive relief).

¹⁵⁶ See Part I, *supra*.

¹⁵⁷ Melanie Evans, *Employers’ Hospital Fees Differ*, WALL ST. J., May 10, 2019, at B3.

¹⁵⁸ *Id.* See also Stephanie Armour & Anna Wilde Mathews, *New Push Calls for Disclosing Medical Price*, WALL ST. J., Mar. 8, 2019, at A1.

¹⁵⁹ *Cortec Indus., Inc. v. Sum Holding L.P.*, 949 F.2d 42, 44 (2d Cir. 1991).

E. REASONABLE SECRECY EFFORTS

In general, the more measures a firm takes to protect its secrets, the more likely a court will treat those secrets as having economic value.¹⁶⁰ The reasonableness of plaintiff's secrecy measures should rarely be subject to a Rule 12(b)(6) motion, as the Federal Circuit held in *ABB Turbo Systems*, unless plaintiff took no secrecy steps at all.¹⁶¹ In *Food Marketing Institute v. Argus Leader Media*,¹⁶² for example, the Supreme Court had no difficulty in finding commercial or financial information that is customarily and actually kept private to constitute "confidential" information for Freedom of Information Act exemption purposes.¹⁶³ *Plas-tronics* furnishes another example: allegations that defendants signed confidentiality agreements will usually get plaintiffs past "failure to state a claim" contentions.

There are three potential twists here, however. One, as the Court noted in *Food Marketing Institute*,¹⁶⁴ is that the information must actually be confidential;¹⁶⁵ an agreement saying it's so doesn't make it so if the information is in the public domain.¹⁶⁶ A second is when confidentiality agreements are facially void for some reason, such as vagueness or lack of geographic or temporal limits.¹⁶⁷

¹⁶⁰ See *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 179 (7th Cir. 1991) (Posner, J.) ("The information contained in the drawings cannot have been worth much if Rockwell did not think it worthwhile to make serious efforts to keep the information secret.")

¹⁶¹ See *ABB Turbo Systems AG v. TurboUSA, Inc.*, 774 F.3d 979, 986 (Fed. Cir. 2014) (reversing Rule 12(b)(6) dismissal; confidentiality agreements, confidentiality legends, and restricted access allegations showed reasonable secrecy measures); *Fail-Safe, LLC v. A.O. Smith Corp.*, 674 F.3d 889, 893 (7th Cir. 2012) (applying Wisconsin law) (affirming defense summary judgement: "We agree with the district court that FS failed to take reasonable steps under the circumstances to maintain the secrecy required for trade secret protection. Indeed, FS failed to take *any* steps to protect its information.")

¹⁶² 139 S. Ct. 2356 (2019).

¹⁶³ *Id.* at 2366 ("At least where commercial or financial information is both customarily and actually treated as private by its owner and provided to the government under an assurance of privacy, the information is 'confidential' within the meaning of Exemption 4.")

¹⁶⁴ *Id.* at 2363 ("[I]t is hard to see how information could be deemed confidential if its owner shares it freely.")

¹⁶⁵ *M.C. Dean, Inc. v. City of Miami Beach*, 199 F. Supp. 3d 1349, 1355-57 (S.D. Fla. 2016) (granting Rule 12(b)(6) motion to dismiss for lack of secrecy measures under the DTSA and the Florida trade secret statute; disclosures to government officials without restriction fell short of reasonable secrecy measures as a matter of law).

¹⁶⁶ See *Tax Track Sys., Corp. v. New Inv'r World, Inc.*, 478 F.3d 783, 787 (7th Cir. 2007) (applying Illinois law) (confidentiality agreement could not protect information that was not actually confidential); *Delta Med. Sys. v. Mid-America Med. Sys., Inc.*, 772 N.E.2d 768, 775, 781-83 (Ill. App. Ct. 2002) (customer information was in the public domain or part of defendants' general skill and knowledge and hence not protectable under the Illinois Trade Secret Act).

¹⁶⁷ See *AssuredPartners, Inc. v. Schmitt*, 44 N.E.3d 463, 475-76 (Ill. App. Ct. 2015) (holding that confidentiality agreement was overbroad and hence unenforceable because it purported to cover vague information regarding "the business or affairs" of the company or its affiliates).

Whether these drafting defects would negate the confidentiality notice functions of agreements for trade secret protection purposes is unclear, even assuming the agreements themselves are independently unenforceable as contracts.¹⁶⁸ A third is plaintiff's failure to comply with contractual requirements calling for confidentiality designations or some other secrecy measure, such as a written demand for return or destruction of documents.¹⁶⁹ Plaintiff's noncompliance might be teased out on a Rule 12(b)(6) motion by citing documents attached or referred to in the complaint;¹⁷⁰ the motion might argue, for example, that plaintiff failed to place "confidential" legends on its engineering drawings attached (albeit under seal) to the complaint,¹⁷¹ that plaintiff failed to allege it made a document demand in accordance with the parties' nondisclosure agreement,¹⁷² or that plaintiff failed to retrieve its documents as contractually required.¹⁷³ Or the motion might flip the script and argue plaintiff's referenced contract affirmatively *allowed* defendant's accused use.¹⁷⁴

¹⁶⁸ See *Metallurgical Indus., Inc. v. Fourtek, Inc.*, 790 F.2d 1195, 1206-07 (5th Cir. 1986) (applying Texas law) (nondisclosure agreement and purchase orders were admissible to show notice of confidentiality, even if those documents were unenforceable as contracts); Deepa Varadarajan, *The Trade Secret-Contract Interface*, 103 IOWA L. REV. 1543, 1561 (2018) (arguing that the mere existence of confidentiality agreements should not be equated with notice).

¹⁶⁹ Christine Streatfeild, Kevin M. O'Brien, Marc R. Paul & Nathaniel A. Douglas, *The Defend Trade Secrets Act in Business Transactions: Risks in Auction Data Rooms and Best Practices for Trade Secrets Protection*, BAKER MCKENZIE (June 18, 2019), <https://www.bakermckenzie.com/en/insight/publications/2019/06/defend-trade-secrets-act-in-business-transactions> (discussing steps sellers should take before disclosing information to auction bidder, including nondisclosure agreements "that require the return or destruction and certification of non-use and nondisclosure, of any information received in the transaction").

¹⁷⁰ See *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007) (on a Rule 12(b)(6) motion to dismiss, court may consider "documents incorporated into the complaint by reference, and matters of which a court may take judicial notice"); Aimee Woodward Brown, *Pleading in Technicolor: When Can Litigants Incorporate Audiovisual Works into Their Complaints?*, 80 U. CHI. L. REV. 1269 (2013) (reviewing Rule 12(b)(6) motion cases on incorporation by reference); Lawrence A. Steckman & Rita D. Turner, *Determining When Extrinsic Evidence Not Attached to or Incorporated by Reference in a Pleading May Be Considered on a Rule 12 Dismissal Motion*, 31 TOURO L. REV. 115 (2014) (discussing Second Circuit precedent on use of extrinsic evidence in Rule 12(b)(6) motions).

¹⁷¹ See, e.g., *Hoover Panel Sys., Inc. v. HAT Contract, Inc.*, No. 3:17-CV-3283-C, 2019 WL 2743589 (N.D. Tex. May 9, 2019) (granting summary judgment in favor of defendant and finding no misappropriation occurred when defendant sent prototypes to overseas supplier who then made products strikingly similar to plaintiff's products; plaintiff/trade secret owner failed to mark documents as "confidential" as required by confidentiality agreement).

¹⁷² See, e.g., *CMBB LLC v. Lockwood Mfg., Inc.*, 628 F. Supp. 2d 881, 886-87 (N.D. Ill. 2009) (trade secret status precluded where plaintiff failed to take reasonable steps to ensure departing employees returned, destroyed or agreed not to use plaintiff's customer information).

¹⁷³ See William Lynch Schaller, *Trade Secret Law: The Role of Information Governance Professionals*, 18 J. MARSHALL REV. INTELL. PROP. 27, 38-44 (2018) (discussing consequences of owners' failure to retrieve their secrets).

¹⁷⁴ See *Texas Advance Optoelectronic Sol's., Inc. v. Renesas Elec's. America, Inc.*, 895 F.3d 1304, 1314 (Fed. Cir. 2018) (applying Texas law) ("Although it is undisputed that Intersil used

Although a summary judgment decision, *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*,¹⁷⁵ a case decided under Florida law, well illustrates the risk of inadequate secrecy measures. Simplified, the unremarkable facts showed that Barker broke away from Yellowfin to form a rival boat firm, copying hundreds of Yellowfin documents on his last day. Even though Yellowfin employed such familiar secrecy measures as limiting employee access to secrets and using passwords on its computer network, “Yellowfin compromised the efficacy of these measures by encouraging Barker to keep the Customer Information on his cell-phone and personal laptop.”¹⁷⁶ Making matters worse, “Yellowfin neither marked the Customer Information as confidential nor instructed Barker to secure the information on his personal devices. And when Barker left Yellowfin, the company did not request that Barker return or delete any of the information.”¹⁷⁷ The Court of Appeals rejected out of hand Yellowfin’s “implicit understanding” with Barker that its information was to be kept secret: Barker had refused to sign a confidentiality agreement, and there was no evidence corroborating their supposed “implicit understanding.”¹⁷⁸ Given these many secrecy deficiencies, one has to wonder how Yellowfin could have alleged sufficient facts to withstand a Rule 12(b)(6) motion challenging the reasonableness of its secrecy measures.

“Bring your own devices” (BYOD) is a serious security problem at many companies,¹⁷⁹ and it seemed to be the problem in *Yellowfin Yachts* to the extent Barker was using his own devices for his massive, last-minute copying efforts.¹⁸⁰ The truth is companies often exercise little or no control over information stored on such devices. It is not hard to imagine an employer pleading itself out of court by referring to personal cell phones and personal laptops without alleging

TAOS’s information for the ‘Build vs. Buy’ analysis, that use was contractually permitted and therefore not a proper basis of liability for trade secret misappropriation.”); James H. Pooley, *Trade Secret Diligence in M & A*, LANDSLIDE, July/August 2019, at 14-16 (2019) (discussing pro-buyer nondisclosure agreement terms designed to protect against “information contamination,” including “residuals” clause allowing the putative buyer to develop its own competing products, to shop for other firms, and to use information retained in the “unaided memory” of its employees).

¹⁷⁵ *Yellowfin Yachts, Inc. v. Barker Boatworks, LLC*, 898 F.3d 1279 (11th Cir. 2018).

¹⁷⁶ *Id.* at 1300.

¹⁷⁷ *Id.*

¹⁷⁸ *Id.*

¹⁷⁹ See The Sedona Conference, *The Sedona Conference Commentary on BOYD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations*, 19 SEDONA CONF. J. 495, 516-17 (2018) (“Traditional risks from theft, hacking, and user negligence are ever present on an organization’s non-BYOD devices and networks. BYOD enhances those risks, however, because technical and administrative protections are substantially more difficult to develop and implement in a BYOD environment.”); Hope A. Comisky & Tracey E. Diamond, *The Risks and Rewards of a BYOD Program: Ensuring Corporate Compliance Without Causing ‘Bring Your Own Disaster’ at Work*, 8 CHARLESTON L. REV. 385, 395-401 (2014) (discussing need for and limitations of confidentiality agreements and BYOD policies in protecting trade secrets).

¹⁸⁰ See *Yellowfin Yachts*, 898 F.3d at 1300.

that company confidentiality legends were stored on those devices and/or without alleging return or destruction of company information kept on those devices. A clever defendant might convince a sympathetic court that confidentiality legends and return of property are essential allegations when an employer admits unfettered use of BYOD devices occurred.

Very much related to this BYOD problem, and perhaps a more serious concern on a Rule 12(b)(6) motion to dismiss, is overclaiming of secrecy. Sophisticated trade secret owners know their information will end up on company-sponsored *and* BYOD devices; it's how business is done today. They also know not all devices will be collected and scrubbed when business relationships end, despite well-intentioned exit interviews and reminder letters. For mid-level managers and corporate IT staff, the knee-jerk reaction is prophylactic: at least make sure to mark everything "confidential" or "trade secret." Is this a prudent practice, or is it fatal overclaiming?

