

# Searching for Standing: Are Improper Acquisition or Threatened Misappropriation of Trade Secrets Cognizable Injuries Sufficient for Article III Standing?

Josh J. Leopold<sup>†</sup>

*Trade secret litigation is on the rise. Meanwhile, modern standing cases have forced courts and commentators to reevaluate what sorts of legal injuries bring factual injuries with them, such that federal courts can adjudicate them as a “case” or “controversy” under Article III of the Constitution.*

*This Comment studies the intersection of Article III standing and federal trade secret law. It is the first piece to provide a taxonomy of trade secret violations and factual injuries in the shadow of standing doctrine’s demand for an injury-in-fact. This Comment submits a bold yet plausible claim: Article III standing should be in question for certain violations of the Defend Trade Secrets Act (DTSA)—improper acquisition and threatened misappropriation. Challenging standing in these cases will ensure that federal courts remain within their constitutional mandate. Moreover, challenging standing in certain trade secret cases will help encourage employee mobility in the marketplace.*

*While this Comment urges courts to assure themselves of Article III standing in these cases, it acknowledges that plaintiffs will have forceful responses to standing arguments made against them. A back-and-forth rally between plaintiffs and defendants will help courts reach the correct results, as the adversarial process intends. At bottom, this piece challenges what some seem to take as a given: that trade secret plaintiffs who plausibly allege a violation of the DTSA have necessarily suffered an injury-in-fact.*

INTRODUCTION .....	2263
I. MODERN STANDING DOCTRINE.....	2269
A. Injury-in-Fact.....	2270
1. Concrete.....	2271
2. Actual or imminent.....	2274
3. Particularized.....	2275
B. The Data Breach Cases .....	2276

---

<sup>†</sup> B.A. 2019, Washington University in St. Louis; J.D. Candidate 2024, The University of Chicago Law School. I thank Professor Lior Strahilevitz for his guidance and thoughtful feedback on an earlier draft. I am also grateful to Dylan Salzman, Kate Gehling, Jaston Burri, Amanda Williams, Jorge Pereira, and the *University of Chicago Law Review* editors for their advice and insight.

C. Standing and the DTSA .....	2277
II. THE DEFEND TRADE SECRETS ACT (DTSA).....	2279
A. An Overview of Trade Secret Law .....	2280
B. Improper Means of Acquisition Is a Form of Misappropriation	2283
1. Breach of a duty to maintain secrecy.....	2283
2. Espionage.....	2284
C. Threatened Misappropriation and Inevitable Disclosure .....	2285
1. “Threatened misappropriation” and its unclear boundaries.	2285
2. Inevitable disclosure as a form of threatened	
misappropriation under the DTSA.....	2286
III. IMPROPER ACQUISITION AND THREATENED MISAPPROPRIATION:	
COGNIZABLE HARMS? .....	2287
A. Improper Acquisition and Threatened Misappropriation: Per Se	
Injuries? .....	2288
B. Mitigation Costs as Injuries Sufficient for Standing.....	2291
C. Decreased Secrecy as Cognizable Harm.....	2292
D. Comparison to Data Breach Harms .....	2295
IV. TWO OBJECTIONS .....	2296
A. Reasonable Measures and Standing.....	2296
B. Congressional Judgment .....	2298
V. THREE (POTENTIAL) PATHS TO STANDING .....	2299
A. Are Trade Secrets a Property Right?.....	2300
1. An understanding of trade secrets as premised on a property	
conception has been adopted by some courts. ....	2301
2. An alternative understanding of trade secrets views them as	
dependent on relational duties rather than property rights.	2302
B. Are Improper Acquisition or Threatened Misappropriation	
Traditionally Recognized Injuries?.....	2305
C. Potential Common Law Analogs.....	2307
1. Threatened misappropriation and improper acquisition likely	
fail to map onto a breach of confidence.....	2308
2. Intrusion upon seclusion likely falls short in most cases.	2309
3. Breach of express or implied contract is likely the best	
analogy, but it might not be the sort of analog accepted by	
courts. ....	2310
D. Do Improper Acquisition or Threatened Misappropriation Result	
in Other Concrete Harms?.....	2311
CONCLUSION.....	2312

## INTRODUCTION

*I see thou wilt not trust the air  
With secrets.  
— Chiron<sup>1</sup>*

Federal trade secret litigation has experienced massive growth over the last several years, in terms of both case volume and damage awards.<sup>2</sup> Well over a thousand trade secret actions were filed in federal court in 2020 alone, representing a more than 30% increase from the mid-2010s.<sup>3</sup> This growth is the result of both the passage of a new federal statute, the Defend Trade Secrets Act of 2016<sup>4</sup> (DTSA), and the growing ubiquity of valuable digital technology, bioscience, and other intangible information harnessed by corporations.<sup>5</sup> Unsurprisingly, the federalization of trade secret law and accompanying sharp increase in trade secret litigation has led to a changing legal landscape.<sup>6</sup> As Professor Camilla Hrdy has observed, because “[t]rade secret law is at an important crossroads,” this is a “crucial time to get the law right.”<sup>7</sup>

This Comment examines the intersection of trade secret law and Article III standing. Its central thesis—that certain trade secret actions may fail to satisfy modern standing doctrine because they may not be per se injuries-in-fact—has implications for both plaintiff companies and defendant employees in federal trade secret actions. This Comment also reveals that the ongoing debate surrounding whether trade secrets should be understood as forms of property has important stakes; that is, standing may

---

<sup>1</sup> WILLIAM SHAKESPEARE, *TITUS ANDRONICUS* act 4, sc. 2, l. 168–69.

<sup>2</sup> See Rachel Bailey, *Trade Secret Litigation Report 2021* (Lex Machina, June 2021).

<sup>3</sup> *Id.*

<sup>4</sup> Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. §§ 1836–1839).

<sup>5</sup> See, e.g., James Pooley, *The Myth of the Trade Secret Troll*, 23 *GEO. MASON L. REV.* 1045, 1067 (2016) (explaining that companies are increasingly relying on trade secrets rather than patents to protect their information); Ariel Porat & Lior J. Strahilevitz, *Personalizing Default Rules and Disclosure With Big Data*, 112 *MICH. L. REV.* 1417, 1435 (2014) (observing that “many uses of Big Data are being kept as proprietary trade secrets”).

<sup>6</sup> See Laura G. Pedraza-Fariña, *Spill Your (Trade) Secrets: Knowledge Networks as Innovation Drivers*, 92 *NOTRE DAME L. REV.* 1561, 1605 (2017) (averring that the DTSA “will have a direct impact on the ability of states to experiment effectively with different levels of local trade secret protection”).

<sup>7</sup> Camilla A. Hrdy, *The Value in Secrecy*, 91 *FORDHAM L. REV.* 557, 564 (2022).

turn on whether trade secrets are, in fact, property.<sup>8</sup> This Comment is ambitious because few, if any, courts or commentators have deeply analyzed whether certain trade secret violations should be considered per se injuries sufficient for Article III standing.<sup>9