As an example, let's look at *GlobalTap LLC v. Elkay Mfg. Co.*,¹⁸¹ a Chicago federal court case involving sophisticated parties and a sophisticated judge. Greatly simplified, GlobalTap developed a bottle-filling station design for vertically held bottles, approached Elkay about manufacturing and selling its proposed station, and then entered into an elaborate confidentiality agreement with Elkay in February 2009. Among other things, GlobalTap shared a confidential business plan spanning some 101 pages. The relationship soured the following year for a variety of reasons, especially after Elkay released a similar product of its own in 2010, and litigation ensued. Multiple secrets were at issue, and the parties battled intensely over identification during discovery. I want to emphasize a single secret in the interest of analytic clarity — the mega-business plan — because it represents the risk of overclaiming: rejection. Here is the district court's evaluation of the 101-page plan:

Elkay argues that GlobalTap has not met its burden because the Business Plan and other documents are "general areas of information," not concrete or particularized secrets. The list of corporate and municipal partners is insufficiently specific, Elkay continues, because "GlobalTap has not identified what aspect of a mere existence of a relationship with a third party is actually protectable as a trade secret." (Elkay's Mem. of Law in Supp. of its Mot. for Summ. J. [88-4], hereinafter "Elkay's Mem.," 11.) The court agrees. In *IDX*, the Seventh Circuit held that a 43-page description of a software program was insufficient because it included items such as descriptions of the appearances of computer screens that were readily ascertainable and the plaintiff did not specify any line of computer code or an algorithm that might actually be a trade secret. [*IDX Systems Corp v. Epic Systems*

¹⁸¹ *GlobalTap LLC v. Elkay Mfg. Co.*, No. 13 C 632, 2015 WL 94235 (N.D. Ill. Jan. 5, 2015).

Corp., 285 F.3d 581, 584 (7th Cir. 2002)]. With respect to the information in the Business Plan in this case, GlobalTap has done nothing more than point to the entire 101-page document. Even more broadly, Mr. Whitman testified that “every word” in the Business plan is a GlobalTap trade secret. (30(b)(6) Dep. of Mr. Whitman, Ex. C to Smolczynski Decl., hereinafter “30(b)(6) Whitman Dep.,” 48:10-13.)

Plaintiff’s vagueness is fatal to its claim for trade secret protection of its Business Plan. Plainly, much of the information contained in that Plan is not a GlobalTap trade secret. For example, the Business Plan includes statistics on “global water issues” from the Blue Planet Run Foundation, such as the fact that “unsafe drinking water is the world’s leading cause of death” and that “one in six of all humans. . . lack safe drinking water.” (Business Plan at 23.) Another page provides examples of governments around the world that have regulated bottled water. (*Id.* at 25.) Finally, another page includes a cartoon sourced from “cartoonstock.com.” (*Id.* at 57.) GlobalTap has merely pointed to the 101-page Business Plan and “invited the court to hunt through the details in search of items meeting the statutory definition.” *IDX*, 285 F.3d at 584. There may well be trade secrets within the 101-page Business Plan, but it was Plaintiff’s burden to identify those secrets and it has repeatedly failed to do so.¹⁸²

“Every word” of it? GlobalTap was too clever by half I would say, as would some Courts of Appeals.¹⁸³ Instead of covering all of the bases, GlobalTap ended up covering none. Now imagine if the same business plan had been attached (under seal) to the complaint, as I contend *Twombly* and *Iqbal* mandate. Would it have survived a Rule 12(b)(6) motion to dismiss? Much of its information was plainly public domain material lacking any “economic value” and therefore unprotectable under any theory. Further, what little of it that could have warranted protection was not isolated and highlighted as “confidential.” These were not reasonable secrecy measures as a matter of law; hence the *GlobalTap* court’s grant of summary judgment in favor of the defense.

All of this takes us back to where we started: “identification.” If federal Courts of Appeals read *Twombly* and *Iqbal* as I do, they may demand identification not only in the complaint, but at the time of access as well — as part of their

¹⁸² *Id.* at *6-*7.

¹⁸³ *See, e.g.,* *Methodist Hosp., Inc. v. Sullivan*, 91 F.3d 1026, 1032 (7th Cir. 1996) (Easterbrook, J.) (“To say that particular *information* is confidential is not to say that the entire document containing that information is confidential.”).

“reasonable secrecy” analyses.¹⁸⁴ Some companies have hundreds or even thousands of secrets,¹⁸⁵ and identification during business relationships will no doubt be a burden for them. Limiting identification to actual secrets without overclaiming will place an even greater burden on them. But who should bear the risk of failure to mark or — in some ways worse — overmarking? The company that owns the secrets, that claims them as “crown jewels,” and that employs computers and administrators galore to protect them? Or hapless employees and other authorized users who only know what they are told? In all instances, the question reduces to the sufficiency of notice, and generalized descriptions are no more useful in business settings than in litigation settings. Indiscriminately stamping everything “confidential” suffers from the same flaw; it is an inherently “unreasonable” practice that shields information with “no economic value.” Worse, it has an enormous negative value — it impedes employee mobility, casts a cloud over competition, and enables false pleading. Here I part company with Judge Posner. If someone is to be placed on the “razor’s edge” in the event of “overclaiming,” as he put it in *Rockwell Graphic Systems*,¹⁸⁶ it ought to be the one

¹⁸⁴ See, e.g., *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 902 (N.D. Ill. 2019) (“It takes virtually no effort and little sophistication to include a header on an Excel spreadsheet identifying a document as ‘proprietary’ or ‘confidential,’ yet [plaintiff] CGW failed even to do that much with respect to the information at issue in this case.”); Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA: THE INTELL. PROP. L. REV. 359, 365 (2009) (“Trade secret owners should work to ensure that those to whom they do grant access know that particular information is confidential. One way to do so is by explicitly legending highly confidential documents with precautionary language warning that they are not to be used or disclosed except as authorized by the identified owner. Such legends may help reduce improper disclosures. They may also help a victimized trade secret owner establish that an unauthorized third-party recipient of the trade secret had ‘reason to know’ that it was not free to use them, a necessary step to prevail on a claim under the Uniform Trade Secrets Act.”) (footnote omitted).

¹⁸⁵ See, e.g., *TianRui Grp. Co. v. Int’l Trade Comm.*, 661 F.3d 1322, 1325 (Fed. Cir. 2011) (“Following a 10-day evidentiary hearing, the administrative law judge found that TianRui had misappropriated 128 trade secrets relating to the ABC process from Datong.”); *E.I. DuPont de Nemours & Co. v. Kolon Indus., Inc.*, No. 12-1260, slip op. at 3 (4th Cir. Apr. 3, 2014) (per curiam) (“After a seven-week trial, the jury returned a verdict finding that Kolon willfully and maliciously misappropriated 149 DuPont trade secrets and awarded DuPont \$919.9 million in damages.”).

¹⁸⁶ *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 176-77 (7th Cir. 1991) (Posner, J.):

DEV suggests that if a firm claims trade secret protection for information that is not really secret, the firm forfeits trade secret protection of information that is secret. There is no such doctrine—even the patent misuse doctrine does not decree forfeiture of the patent as the sanction for misuse—and it would make no sense. This is not only because there are any number of innocent explanations for Rockwell’s action in “overclaiming” trade secret protection (if that is what it was doing)—such as an excess of caution, uncertainty as to the scope of trade secret protection, concern that clerical personnel will not always be able to distinguish between assembly and piece part drawings at a glance, and the sheer economy of a uniform

in the best position to mitigate the risk – the owner. This should be true of all businesses, large and small.¹⁸⁷

F. ALLEGING MISAPPROPRIATION

Misappropriation is much trickier to allege than the existence of a trade secret. Every plaintiff knows why it thinks defendant has taken or wrongfully obtained its secrets, but the accused's conduct is usually cloaked, and thus plaintiff's beliefs are almost always uncertain. Compounding the problem, every defendant knows what it did and didn't do, thereby enabling defendants to point with precision to what's missing from or hazy in the complaint with respect to defendant's supposed misappropriation. So begins a game of cat and mouse at the pleadings stage.

Misappropriation actually presents two inquiries. First, did defendant have access to plaintiff's secrets? Second, if so, did defendant knowingly and wrongfully obtain, disclose or use them, i.e., steal them itself or acquire them through someone else's theft and then disclose or use them?¹⁸⁸ Sometimes these separate questions converge and become difficult, as seen in cases where a person with authorized access mysteriously begins accessing secrets on the eve of departure,¹⁸⁹ but more often the first is easy to answer. Still, the first question needs to be asked because every now and then it turns out a defendant had no access to the secrets — a recipe for disaster when the plaintiff has alleged the

policy—but also because it would place the owner of trade secrets on the razor's edge. If he stamped “confidential” on every document in sight, he would run afoul of what we are calling (without endorsing) the misuse doctrine. But if he did not stamp confidential on every document he would lay himself open to an accusation that he was sloppy about maintaining secrecy—and in fact DEV's main argument is that Rockwell *was* impermissibly sloppy in its efforts to keep the piece part drawings secret.

¹⁸⁷ Cf. Jermaine S. Grubbs, Note, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the “Reasonable Efforts” Taken by Small Businesses Should Be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421, 437-38 (2005) (“Courts should first determine whether the small business seeking trade secret protection was able to identify the information as requiring or being subject to trade secret protection. If the small business was reasonably able to identify the information as a potential trade secret, the small business will have a heavier burden to show why it did not employ protective measures to maintain the secrecy of the information. If the small business was not reasonably able to identify the information as a potential trade secret, the burden on the small business to show that its efforts were reasonable will be lessened.”).

¹⁸⁸ See Aarti K. Wilson, *What to Expect When You're (Not) Expecting Misappropriation*, LANDSLIDE, July/August 2019, at 20 (“Misappropriation can take three forms: (1) improper taking, (2) improper use, or (3) improper disclosure, and the degree of ‘improper’ conduct can run the gamut.”).

¹⁸⁹ See, e.g., *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) (discussing whether departing employee exceeded authorized access to company computers by downloading confidential information shortly before quitting to join a rival); *WEC Carolina Energy Sol's, LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012) (same); *Int'l Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (same).

opposite.¹⁹⁰

The far harder issue is whether plaintiff has enough facts to allege a knowing and wrongful taking, disclosure, or use. As I discussed earlier, “plausible on its face” for misappropriation purposes must mean something more than just accessing someone’s secrets and then leaving them to compete. Otherwise, all employee mobility cases would become employee liability cases and all business separation cases would become business reparation cases.¹⁹¹ So the question is how much more, which takes us along the actual/threatened/inevitable continuum.¹⁹² Actual theft is easy if someone is lucky enough to see it;¹⁹³ threatened theft is simple if someone is dumb enough to say it;¹⁹⁴ and inevitable theft is impossible — at least in injunction cases brought solely under the DTSA against employees — because Section 1836 bars it.¹⁹⁵ But what about the far more common case of clandestine conduct?

¹⁹⁰ See, e.g., *Wolters Kluwer Fin. Servs., Inc. v. Scivantage*, 525 F. Supp. 2d 448 (S.D.N.Y. 2007) (publicly reprimanding attorney and plaintiff Wolters Kluwer where trade secret case proceeded through discovery and multiple hearings over defendants’ protest at the outset that as management-level employees they had no access to plaintiff’s computer code — a defense objection the court later determined to be valid), *aff’d in part and rev’d in part*, 564 F.3d 110 (2d Cir. 2009).

¹⁹¹ See William Lynch Schaller, *Method Matters: Statutory Construction Principles and the Illinois Trade Secrets Act Preemption Puzzle in the Northern District of Illinois*, 39 N. ILL. U. L. REV. 195 (2019) (surveying approximately 50 Illinois federal district court opinions that struggled with trade secret and related claims in a wide range of employee mobility and business divorce settings).

¹⁹² See William Lynch Schaller, Russell Beck & Randall E. Kahnke, *Trade Secret “Triggers”: What Facts Warrant Litigation?*, 19 SEDONA CONF. J. 625 (2018) (analyzing jumping ship, inevitable disclosure, and failed deal scenarios as the most common fact patterns giving rise to trade secret misappropriation claims).

¹⁹³ See *United States v. Williams*, 526 F.3d 1312, 1316, 1318 (11th Cir. 2008) (Coca-Cola Company executive assistant, caught on camera stealing trade secrets, sentenced to ninety-six months in prison); *United States v. Yang*, 281 F.3d 534, 540–41 (6th Cir. 2002) (recounting FBI “sting” operation in which defendants were caught on camera exchanging Avery Dennison documents marked “confidential”).

¹⁹⁴ See *FLIR v. Parrish*, 174 Cal. App. 4th 1270, 1279 (2009) (“[T]hreatened misappropriation’ means a threat by a defendant to misuse trade secrets, manifested by words or conduct, where the evidence indicates imminent misuse.”); *B.F. Goodrich Co. v. Wohlgemuth*, 192 N.E.2d 99, 104 (Ohio Ct. App. 1963) (enjoining trade secret misappropriation threatened by B.F. Goodrich employee Wohlgemuth, who when resigning said “loyalty and ethics had their price: insofar as he was concerned, [his new employer] was paying the price”); *CITIZEN ESPIONAGE: STUDIES IN TRUST AND BETRAYAL* 136 (Theodore R. Sarbin et al. eds., Praeger Publishers 1994) (“Few employees are so forthcoming as Wohlgemuth about the way they see things; or, at least, what employees say and think almost never finds its way into appellate court opinions.”)

¹⁹⁵ 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2018) (court may issue an injunction to prevent actual or threatened misappropriation, provided the order does not “prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows”).

The misappropriation element was not at issue in *Plastronics*, but it was very much at issue in *Molon Motor*,¹⁹⁶ an Illinois case decided in 2017 on a Rule 12(b)(6) motion. *Molon Motor* is especially illuminating because it implicated all facets of misappropriation. Somewhat simplified, the facts were typical: Desai, Head of Quality Control for Molon Motor, had access to all Molon trade secrets through his work computer; Desai allegedly copied confidential Molon data onto a Kingston thumb drive; and Desai then decamped to rival Nidec Motor, “taking up responsibilities similar to those he had at Molon.”¹⁹⁷ Molon set forth the thumb drive-copied secrets in a sealed appendix to its third amended complaint and established Desai’s secrecy obligations by referencing his employment agreement, which barred the unauthorized use of Molon data. With no trade secret identification and secrecy measures seriously in dispute, Nidec trained its guns on the “plausibility” of Molon’s misappropriation claims, arguing (1) that Desai’s actions did not constitute “misappropriation” under the DTSA or its Illinois state law counterpart, the Illinois Trade Secrets Act (ITSA), and (2) that, even if Desai’s actions did amount to misappropriation, Nidec did not know or have reason to know about Desai’s alleged misappropriation.¹⁹⁸ Desai himself filed nothing; he wasn’t named as a defendant.

The tipping point for the court on the misappropriation question was Desai’s copying of “dozens of Molon’s engineering, design, and quality control files onto a personal Kingston portable data drive” before leaving Molon to join Nidec, conduct the court thought suspicious since Molon did “not provide or use memory sticks for access to its computer network.”¹⁹⁹ This was the thinnest of reeds; Molon corporate policy did not prohibit use of such devices, as the court

¹⁹⁶ *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

¹⁹⁷ *Id.* at *2.

¹⁹⁸ Defendant Nidec Motor Corporation’s Motion to Dismiss Counts III and IV of Plaintiff’s Third Amended Complaint at 2, No. 16-C-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017) (“While Molon does identify the allegedly proprietary information that was allegedly copied in 2013 by Molon’s former employee Manish Desai, Molon still has not pleaded any legitimate basis to assert that these files were wrongfully copied or that NMC was responsible for the acts of Mr. Desai or otherwise misappropriated a trade secret of Molon.”); Defendant Nidec Motor Corporation’s Memorandum in Support of Its Motion to Dismiss Counts III and IV of Plaintiff’s Third Amended Complaint at 7, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2016 WL 6777681 (N.D. Ill. May 11, 2017) (“Molon has no legitimate basis to assert that NMC was responsible for the acts of Mr. Desai in 2013 or that NMC has otherwise misappropriated any of Molon’s trade secrets. Molon provides no specific allegations that could plausibly show that Mr. Desai disclosed the alleged trade secrets to NMC or that NMC otherwise obtained and used any information allegedly copied by Mr. Desai.”); Defendant’s Reply in Support of Its Motion to Dismiss Counts III and IV of Plaintiff’s Third Amended Complaint at 4, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2016 WL 8453840 (N.D. Ill. May 11, 2017) (“Molon has also not provided a plausible basis that NMC ‘knew or had reason to know’ that the alleged trade secrets acquired by Mr. Desai were to be maintained under secrecy.”).

¹⁹⁹ *Molon Motor*, 2017 WL 1954531, at *5.

acknowledged,²⁰⁰ and the propriety of Desai's copying was unclear, as was the timing.²⁰¹ Nonetheless, the court found this memory-stick copying sufficient to draw a plausible inference of misappropriation by Desai, especially since he took a similar position at competitor Nidec, evidently not long after the copying.²⁰² In other words, the court implicitly inferred Desai knew or had reason to know he was acquiring Molon's secrets through "improper means" — breach of his duty to maintain secrecy — implicit because the court did not use the phrase "knew or had reason to know" in so holding. In short, for purposes of evaluating Desai's actions, access and misappropriation were supported by sufficient facts to satisfy *Twombly* and *Iqbal*.

But did these circumstances really show access — much less misappropriation — *by Nidec*, the sole defendant? Nidec certainly didn't think so, but it didn't develop its "knew or reason to know" argument or cite case law glossing this statutory phrase (appearing in both the DTSA and the ITSA), apparently viewing the point as self-evident. These statutes expressly condition liability on a defendant's actual or constructive knowledge that it is stealing secrets or acquiring them from someone who stole them. There was no allegation that Nidec enlisted Desai to act as its mole while he was still a Molon employee, for instance, and there was certainly no allegation that Nidec itself hacked into Molon's computers, broke into Molon's premises, or employed some other improper means to acquire Molon's secrets.²⁰³ Nor was *respondeat superior* alleged against Nidec,

²⁰⁰ *Id.* at *5 n. 12.

²⁰¹ On this timing question, the Third Amended Complaint simply alleged:

On multiple occasions prior to the time Mr. Desai left Molon's employment to begin employment at [Nidec], his computer was accessed under his username and password and a significant amount of files related to the engineering and design, quality control protocols and data, and customer specific data for Molon Motor was copied to a Kingston portable data drive.

Third Amended Complaint at 16, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2016 WL 8453840 (N.D. Ill. May 11, 2017). Nidec's Reply clarified that the "multiple occasions" occurred during "the months preceding [Desai's] June 2013 departure from Molon," citing paragraph 65 of the Third Amended Complaint. Defendant's Reply in Support of Its Motion to Dismiss Counts III and IV of Plaintiff's Third Amended Complaint at 3 n.4, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017). However, the phrase "months preceding" does not actually appear in paragraph 65 or anywhere else in the Third Amended Complaint. *See* Third Amended Complaint, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2016 WL 8453840 (N.D. Ill. May 11, 2017).

²⁰² *Molon Motor*, 2017 WL 1954531, at *5.

²⁰³ *See* DTSA, 18 U.S.C. § 1839(6) (2018) (improper means "include[] theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means"); ITSA, 765 ILL. COMP. STAT. 1065/2(a) (2019) (improper means "include[] theft, bribery, misrepresentation, breach or inducement of a breach of a confidential relationship or other duty to maintain secrecy or limit use, or espionage through electronic or other means"); Matthew B. Kugler & Thomas H. Rousse, *The Privacy Hierarchy: Trade Secret and Fourth Amendment Expectations*, 104 IOWA L. REV. 1223 (2019) (exploring ambiguous

presumably because Desai's misappropriation took place before he joined Nidec, not after. And this assumes vicarious or secondary liability would have been a viable theory — hardly a given in light of the actual or constructive knowledge strictures imposed by the DTSA and the ITSA.²⁰⁴ To rescue Molon's trade secret claims in the absence of these allegations, the court looked to a more controversial theory: the inevitable disclosure doctrine.

G. ALLEGING DISCLOSURE OR USE — AND “INEVITABILITY”

Nidec not only emphasized the complete lack of allegations on actual or constructive knowledge; it also forcefully argued there was “no ground for inferring that it accessed or used any of the information Desai pulled.”²⁰⁵ As noted, some cases treat use, whether actual or threatened, as a separate element of a trade secret misappropriation claim, and the same is true of disclosure.²⁰⁶ It would be more precise to say, however, that that these are simply subsets of misappropriation, along with “acquisition through improper means,” as all three are found in the “misappropriation” definition set forth in the DTSA and the ITSA, and all three are subject to the same “knew or had reason to know” requirement.

applications of “improper means,” including corporate surveillance and investigator deception, and their relationship to “reasonable” secrecy measures).

²⁰⁴ See Tanya J. Dobash, *Trade Secret Theft & Employer Vicarious Liability in Hagen v. Burmeister & Associates, Inc.*, 29 WM. MITCHELL L. REV. 375 (2002) (discussing trade secret vicarious liability under Minnesota law); Robert G. Bone, *Secondary Liability for Trade Secret Misappropriation: A Comment*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 529, 536 (2006) (noting that case law examining *respondeat superior* liability for trade secret theft was “quite thin and the opinions relatively recent” as of 2006 and questioning the need for secondary liability since trade secret theft is not based on strict liability, unlike patent and copyright law). As Professor Bone correctly observed:

The principal trade secret doctrine imposing liability on third parties is in fact based on a form of primary rather than secondary liability. This doctrine holds that a third party is liable when the third party acquires a trade secret from another and then discloses or uses the secret under circumstances where he knows or should have known that the trade secret was wrongfully acquired. The third party is liable for his own use or disclosure, and the knowledge requirement assures some degree of individual culpability.

Id. at 536 (footnote omitted.)

²⁰⁵ *Molon Motor*, 2017 WL 1954531, at *2 (citation omitted).

²⁰⁶ See, e.g., *Lakeview Tech, Inc. v. Robinson*, 446 F.3d 655, 657 (7th Cir. 2006) (applying Illinois law) (district court erred in denying injunctive relief based solely on ex-employee's promise not to disclose secrets in light of employee's previous lies); *Lucini Italia Co. v. Grapolini*, 288 F.3d 1035, 1038 (7th Cir. 2002) (applying Illinois law) (“voluntary cessation” defense should be rejected in trade secret case unless there is no reasonable chance the wrongful use or disclosure will be repeated, and the defense bears the burden of proof); *Metallurgical Indus. Inc. v. Fourtek, Inc.* 790 F.2d 1195, 1204-05 (5th Cir. 1986) (applying Texas law) (discussing meaning of “disclosure” and “use” in trade secret law with reference to §757 of the Restatement of Torts).

The difference is that disclosure or use can trigger a claim against a third party who *did not* steal the secrets, so long as the third party knew or had reason to know the secrets it was using or disclosing were acquired by someone else through improper means.

In response to Nidec's "no use" argument, Molon invited the court to visit the inevitable disclosure doctrine embraced by the Seventh Circuit in its famous preliminary injunction decision, *PepsiCo, Inc. v. Redmond*.²⁰⁷ Nidec put up a furious fight on this issue, arguing (1) that Desai's role at Nidec did not materially overlap his role at Molon and hence presented an insufficient threat of "inevitability," (2) that the district court's own decision in *Saban v. Caremark Rx, L.L.C.*²⁰⁸ had rejected a comparable "inevitability" claim because the executive's responsibilities at the old and new employers there were dissimilar, and (3) that unlike other inevitable disclosure cases, here the new employer was sued but the purportedly dangerous employee was not.²⁰⁹

The court accepted Molon's invitation to tour the wondrous world of ITSA inevitable disclosure case law – case law that arguably allowed the court to infer access, use, and knowledge on Nidec's part.²¹⁰ From its reading of *PepsiCo* and other Illinois inevitable disclosure cases, the court found that two of three required factors were demonstrated: (1) the employee's old and new employers were competitors, and (2) the employee's old and new positions were comparable. Factor (3), whether the new employer has taken steps to prevent the incoming employee from using or disclosing the former employer's trade secrets, was plainly *not* alleged, yet the court allowed the third amended complaint to survive:

On the third factor that courts examine when deciding whether the inevitable disclosure doctrine has been triggered, namely, actions the new employer has taken to prevent the incoming employee from using or disclosing the former employer's trade secrets, the record is silent. At this stage of the litigation, that silence is not surprising, because a complaint is not likely to

²⁰⁷ *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262 (7th Cir. 1995) (affirming inevitable disclosure injunction under ITSA against ex-employee who left to take a directly competing position).

²⁰⁸ *Saban v. Caremark Rx, L.L.C.*, 780 F. Supp.2d 700 (N.D. Ill. 2011).

²⁰⁹ Defendant's Reply in Support of Its Motion to Dismiss Counts III and IV of Plaintiff's Third Amended Complaint at 4–9, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16-C-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

²¹⁰ *See, e.g.*, *Archer Daniels Midland Co. v. Sinele*, 139 N.E.3d 1036, 1042-44 (Ill. App. Ct. 2019) (discussing nuances of inevitable disclosure doctrine under the ITSA, and distinguishing *PepsiCo* as involving an employee who joined a direct competitor, in reversing trade secret injunction against employee who left to become a general broker); *Destiny Health, Inc. v. Conn. Gen. Life Ins. Co.*, 39 N.E.3d 275 (Ill. App. Ct. 2015) (rejecting ITSA inevitable disclosure claim against company that declined deal and later emerged with a new partner); *Strata Mktg., Inc. v. Murphy*, 740 N.E.2d 1166 (Ill. App. Ct. 2000) (denying motion to dismiss complaint alleging ITSA claim against employee who left to take a directly competing position).

contain any allegations about what, if anything, the competitor did to safeguard the plaintiff's secrets.

All told, Molon's allegations on the direct competition between the parties, as well as the allegations on the employment breadth and similarity of Desai's quality control work at the two companies, are enough to trigger the circumstantial inference that the trade secrets inevitably would be disclosed by Desai to Nidec. To be sure, going forward, Molon ultimately will bear the burden of *proving*—not just alleging—enough facts such that disclosure is not premised on a mere unsubstantiated fear. *PepsiCo, Inc.*, 54 F.3d at 1268-69; *Saban*, 780 F. Supp. 2d at 734; *Teradyne*, 707 F. Supp. at 357. For now, Molon has pled enough for the trade secrets claims to avoid the Rule 12(b)(6) chopping block.²¹¹

I leave for another day whether this three-factor test really represents the inevitable disclosure doctrine under the ITSA; you won't find its paternity in the Seventh Circuit's *PepsiCo* decision from which *Molon Motor* and other decisions claim descent, as the *Molon Motor* court itself conceded.²¹² What is more important for our purpose here was the *Molon Motor* court's uncertainty over which facts suffice to state an inevitable disclosure misappropriation claim against a new employer, a question the court acknowledged as the "closest" in the case.²¹³ Inferring Nidec's access was easy given Desai's hiring and his alleged copying. The court's hesitancy on the remaining issues, however, was understandable: Nidec's disclosure, use, and actual or constructive knowledge were all shrouded in mystery at the pleadings stage. Even assuming the inevitable disclosure doctrine satisfied the disclosure or use requirement, it plainly did not meet the knowledge prong of the DTSA and ITSA with respect to Nidec, and neither did Molon's conclusory knowledge allegations:

58. Nidec Motor, through its subsidiaries and divisions, knew or should have known that the employees they hired from Molon would be covered by employment contracts with restrictive covenants. Despite this knowledge, Nidec Motor conspired with a former Molon employee after he voluntarily terminated his position at Molon to engage in unfair and unlawful competition with Molon, namely, Manish Desai who was Molon's Head of

²¹¹ *Molon Motor*, 2017 WL 1954531 at *7 (footnote 18 omitted).

²¹² *See id.* at *5 n.13 ("It is worth noting that calling a line of reasoning a 'doctrine' poses the risk of ossifying the 'factors' into a rigid test. At bottom, whether a trade secret would be inevitably disclosed is really a question of circumstantial evidence, and those types of questions defy straitjacket formulas.")

²¹³ *Id.* at *5.

Quality Control and left Molon to go to [Nidec predecessor] Merkle-Korff in June 2013.

59. Upon information and belief, Nidec Motor has used and disclosed Molon's trade secrets and confidential information in violation of both Federal law and the law of the State of Illinois.

....

67. Upon information and belief, Mr. Desai unlawfully disclosed Molon's trade secrets, that he had wrongfully copied from his Molon work computer. Mr. Desai left Molon for employment in a similar position with Molon's competitor and Nidec Motor's predecessor, Merkle-Korff. Under these circumstances, given Mr. Desai's prior employment with Molon and his wrongful copying of Molon's trade secrets . . . Nidec Motor's use of the trade secrets can be inferred under the "inevitable disclosure doctrine."²¹⁴

As these paragraphs show, there were no alleged facts *relating to Nidec* which, if believed, made Nidec's knowledge more likely than not, or "plausible," as *Twombly* and *Iqbal* put it. Desai's "restrictive covenant" was just a confidentiality agreement, the "conspiracy" was just his hiring, Molon's "information and belief" was just a conclusion, and Desai's "inevitable disclosure" spoke to his conduct, not Nidec's "knowledge." These deficiencies no doubt account for the court's failure to analyze the factual basis for Nidec's supposed knowledge at the start of its misappropriation discussion as well as the court's own conclusory treatment of Nidec's knowledge at the very end of its opinion:

The next question arises from the second half of the federal and Illinois trade secrets acts' "misappropriation" definition: did Nidec know or have reason to know that the trade secret was acquired by "improper means"? Nidec argues that Desai's behavior does not fit this definition. Nidec's Mot. to Dismiss at 6. It contends that Desai's access to the files in the Molon computer system was authorized. *Id.* To Nidec's way of thinking, nothing improper happened because Desai was still an employee when he put the data on the thumb drive, and used his normal username and password to get access. *Id.* So even if what Desai

²¹⁴ Third Amended Complaint at 15, 17, *Molon Motor and Coil Corp. v. Nidec Motor Corp.*, No. 1:16-CV-03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

took was ultimately a trade secret, he did not, in Nidec's view, take it through "improper means." . . .

. . . .

. . . Molon need not allege that Nidec was responsible for Desai's downloading *at the time* it happened in order to state a claim for trade secret misappropriation. It is enough that Desai (allegedly) later disclosed the information to Nidec and that Nidec made use of it, knowing (or having reason to know) that the secrets were acquired by improper means.²¹⁵

Whether intentionally or not, the court conflated Nidec's argument about Desai's lack of "improper conduct" at Molon with Nidec's separate argument about Nidec's lack of knowledge concerning Desai's improper conduct at Molon. Again the court begged the question of Nidec's knowledge when, at the end of its opinion, it offered a series of *non sequiturs* to the effect (1) that Molon did not have to allege Nidec urged Desai to steal while Desai was still at Molon (true but irrelevant to Nidec's knowledge); (2) that Molon alleged Desai later inevitably disclosed Molon's information to Nidec (true but irrelevant to Nidec's knowledge); and (3) that Molon alleged Nidec made use of this information (true but irrelevant to Nidec's knowledge). These allegations and non-allegations may have sufficiently shown Desai's guilty knowledge, but they did nothing, without more, to distinguish innocent acquisition from wrongful acquisition *on Nidec's part*, and Nidec was the only defendant.²¹⁶

In *Twombly* terms, these allegations offered a state of equipoise: there were no facts alleged which, if believed, made it "plausible," meaning more likely than not, that Nidec knew or had reason to know there was something amiss with what Desai was doing while at Molon, or for that matter, that Nidec knew or had reason to know there was something amiss with what Desai was doing while at Nidec. These were no small omissions, given the Supreme Court's subsequent holding in *Iqbal* that the complaint there did not "contain any factual allegation sufficient to plausibly suggest petitioners' discriminatory state of mind."²¹⁷ Indeed, the Supreme Court in *Iqbal* made it clear that even when a pleading rule otherwise allows plaintiff to allege a person's state of mind generally — as Rule

²¹⁵ *Molon Motor*, 2017 WL 1954531, at *4, *7 n.18.

²¹⁶ Innocent acquisition takes on even more significance when defendants are further removed from the original thief, as with downstream defendants who unknowingly acquire infected products and are later advised that the products are "derived" from stolen secrets. See generally Benjamin J. Bradford & Remi Jaffre, *The Uncertain Protection of "Derivative" Trade Secrets*, 18 J. MARSHALL REV. INTELL. PROP. L. 241 (2019).

²¹⁷ *Ashcroft v. Iqbal*, 556 U.S. 662, 683 (2009); cf. *Intel Corp Investment Policy Committee v. Sulyma*, 140 S. Ct. 768, 779 (2020) (discussing proof of "actual knowledge" under ERISA, including proof through "circumstantial evidence" and proof of "willful blindness").

9(b) does — that “does not require courts to credit a complaint’s conclusory statements without reference to its factual context.”²¹⁸

The proper course, then, was for the *Molon Motor* court to dismiss Nidec. This straightforward outcome was made difficult by Molon first suing Nidec instead of Desai, thereby running the risk of Nidec being dismissed with prejudice and *res judicata* attending that dismissal. This is not to say that plaintiff must always skip the new employer and first sue the ex-employee; if plaintiff has enough facts against the new employer,²¹⁹ it need not sue the ex-employee first or at all.²²⁰ But the safer approach would have been for Molon to sue Desai, to depose him about his conduct with Nidec and Nidec’s knowledge of that conduct, and then to add Nidec as a defendant based on newly-discovered and now-alleged facts showing Nidec’s role and knowledge.²²¹ Indeed, the reverse sequence — suing the new employer first without adequate facts — could amount in many cases to “sue first, investigate later,” a prescription for Rule 11 sanctions.²²² To repeat: “It may be that little more is needed, but falling a little short is still

²¹⁸ *Iqbal*, 556 U.S. at 686; *accord* *CleanFish, LLC v. Sims*, No. 19-CV-03663-HSG, 2020 WL 1274991, at *8, *10 (N.D. Cal. Mar. 17, 2020) (in case brought under D’TSA and California law, citing *Iqbal* at the outset of its Rule 12(b)(6) analysis and then later ruling that no facts were alleged to show the Island Sea Farm defendants, as mere suppliers to defendant Sims, knew or had reason to know Sims had stolen trade secrets from his former employer, plaintiff CleanFish: “Plaintiff must allege facts that . . . tend to exclude an innocent explanation.”) (internal citations omitted).

²¹⁹ *Cf. Experian Info. Sols., Inc. v. Nationwide Mktg. Servs. Inc.*, 893 F.3d 1176, 1188-89 (9th Cir. 2018) (applying Arizona law) (reversing summary judgment and holding that Experian could sue Nationwide for trade secret theft due to suspicious circumstances under which Nationwide acquired its data closely resembling Experian’s secret data — even though Experian had not sued the person or firm that sold the data to Nationwide).

²²⁰ See *In re Muhs*, 923 F.3d 377, 380 (4th Cir. 2019) (discussing bankruptcy litigation arising out of plaintiff’s trade secret theft suit against its ex-employee Muhs, under a collateral estoppel theory, after plaintiff first obtained a \$20 million trade secret theft judgement against Muhs’ new employer); Dara Kerr, *Ex-Uber Engineer Levandowski Ordered to Pay Google \$179 Million*, CNET (Mar. 5, 2020), <https://www.cnet.com/news/ex-uber-self-driving-car-head-ordered-to-pay-google-179-million/> (reporting court confirmation of Google’s \$179 million trade secret theft arbitration judgement against Anthony Levandowski after Google first obtained a \$245 million settlement with Uber in earlier trade secret theft litigation).

²²¹ See *Comput. Assoc. Int’l, Inc. v. Altai, Inc.* 982 F.2d 693, 718-20 (2d Cir. 1992) (extended discussion of evidence suggesting Altai knew or had reason to know that its new employee, Arney, was using his ex-employer Computer Associates’ source code to develop source code for Altai); *Union Carbide Corp. v. UGI Corp.*, 731 F.2d 1186, 1191 (5th Cir. 1984) (inferring AmeriGas’ knowledge because AmeriGas “took no precautions to insulate Sutton from [the] strategy meetings” concerning his ex-employer Carbide’s secret pricing); William Lynch Schaller, *Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiff’s Perspective*, 29 REV. LITIG. 729, 761-71 (2010) (discussing tactical considerations in choosing theories and defendants in trade secret misappropriation cases).

²²² See *Bus. Guides, Inc. v. Chromatic Commc’ns. Enters., Inc.*, 498 U.S. 531, 537-38, 554 (1991) (witness and law firm assumed, without investigating, that affidavit describing business directory information was accurate when it was not, triggering Rule 11).

falling short.”²²³

H. INEVITABLE DISCLOSURE AND THE DTSA

I have deconstructed *Molon Motor* at the risk of belaboring it because its intersection with *Twombly* highlights some problematic aspects of deploying the inevitable disclosure doctrine in DTSA cases. Five stand out.

First, as noted, *Molon Motor* is one of the few inevitable disclosure cases where a new employer was sued but not the employee who jumped ship, a fact properly flagged by Nidec in its Rule 12(b)(6) motion. Even if one believes inevitable disclosure is a useful gap-filler under state law, it only fills gaps against certain employees and only does so under certain state laws. All or nearly all such cases, however, never dwell on the “knows or had reason to know” language found in the UTSA (and the ITSA, and now the DTSA), apparently on the unstated assumption that the targeted employees necessarily know or have reason to know they will inevitably disclose or use their former employers’ trade secrets even when their intentions are benign. This assumption is not self-evident.²²⁴

Second, even assuming employees can be said to know what they’re doing in these cases, the same knowledge level cannot be attributed to their new employers, who rarely have independent access to another employer’s secrets and thus are in no position to know what’s in a new employee’s seemingly well-intentioned head. *PepsiCo* itself was such a case; there was no discussion of whether (much less how) Quaker Oats, the new employer, knew or had reason to know what Redmond was about to inevitably disclose, although Quaker Oats took prophylactic steps to prevent disclosure of whatever PepsiCo secrets Redmond might have possessed.²²⁵ Indeed, a close reading of *PepsiCo* reveals no explicit discussion of how Redmond’s own plight met the “knows or had reason to know”

²²³ *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1269 (7th Cir. 1995) (quoting *Teradyne, Inc. v. Clear Commc’ns. Corp.*, 707 F. Supp. 353, 357 (N.D. Ill. 1989)).

²²⁴ See *C & F Packing Co. Inc. v. IBP, Inc.*, No. 93 C 1601, 1998 WL 1147139, at *8 -*9 (N.D. Ill. Mar. 16, 1998) (offering *verbatim* questions and answers showing that ex-employee McDaniel tried to honor his confidentiality obligations owed to C & F Packing, that if he violated them “it was completely unintentional,” and that he did not knowingly draw on his C & F Packing experience: “I tried to keep things separate. Whether I did it unknowingly or not, I cannot say.”); Charles Tait Graves, *Is There an Empirical Basis for Predictions of Inevitable Disclosure?*, 18 WAKE FOREST J. BUS. & INTELL. PROPERTY L. 190, 193 (2018) (highlighting lack of expert testimony on, and lack of empirical basis for, assumption that ex-employees will inevitably disclose secrets upon joining a competitor).

²²⁵ *PepsiCo*, 54 F.3d at 1266 (“The defendants also pointed out that Redmond had signed a confidentiality agreement with Quaker preventing him from disclosing ‘any confidential information belonging to others,’ as well as the Quaker Code of Ethics, which prohibits employees from engaging in ‘illegal or improper acts to acquire a competitor’s trade secrets.’ Redmond additionally promised at the hearing that should he be faced with a situation at Quaker that might involve the use or disclosure of PCNA information, he would seek advice from Quaker’s in-house counsel and would refrain from making the decision.”).

standard, even though the Court of Appeals cited that standard in its opinion.²²⁶ So understood, inevitable disclosure, at least in its “pure” form (meaning switching jobs without bad acts or bad intent), is a form of unwitting conduct and thus the very opposite of the conscious wrongdoing contemplated by the UTSA and now the DTSA.²²⁷ Given this explicit statutory “knowledge” requirement, given its location in a criminal statute, and given the rule of lenity, it remains a very real possibility the Supreme Court will reject inevitable disclosure under the DTSA as a matter of statutory construction based upon the statutory definition of misappropriation alone.²²⁸

²²⁶ *Id.* at 1268 n.6.

²²⁷ To borrow from Jeffrey Kang et al., *Implicit Bias in the Courtroom*, 59 U.C.L.A. L. REV. 1124, 1160 (2012) (commenting on discrimination litigation), “[W]hen judges turn to their judicial experience and common sense [as commanded by *Twombly* and *Iqbal* on Rule 12(b)(6) motions], what will this store of knowledge tell them about whether some particular comment or act happened and whether such behavior evidences legally cognizable [misappropriation]?” Or as psychologist William James said long ago, “a great many people think they are thinking when they are merely rearranging their prejudices.” Emily Bobrow, *The Intelligence Trap: Review: How Smart Is Too Smart?*, WALL ST. J. (Aug. 5, 2019 6:49 PM), <https://www.wsj.com/articles/the-intelligence-trap-review-how-smart-is-too-smart-11565045370>. There are more than a few doubters about the “science” behind implicit bias in general and inevitable disclosure in particular. See Jesse Singal, *The Creators of the Implicit Association Test Should Get Their Story Straight*, INTELLIGENCER (Dec. 5, 2017), <http://nymag.com/intelligencer/2017/12/iat-behavior-problem.html> (collecting methodological criticisms of Implicit Association Test widely assumed to predict implicit bias on racial matters); Gregory Mitchell & Philip E. Tetlock, *Facts Do Matter: A Reply to Bagenstos*, 37 HOFSTRA L. REV. 737 (2009) (reviewing then-existing literature on Implicit Association Test); Michael Noon, *Pointless Diversity Training: Unconscious Bias, New Racism and Agency*, Debates & Controversies (2018), <https://journals.sagepub.com/doi/pdf/10.1177/0950017017719841> (reviewing the literature and questioning the value and use of implicit bias training); Graves, *supra* note 224 (questioning evidentiary basis for the inevitable disclosure assumption that honest employees will disclose secrets upon joining a competitor).

²²⁸ See, e.g., *Rehaif v. United States*, 139 S. Ct. 2191, 2196 (2019) (“Scienter requirements advance this basic principle of criminal law by helping to ‘separate those who understand the wrongful nature of their act from those who do not.’”) (quoting *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 72-73 n.3 (1994)); *Morisette v. United States*, 342 U.S. 246, 251 (1952) (defendant must be proven to have known the facts that made conversion wrongful, meaning they had not been abandoned by its owner; in the Anglo-American legal tradition, crime is “generally constituted only from concurrence of an evil-meaning mind with an evil-doing hand”); *United States v. Ford*, 821 F.3d 63, 73 (1st Cir. 2016) (analyzing jury instruction using the “knew or had reason to know” formulation and distinguishing “know” from “reason to know,” as the latter “suggests a negligence standard”); Paul Larkin, Jr., Jordan Richardson & John-Michael Seibler, *The Supreme Court on Mens Rea: 2008-2015*, THE HERITAGE FOUND. (Jan. 14, 2016), <https://www.heritage.org/courts/report/the-supreme-court-mens-rea-2008-2015> (“Oliver Wendell Holmes, Jr., was on to something when he said that even a dog knows the difference between ‘being stumbled over and being kicked.’ Anglo-American criminal law traditionally has marked a person as a criminal only if he or she committed a morally blameworthy act, known as the *actus reus*, along with an ‘evil’ frame of mind, known as *mens rea* or *scienter*. A *mens rea* requirement distinguished individuals who break the law only accidentally or inadvertently from ones who do so wantonly, with only the latter being held criminally responsible for their actions. Requiring the government to prove that a defendant acted

Third, unlike the UTSA or its ITSA cousin at issue in *Molon Motor*, the DTSA contains language that appears to be an express limitation on inevitable disclosure — a limitation that would seem to prohibit injunctions solely based on what’s in an employee’s head. Section 1836(b)(3)(A)(i) of the DTSA provides:

(3) **Remedies.**—In a civil action brought under this subsection with respect to the misappropriation of a trade secret, a court may—

(A) grant an injunction—

(i) to prevent any actual or threatened misappropriation described in paragraph (1) on such terms as the court deems reasonable, provided the order does not—

(I) prevent a person from entering into an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation and not merely on the information the person knows; or

(II) otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business[.]²²⁹

This language went unremarked upon in *Molon Motor*, perhaps because Molon invoked inevitable disclosure under the ITSA rather than the DTSA. Section 1836(b)(3)(A)(i) modifies injunctive relief as a remedy, yet it apparently does not have a role with respect to other forms of relief under the DTSA, such as damages, disgorgement or reasonable royalties, all of which are set forth later in the statute.²³⁰ I recognize that inevitable disclosure can be put to a variety of uses,²³¹ but by far its most common application is in injunction cases — the one place where Section 1836(b)(3)(A)(i) expressly bars it. The first subclause, Section 1836(b)(3)(A)(i)(I), could hardly be clearer: injunctions are prohibited based

with criminal intent was a hallowed feature of Anglo–American criminal law.”) (footnotes omitted).

²²⁹ 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2018).

²³⁰ See 18 U.S.C. § 1836(b)(3)(B), § 1836(b)(3)(C).

²³¹ See William Lynch Schaller, *Trade Secret Inevitable Disclosure: Substantive, Procedural & Practical Implications of an Evolving Doctrine (Part I)*, 86 J. PAT. & TRADEMARK OFF. SOC’Y 336 (May 2004) (analyzing inevitable disclosure cases in a wide range of settings besides injunctions, including jury instructions, summary judgement inferences, protective orders, and lawyer and expert witness disqualification).

“merely on the information the person knows,” the heart and soul of inevitable disclosure injunctions.²³² The immediately following subclause, Section 1836(b)(3)(A)(i)(II), reinforces this prohibition on inevitable disclosure injunctions by incorporating state-level rules against “restraints on the practice of a lawful profession, trade, or business.” The most prominent of these would seem to be California’s rejection of inevitable disclosure in view of California’s general bar on noncompetition agreements, as Ken Vanko, Dave Bohrer and others have pointed out.²³³ It seems a safe bet the Supreme Court will enforce Section 1836(b)(3)(A)(i)’s anti-inevitable disclosure language according to its plain terms,²³⁴ but that might end up meaning only “pure” inevitable disclosure injunctions are barred under the DTSA, while expansive, inevitable disclosure-like “threatened misappropriation” injunctions carry the day, as has been argued elsewhere.²³⁵

Fourth, dressing up conclusory “inevitable” disclosure allegations with “information and belief” labels also should make no difference in DTSA cases. Molon pursued this strategy,²³⁶ as have others.²³⁷ This approach runs directly counter to *Twombly*, where the Supreme Court directed its entire Rule 12(b)(6) analysis at the complaint’s defective “information and belief” allegations attempting to show an antitrust conspiracy on nothing more than parallel conduct facts.²³⁸

²³² 18 U.S.C. § 1836(b)(3)(A)(i)(I) (2018).

²³³ See Kenneth J. Vanko, *Revisiting the Seventh Circuit’s Decision in PepsiCo: Inevitable Disclosure Injunctions in the Wake of the Federal Defend Trade Secrets Act of 2016*, CIRCUIT RIDER, Apr. 2017, at 46, 50 (highlighting DTSA’s restriction on inevitable disclosure); David Bohrer, *Threatened Misappropriation of Trade Secrets: Making a Federal (DTSA) Case Out of It*, 33 SANTA CLARA COMPUTER & HIGH TECH. L.J. 506, 524-30 (2017) (reviewing inevitable disclosure decisions in California, collecting DTSA commentary, analyzing the DTSA’s language, and predicting the DTSA will be construed to bar inevitable disclosure consistent with the California approach).

²³⁴ *Cf.* Fourth Estate Pub. Benefit Corp. v. Wall-Street.com, LLC, 139 S. Ct. 881 (2019) (enforcing Copyright Act registration requirement as a precondition to lawsuits).

²³⁵ See M. Claire Flowers, *Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016*, 75 WASH. & LEE L. REV. 2207, 2225-41 (2018) (reviewing language and legislative history of the DTSA and arguing that “threatened misappropriation” has often been read expansively to include inevitable disclosure or circumstances very near it).

²³⁶ Third Amended Complaint at 15, 17, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017).

²³⁷ See, e.g., *Jazz Pharms., Inc. v. Synchrony Grp., LLC*, 343 F. Supp. 3d 434, 445, 445–46 nn. 50 & 52 (E.D. Pa. 2018) (approving “information and belief” allegations in support of “threatened” misappropriation claim and endorsing “inevitable disclosure” in DTSA case).

²³⁸ See *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 551 (2007). The Supreme Court explicitly quoted the following allegations in the complaint:

In the absence of any meaningful competition between the [ILECs] in one another’s markets, and in light of the parallel course of conduct that each engaged in to prevent competition from CLECs within their respective local telephone and/or high speed internet services markets and the other facts and market circumstances alleged above, Plaintiffs allege *upon information and belief* that [the ILECs] have entered into a contract, combination or

That some facts may be within the defendant's control does not excuse plaintiff's duty to allege facts sufficient to trigger a complaint. Plaintiff must offer enough facts to move beyond speculation and satisfy *Twombly*, and information in the defendant's head — without more — is not enough in light of Section 1836(b)(3)(A)(i)'s prohibitions.

Fifth, but less clear, is the impact these exclusions might have on state-law inevitable disclosure claims brought in federal court. The prefatory language of Section 1836(b)(3)(A) ties its inevitable disclosure restrictions to “a civil action brought under this subsection with respect to the misappropriation of a trade secret.”²³⁹ The reference to “this subsection” means Section 1836(b), as Section 1836(b) — the subsection that codifies the DTSA's private right of action — opens with “[a]n owner of a trade secret that is misappropriated may bring a civil action under this subsection[.]” The Supreme Court has said a claim “arises under” federal law only when “the well-pleaded complaint establishes either that federal law creates the cause of action or that the plaintiff's right to relief necessarily depends on resolution of a substantial question of federal law.”²⁴⁰ If federal question jurisdiction under the DTSA is the sole basis for federal subject matter jurisdiction, and if injunctive relief under the DTSA pursuant to “pure” inevitable disclosure is the sole theory, the claim both arises under and is “brought under this subsection” and thus triggers the inevitable disclosure bars found in Section 1836(b)(3)(A)(i)(I) and (II). The court in this narrow situation should therefore dismiss the case for lack of subject matter under Rule 12(b)(1), as I noted earlier in this paper.²⁴¹

The same result would not obtain, however, if a state law inevitable disclosure claim was brought and the federal court's subject matter jurisdiction instead rested exclusively on either diversity jurisdiction or some other statute, like the Patent Act or the Copyright Act;²⁴² in those circumstances the inevitable

conspiracy to prevent competitive entry in their respective local telephone and/or high speed internet services markets and have agreed not to compete with one another and otherwise allocated customers and markets to one another.

Id. (emphasis added) (alterations in original).

²³⁹ 18 U.S.C. § 1836(b)(3) (2018).

²⁴⁰ *Christianson v. Colt Indus. Operating Corp.*, 486 U.S. 800, 808 (1988) (quoting *Franchise Tax Bd. of Cal. v. Constr. Laborers Vacation Tr.*, 463 U.S. 1, 27-28 (1983)). *See also* *Am. Well Works v. Layne*, 241 U.S. 257, 259–60 (1916) (Holmes, J.) (“A suit for damages to business caused by a threat to sue under the patent law is not itself a suit under the patent law. . . A suit arises under the law that creates the cause of action.”); *Intellisoft, Ltd. v. Acer America Corp.*, No. 19-1522, ___ F.3d ___ (Fed. Cir. April 3, 2020) (holding that a state court claim under state trade secret law does not “arise under” the federal patent law, for removal purposes, just because the defendant files a patent inventorship counterclaim relating to the alleged trade secret theft).

²⁴¹ *See* Part I, *supra*.

²⁴² *See, e.g., Computer Assoc. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 719 (2d Cir. 1992) (state law trade secret misappropriation claim supplemental to copyright infringement claim).

disclosure claim could not be thought to “arise under” or to be “brought under” the absent DTSA. The DTSA would not form any part of or be necessary to the state law claim, and it’s hard to see how plaintiff’s right to relief would turn on resolution of a substantial question relating to the DTSA, especially since the DTSA expressly states in Section 1838 that it does not preempt state law. The same would be true even if plaintiff included a DTSA claim in the mix. In this circumstance, the DTSA would not be necessary to the state law trade secret claim because separate federal question jurisdiction would exist under the Patent Act or the Copyright Act. This assumes, of course, that the state trade secret law claim shares sufficient factual overlap with the patent or copyright claims, whether under the old “common nucleus of operative fact” test originated in *United Mine Workers v. Gibbs*²⁴³ or under the new “case or controversy” test found in Section 1367.²⁴⁴

Indeed, about the only way Section 1836(b)(3)(A)(i)(I) or (II) might come into play on a state-law inevitable disclosure claim would be if the state-law claim was included as a supplemental claim to bolster a weak DTSA claim and no diversity or other federal question existed. This was actually the case in *Molon Motor*. Molon alleged patent infringement claims in Counts I and II, but it did not tie its ITSA claim to its patent claims, nor did it allege diversity of citizenship as an alternative subject matter ground for its ITSA claim. Rather, Molon expressly alleged that its DTSA claim in Count III served as the basis for supplemental jurisdiction over its ITSA claim in Count IV.²⁴⁵ Given this claim presentation, the court should have been forced to conclude it could not reach the ITSA claim under *PepsiCo* for lack of a viable claim against Nidec under the DTSA, if

²⁴³ *United Mine Workers v. Gibbs*, 383 U.S. 715, 725 (1966) (“The state and federal claims must derive from a common nucleus of operative fact.”).

²⁴⁴ *See, e.g., Arbaugh v. Y&H Corp.*, 546 U.S. 500, 506 (2006) (stating that “under 28 U.S.C. § 1367, federal courts may exercise ‘supplemental’ jurisdiction over state-law claims linked to a claim based on federal law,” without specifying what test that “link” needs to meet); *Achtman v. Kirby, McInerney & Squire*, 464 F.3d 328, 335 (2d Cir. 2006) (“When both pendent and ancillary jurisdiction were codified in 1990 as §1367, however, the [*Gibbs*] ‘common nucleus’ test was retained by nearly all the Circuits to interpret the statute’s ‘case or controversy’ language.”) (citing 16 MOORE & PRATT, MOORE’S FEDERAL PRACTICE §106.21[1] (3d ed. 1998)); *Jones v. Ford Motor Credit Co.*, 358 F.3d 205, 213 n.5 (2d Cir. 2004) (expressing uncertainty as to whether Section 1367’s “case or controversy” language is co-extensive with “common nucleus” test of *Gibbs*); *Channell v. Citicorp Nat’l Servs.*, 89 F.3d 379, 385 (7th Cir. 1996) (a “loose factual connection between the claims” satisfies Section 1367); F. Andrew Hessick III, *The Common Law of Federal Question Jurisdiction*, 60 ALA. L. REV. 895, 926 (2009) (noting the Court in *Arbaugh* adopted “a presumption against reading federal statutes as restricting federal court jurisdiction”).

²⁴⁵ *See* Third Amended Complaint at 2–3, *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, No. 16 C 03545, 2017 WL 1954531 (N.D. Ill. May 11, 2017) (“This Court has supplemental or pendent jurisdiction over the remaining claims [in Count IV] pursuant to 28 U.S.C. § 1367 because such claims are so closely related to Molon’s claim for misappropriation of trade secrets under the Defend Trade Secrets Act of 2016 that they form part of the same case or controversy.”).

Molon was seeking injunctive relief as its sole remedy, as Section 1836(b)(3)(A)(i)(I) foreclosed a DTSA inevitable disclosure claim and Molon offered no other allegations to show Nidec's use or disclosure. Whether the state law inevitable disclosure claim was or was not in some sense "brought under" the DTSA was irrelevant; without the DTSA claim there was no federal question jurisdiction to support Section 1367 supplemental jurisdiction. Of course, if plaintiff has enough facts to allege a sufficient DTSA misappropriation claim, whether for injunctive or monetary relief purposes, plaintiff has no need to resort to a state law inevitable disclosure claim.

IV. PLEADING UNDER THE DTSA: A UNIFIED THEORY AND ITS CONSEQUENCES

A. PROPER PLEADING

On the whole, the DTSA resembles its model, the UTSA. The DTSA generally provides the same claims and the same relief as the UTSA, using nearly the same definitions of "trade secret" and "misappropriation" for claims, but goes slightly further on relief by omitting the "head start" injunction limitation found in the UTSA and by authorizing *ex parte* searches and seizures.²⁴⁶ In keeping with the UTSA, the DTSA also generally tracks the UTSA's defenses available to employees and other "persons" accused of trade secret theft,²⁴⁷ by allowing them to defend on the grounds of reverse engineering and independent development. The DTSA goes a bit further than the UTSA, though, by explicitly allowing "any other lawful means of acquisition" as a defense as well.²⁴⁸ This last limitation might prove pivotal in "commercial morality" cases involving questionable but not necessarily illegal conduct, such as sky surveillance, dumpster diving, and other sharp investigative practices.²⁴⁹ It might also provide a statutory window

²⁴⁶ I say "slightly further" because unlimited injunctions remain possible under the UTSA, as in *Wyeth v. Nat. Biologics, Inc.*, 395 F.3d 897, 902-03 (8th Cir. 2005) (applying Minnesota law), and because *ex parte* orders to preserve evidence, though rare, have always been permitted in principle under Rule 65 and its state law equivalents, as in *In re Vuitton et Fils S.A.*, 606 F.2d 1 (2d Cir. 1979); *Am. Can Co. v. Mansukhani*, 742 F.2d 314, 322 (7th Cir. 1984), and *Mitchell v. Mitchell*, 135 N.E.2d 109, 112 (Ill. App. Ct. 1956).

²⁴⁷ "Person" — left undefined in the DTSA itself—defaults to the broad definition in 1 U.S.C. § 1: "In determining the meaning of any Act of Congress, unless the context indicates otherwise . . . the words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals[.]" 1 U.S.C. § 1 (2018).

²⁴⁸ 8 U.S.C. § 1839(6)(B) (2018).

²⁴⁹ See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974) (trade secret law fosters commercial ethics); *E.I. du Pont de Nemours & Co. v. Christopher*, 431 F.2d 1012, 1016-17 (5th Cir. 1970) (flight surveillance of plant under construction violated commercial morality); *Frank W. Winne and Son, Inc. v. Palmer*, No. 91-2239, 1991 WL 155819, at *4 (E.D. Pa. Aug. 7, 1991) (permitting dumpster diving); *Brunswick Corp. v. Outboard Marine Corp.*, 404 N.E.2d 205, 207 (1980) (reciting commercial morality as a trade secret concern); Kurt M.

for arguing “general skill and knowledge” as a defense if the reference to “another person” in the definition of “trade secret” does not.²⁵⁰

These general similarities mask important differences between the DTSA and the UTSA, however. For example, subject matter jurisdiction under the DTSA is cabined by the federal statute’s “commerce” and “relatedness” conditions, unlike the state law-based UTSA.²⁵¹ In addition, the DTSA’s placement within the EEA, a criminal statute, likely implicates “the rule of lenity” and hence demands narrow construction of shared terms like “trade secret” and “misappropriation” as well as the identical “commerce” and “relatedness” jurisdiction conditions found in both laws. This statutory interpretation constraint finds no equivalent in the purely civil UTSA. The rule of lenity’s power should not be underestimated in close cases: its bearing on jurisdiction was outcome-determinative in the famous federal criminal prosecution that failed in *Aleynikov*.²⁵² Even though the DTSA’s jurisdiction language is slightly different from the language at issue in *Aleynikov*, Rule 12(b)(1) jurisdiction challenges still lurk on lenity, “commerce,” and “relatedness” grounds in all DTSA cases involving purely local products and services.

These jurisdictional concerns underscore a larger DTSA statutory construction issue: To what extent will the Supreme Court follow the UTSA rather than the Restatement of Torts or even the common law? Will *Masland* arise and bring with it “breach of confidence,” or will *Ruckelshaus* prevail with its “property” view? The DTSA is a blend of both. I suspect the “property” approach will carry greater weight, if not control, however, largely because it is more protective of defendants and thus more consistent with the rule of lenity. For the same reason, the restrictive “property” theory also seems a better fit with the “not generally known” prong of the DTSA’s “trade secret” definition, as this prerequisite operates to forgive thieving defendants if (unbeknownst to them) the “secret” they sought to steal turns out to be well known to others in the industry. On this view there’s no theft if there’s no property.

Twombly and *Iqbal* represent another set of pro-defense hurdles, particularly if the “property” concept takes center stage. The tendency to date, as reflected in the almost complete absence of federal appellate precedent on trade secret pleading, has been for courts and counsel to treat trade secret cases as fact-intense

Saunders, *The Law and Ethics of Trade Secrets: A Case Study*, 42 CAL. WEST. L. REV. 209 (2006) (discussing trade secret law and then analyzing various ethics approaches, including formalism, rights, utilitarianism, and justice theories); William M. Fitzpatrick, *Uncovering Trade Secrets: The Legal and Ethical Conundrum of Creative Competitive Intelligence*, 68 SAM ADVANCED MGMT J. No. 3, at 4 (Summer 2003) (general discussion of trade secrets and competitive intelligence practices).

²⁵⁰ 18 U.S.C. § 1839(3)(B) (2018).

²⁵¹ See *id.* at § 1832(a).

²⁵² See MICHAEL LEWIS, FLASH BOYS: A WALL STREET REVOLT (W.W. Norton & Co. 2014) (best-selling book opening the introduction with Sergey Aleynikov’s arrest and then devoting all of Chapter Five to his plight).

affairs better left to discovery. This approach is wrong on my reading of *Twombly* and *Iqbal*. At a minimum, *Twombly* and *Iqbal* teach that a “trade secret” and “misappropriation” must both be properly alleged at the outset so that discovery, if necessary, is properly tailored to the needs of the case. This is notice pleading and issue narrowing at their most basic. For Rule 12(b)(6) purposes, how can the court decide whether a secret exists and whether it has been stolen if the court doesn’t know the metes and bounds of the secret? How can the court determine if all or part of the secret is in the public domain if it doesn’t know what the secret is? If reasonable secrecy measures are a function of the secret they are designed to protect, how can the court assess the reasonableness of those measures without knowing what they are intended to guard? How can an employee or other “person” with authorized access “know or have reason to know” he is engaging in misappropriation when he doesn’t know what he is forbidden from taking or using? How can that person’s new employers or new partners “know or have reason to know” something is amiss if the person who had authorized access doesn’t even know himself?

If all roads lead to Rome, in trade secret litigation they all lead to “identification.” To satisfy notice pleading under *Twombly* and *Iqbal*, plaintiffs should attach (under seal) the secrets in issue in the same manner and in the same detail as they were disclosed to the defendant who allegedly misappropriated them. To meet reasonable secrecy requirements, the designated secrets should be password-protected and otherwise restricted to those with a “need to know,” and they should bear a “confidential,” “secret,” or “proprietary” legend warning the recipient that the information is not to be disclosed or used other than for authorized purposes, thereby putting the recipient on explicit notice as to what is specifically off limits. To the extent secrets are kept only in “intangible” form — as expressly allowed by the DTSA’s definition, in a departure from the UTSA’s silence on the subject — evidence of the description actually given to users should be made exhibits. “Click” screen acknowledgments and signed confidentiality agreements should be attached to show the recipient understood the information was to be kept secret. The trade secret owner should also allege how the secrets were developed or perfected in-house or under confidentiality agreements with outsiders and why, as a result, the secrets have “economic value” by giving the owner and others a market advantage — an advantage that cannot be readily gleaned from public or industry sources. If this is a correct understanding of *Twombly* and *Iqbal*, the *Plastronics* complaint would not have passed muster.

Assuming a complaint satisfies the “trade secret” definition, it should also allege “misappropriation” by reciting facts reflecting unauthorized activities knowingly undertaken. To get beyond equipoise, to establish “plausibility” under *Twombly* and *Iqbal*, those facts must show more than mere interviewing, preparing to compete, divorcing a partner, dropping a deal, joining a competitor, or entering a market. They must show downloading, copying, or taking (or in rare cases, memorizing) by someone who “knows or has reason to know” he is not authorized to do it. An authorized user’s failure to return documents, without

more, is not enough; a proper “trigger” allegation should offer facts showing the owner’s demand followed by the defendant’s knowing refusal, whether at an exit interview or in response to a demand letter. The same is true for downstream recipients, meaning persons who did not steal the secrets but have received them from someone who did: facts showing their knowledge are needed to meet the “knows or had reason to know” language found in the DTSA’s “misappropriation” definition. Common law conversion cases supply a useful model for these trade secret scenarios, if one is needed.²⁵³ Of course, “knowledge” on the part of any of these potential defendants returns us to the “identification” requirement – they can’t know they are stealing or receiving a stolen secret if they don’t know it is a secret in the first place.

The “knowledge” requirement alone should also bar “pure” inevitable disclosure claims under the DTSA; they turn on unwitting, unavoidable conduct. If federal Courts of Appeals hold that the “knowledge” condition precludes such claims under the DTSA, one has to wonder whether those same appellate courts will say the same about state law inevitable disclosure claims given the identical “knowledge” language in all UTSA-based trade secrets laws. We see most clearly how this might play out in *Molon Motor*, where lack of knowledge on defendant Nidec’s part was a glaring problem. If Molon’s ex-employee Desai didn’t know he was engaged in wrongdoing, how could his new employer? And even if Desai did know he was engaged in wrongdoing, it didn’t follow that Nidec knew. The proper course was for Molon to sue Desai first, to learn what he said and did at Nidec, and then to add Nidec if newly-discovered evidence justified it. Instead, Molon Motor sued Nidec first without a proper basis and then tried to transmute Desai’s lack of knowledge into Nidec’s fount of knowledge in an effort to bridge the Third Amended Complaint’s “knowledge” gap.

DTSA inevitable disclosure injunction claims face a second bar: Section 1836(b)(3)(A)(i)’s express ban on injunctions that preclude employment “merely on the information the person knows” or that “otherwise conflict with an applicable State law prohibiting restraints on the practice of a lawful profession, trade, or business.” These limitations should also work to stop state law inevitable disclosure claims like the one in *Molon Motor*. If federal supplemental jurisdiction over state-law claims is linked solely to a DTSA claim, and if an injunction is the sole relief sought (as is typical of such state-law claims), the DTSA claim should founder under Section 1836(b)(3)(A)(i) and the state law trade secret claim should sink with it for lack of subject matter jurisdiction. This should have been the result in *Molon Motor*, as the ITSA inevitable disclosure claim there was tied exclusively to the DTSA claim and only injunctive relief was sought. However, state-law inevitable disclosure injunction claims should escape Section

²⁵³ See, e.g., *Van Diest Supply Co. v. Shelby County State Bank*, 425 F.3d 437, 439 (7th Cir. 2005) (applying Illinois law) (to establish a conversion claim, a plaintiff must show: “(1) a right to the property; (2) an absolute and unconditional right to the immediate possession of the property; (3) a demand for possession; and (4) that the defendant wrongfully and without authorization assumed control, dominion, or ownership over the property.”).

1836(b)(3)(A)(i)'s prohibitions when such claims rest on diversity jurisdiction or are supplemental to federal claims other than ones "brought under" the DTSA.

B. CONSEQUENCES OF IMPROPER PLEADING

What, then, should be the consequences of this unified theory of pleading under the DTSA? Early dismissal should certainly be one, and denial of leave to amend should be another, if amendment would be futile. Amendment *would* be futile in most of the scenarios described above; information in the public domain, lack of identification, or the absence of secrecy measures should be fatal to "trade secret" allegations, and the absence of true "trigger" facts should be fatal to "misappropriation" allegations. The one circumstance in which amendment should be routine is when plaintiff seeks to add claims or defendants based on new evidence learned during discovery directed at the original defendant. Plaintiff should not be penalized for exercising procedural caution by first stating a claim against the original defendant, and plaintiff may need discovery to determine if other defendants "knew or had reason" to know as a result of dealing with the original. However, the engines of discovery should not be started without plaintiff first stating a viable claim.

If we take to heart the Seventh Circuit's observation in *PepsiCo* that "falling a little short is still falling short," Rule 11 sanctions should be imposed as a matter of course when trade secret complaints suffer from incurable defects. Because Rule 11 warrants sanctions whenever plaintiff has failed to conduct an objectively reasonable factual and legal investigation,²⁵⁴ Rule 11 is easier to meet than the DTSA's "bad faith" standard for fee award purposes.²⁵⁵ If a readily ascertainable patent or publication discloses plaintiff's "secret," for example, plaintiff cannot be thought to have done a reasonable pre-filing investigation. Similarly, if plaintiff's complaint (in a sealed appendix) cannot identify with particularity the secrets in issue, plaintiff has no business suing. And the complaint's identification should match the description given employees or other users at the time the owner granted them access; lack of sufficient access identification back then should be deemed an unreasonable secrecy measure as a matter of law for Rule 12(b)(6) purposes. Most important, if all plaintiffs can allege "is that defendants could misuse plaintiffs' secrets, and plaintiffs fear they will," as the *PepsiCo* court put it, then plaintiffs have not done an adequate investigation and should not be suing.

An adequate pre-filing investigation should look like the one undertaken in

²⁵⁴ See *Bus. Guides, Inc. v. Chromatic Commc'ns Enters.*, 498 U.S. 533, 540-51 (1991) (Rule 11's objective standard—calling for a reasonable investigation of the facts and law—applies to lawyers and their clients).

²⁵⁵ See 18 U.S.C. § 1836(b)(3)(D) (2018) ("[I]f a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated, award reasonable attorney's fees to the prevailing party.").

Experian Information Solutions, Inc. v. Nationwide Marketing Services Inc.,²⁵⁶ where information a data broker provided to plaintiff Experian caused Experian to suspect the broker's source, defendant Nationwide, had wrongfully obtained it from Experian in some manner. Instead of immediately suing, Experian first tested the data from the broker and determined it matched Experian's data 97% of the time. Experian thereafter confronted Nationwide with this evidence and then followed up with a lawsuit that revealed other suspicious circumstances, including Nationwide's lack of a written agreement with its source and Nationwide's payment of an unusually low fee to that source — suspicious circumstances that bolstered the inference that Nationwide “knew or had reason to know” its source had acquired the information improperly.

One particular complexity is the sanction, if any, for “overclaiming” trade secrets. In *Rockwell Graphic Systems*, Judge Posner dismissed the notion that “overclaiming” some trade secrets should result in forfeiture of others.²⁵⁷ As mentioned earlier, I am not so sure about this. First, as cases like *GlobalTap* demonstrate, courts sometimes deny trade secret status to purported secrets buried in larger documents containing non-trade secret material. As a matter of fact, the Seventh Circuit, Judge Posner's own court, has frequently criticized lengthy descriptions that fail to identify secrets or that bury them in long documents that do not distinguish aspects known to the trade from those that are secret.²⁵⁸ Second, claiming secrecy rights in things that are not secret borders on improper pleading and, in fact, crosses the line when reasonable minds would conclude the information does not constitute a trade secret. The Supreme Court in *Business Guides, Inc. v. Chromatic Communications Enterprises*,²⁵⁹ for example, had no difficulty allowing Rule 11 sanctions against a client who wrongly identified “seeds” planted in documents to detect competitor copying, when it turned out no seeds had actually been planted.²⁶⁰ In other words, for pleadings purposes, the Court held, a company must be responsible for knowing the contents of its own documents. Third, and most important, Judge Posner's view privileges property over people. Not only are trade secret owners in a better position than employees and other authorized users to know what is and is not a secret;²⁶¹ owners may face

²⁵⁶ *Experian Info. Sols., Inc. v. Nationwide Mktg. Servs. Inc.*, 893 F.3d 1176 (9th Cir. 2018) (applying Arizona law).

²⁵⁷ *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 176-77 (7th Cir. 1991) (Posner, J.) (rejecting DEV's argument “that if a firm claims trade secret protection for information that is not really secret, the firm forfeits trade secret protection of information that is secret”).

²⁵⁸ See William Lynch Schaller, *Secrets of the Trade: Tactical and Legal Considerations from the Trade Secret Plaintiff's Perspective*, 29 REV. LITIG. 729, 801-02 (2010) (discussing Seventh Circuit trade secret identification opinions).

²⁵⁹ *Bus. Guides, Inc. v. Chromatic Commc'ns Enters.*, 498 U.S. 533 (1991).

²⁶⁰ *Id.* at 540-41.

²⁶¹ *Cf. Glenayre Elecs., Ltd. v. Sandahl*, 830 F. Supp. 1149, 1152 (C.D. Ill. 1993) (“Defendants state that the first mention of the technology at issue appears in documents prepared months after Tanner's departure. Also, when Tanner left, Glenayre's vice-president sent him

potential liability for tortious interference, defamation, and other business torts for overclaiming in statements to third-parties.²⁶² Indeed, it seems only a question of time until an enterprising ex-employee sues a former employer for overclaiming in statements made only to the employee himself, perhaps framing such a claim as an independent tort for wrongful dismissal or for some other adverse employment action,²⁶³ or perhaps pursuing it as free-standing tort of unfair competition.²⁶⁴ In short, overclaiming, whether before or during litigation, should be revisited as a matter of first principle, with sanctions the consequence.

Finally, orders staying discovery should be granted almost as a matter of course if a trade secret complaint is defective on its face, either for lack of subject matter jurisdiction or for failure to state a claim.²⁶⁵ Fishing expeditions should

be thwarted, not encouraged. Here, Rule 9(b) comes to mind. Fraud allegations are supposed to be alleged with “particularity” under Rule 9(b), and courts routinely stay discovery when a Rule 12(b)(6) motion challenges a fraud complaint for lack of particularity in accordance with Rule 9(b). Indeed, though it’s uncommon, one can make a fairly strong argument that Rule 9(b) should govern trade secret actions: most trade secret actions involve species of actual or fiduciary fraud,²⁶⁶ at least with respect to the primary wrongdoers who acquired the

a letter stating that Glenayre believed that he had trade secrets which should be kept confidential. Tanner replied that he would respect the confidentiality of any valid trade secrets he possessed and requested that Glenayre identify such information which he possessed. Glenayre did not respond to this request.”)

²⁶² See William Lynch Schaller, *Jumping Ship: Legal Issues Relating to Employee Mobility in High Technology Industries*, 17 LAB. LAW. 25, 93-94 n.286 (2001) (collecting cases).

²⁶³ See *D’Sa v. Playhut, Inc.* 85 Cal. App. 4th 927 (2000) (employer may be liable in tort for wrongful termination if it fires employee for refusing to sign an employment agreement containing an unenforceable noncompetition agreement); *Palmateer v. Int’l Harvester Co.*, 421 N.E.2d 876, 879 (Ill. 1981) (approving employee’s independent tort action for wrongful dismissal in violation of Illinois public policy favoring cooperation with criminal law enforcement authorities); *Kelsay v. Motorola, Inc.*, 384 N.E.2d 353, 357 (1978) (approving employee’s independent tort action for wrongful dismissal in violation of Illinois public policy favoring workers’ compensation claims).

²⁶⁴ Cf. Elizabeth Smith, *Eliminating Predatory Litigation in the Context of Baseless Trade Secret Claims: The Need for a More Aggressive Counterattack*, 23 SANTA CLARA L. REV. 1095, 1125-28 (1983) (arguing for recognition of a new predatory litigation claim for trade secret litigation abuse).

²⁶⁵ See Kevin J. Lynch, *When Staying Discovery Stays Justice: Analyzing Motions to Stay Discovery When a Motion to Dismiss Is Pending*, 47 WAKE FOREST L. REV. 71 (2012) (discussing the tension between permitting and staying discovery when a potentially dispositive Rule 12(b)(6) motion to dismiss is pending).

²⁶⁶ See 18 U.S.C. § 1839(6)–(6)(A) (“[T]he term ‘improper means’— (A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means.”); UNIF. TRADE SECRET ACT WITH 1985 AMENDMENTS § 1.1 (UNIF. LAW COMM’N 1985) (“‘Improper means’ includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or

secrets through improper means.²⁶⁷

V. CONCLUSION

Trade secrets are important assets. Indeed, for many if not most firms, they are the most important assets, often the proverbial “crown jewels.” Companies should protect them and courts should too. Congress plainly recognized these concerns in passing the DTSA, which allows trade secret owners and their licensees to bring federal claims in federal court.

Given these powerful concerns, why should the Courts of Appeals, and ultimately the Supreme Court, insist upon strict pleading compliance along the lines I’ve outlined here? The reasons the Supreme Court offered in *Twombly* and *Iqbal* are reasons enough: ferreting out baseless claims and ending unwarranted litigation long before discovery clogs conscientious courts and overwhelms innocent defendants. But if more reasons are needed, consider these supplied by Professor Orly Lobel:

Entrepreneurship is especially harmed when workers fear leaving their employers. If employees are unable to use their knowledge, or human capital learned through their employment with established firms, they are not only less likely to leave, they are particularly less likely to go to less established, more vulnerable entities. Consequently, employees are less likely to consider starting their own businesses, build their own products, or create new services. Competitors might also be reluctant to hire away employees for fear of being criminally or civilly prosecuted. Smaller, newer companies can be restricted from growing or entering a market by larger, long-established firms with more resources. Such

espionage through electronic or other means.”); *Mueller Indus., Inc. v. Berkman*, 927 N.E.2d 794, 809 (Ill. App. Ct. 2010) (holding that intentional breach of fiduciary duty is analogous to the tort of fraud for purposes of the crime-fraud exception to the attorney-client privilege), *abrogated on other grounds*, *People v. Radojcic*, 998 N.E.2d 1212 (Ill. 2013); Morwenna Borden, Note, *Particulars of Particularity: Alleging Scierter and the Proper Application of Rule 9(b) to Duty-Based Misrepresentations*, 98 MINN. L. REV. 1110, 1113-14, 1115-27 (2014) (describing minimal history behind Rule 9(b) and conflicting interpretations of its application outside of traditional fraud context).

²⁶⁷ See *Foam Supplies, Inc. v. The Dow Chem. Co.*, No. 4:05CV1772 CDP, 2006 WL 2225392, at *14 (E.D. Mo. Aug. 2, 2006) (“[W]here a plaintiff alleges fraud as the improper means by which a party misappropriated trade secrets, Rule 9(b)’s particularity requirement applies.”); Hannah Ruth Roberts, *Anything But General: Pleading Scierter in Rule 9(b) Claims*, AM. BAR ASS’N (May 23, 2017), <https://www.americanbar.org/groups/litigation/committees/business-torts-unfair-competition/practice/2017/pleading-scierter-in-rule-9b-claims/> (discussing varying approaches of Courts of Appeals on pleading scierter under Rule 9(b) in light of *Twombly* and *Iqbal*).

established firms can threaten IP litigation for the purpose of stifling entrepreneurs as well as new startups, and competitors.²⁶⁸

Professor Lobel's worries bring to mind the "Traitorous Eight" — Julius Blank, Victor Grinich, Jean Hoerni, Eugene Kleiner, Jay Last, Gordon Moore, Robert Noyce and Sheldon Roberts. They worked for Shockley Semiconductor Laboratory until 1957,²⁶⁹ when they quit and founded Fairchild Semiconductor. Although Nobel Prize-winner William Shockley considered their departure a betrayal (no small irony, since he himself had quit Bell Labs in 1956 to form Shockley Semiconductor), the Traitorous Eight and their proteges eventually spawned the "Fairchildren," firms like Intel and AMD that, along with Fairchild, came to form the backbone of modern Silicon Valley.²⁷⁰ Surely this runaway success was due in no small part to employee mobility and knowledge "spillover."²⁷¹ If courts fail to police the DTSA's boundaries, how many firms will risk massive litigation expenses just to hire away competitors' partners and employees? How many partners and employees will do the same? With the "Organization Man" long gone and job-hopping now a way of life, these questions have never been more important.²⁷²

²⁶⁸ Orly Lobel, *The DTSA and the New Secrecy Ecology*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 369, 377 (2017). See also David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?*, 94 NOTRE DAME L. REV. 751 (2018) (exploring the lack of empirical research on trade secret use by startups).

²⁶⁹ Together with John Bardeen and Walter Brattain, William Shockley invented the transistor at Bell Labs, for which the three received the Nobel Prize in Physics in 1956 ("for their researches on semiconductors and their discovery of the transistor effect"), ushering in microelectronics, integrated circuits, semiconductors and the Information Age. See generally JON GERTNER, *THE IDEA FACTORY: BELL LABS AND THE GREAT AGE OF AMERICAN INNOVATION* (Penguin Press 2012).

²⁷⁰ See generally MARGARET O'MARA, *THE CODE: SILICON VALLEY AND THE REMAKING OF AMERICA* 41, 52 (Penguin Press 2019) ("Modern Silicon Valley started with Fairchild and the 'Traitorous Eight' who founded it . . . A swelling number of young men spun out new semiconductor firms of their own. Many had worked at Fairchild, and their start-ups became known, naturally, as 'the Fairchildren.'").

²⁷¹ See Laura G. Pedraza-Fariña, *Spill Your (Trade) Secrets: Knowledge Networks as Innovation Drivers*, 92 NOTRE DAME L. REV. 1561 (2017) (arguing innovation in complex fields is often the product of networks of learning and collaboration across firms rather than within a single firm).

²⁷² See Nicolas Lemann, *When Corporations Changed Their Social Role — and Upended Our Politics*, WALL ST. J., Sept. 7, 2019, at C1 (describing the rise of financial engineering and globalization starting in the late 1970s: "There was no more payoff, evidently, to being an exemplar of that venerable type, the Organization Man. Now the payoff was for the Transaction Man or Woman, someone who took established economic institutions apart and reassembled them in a more strictly market-oriented form.").

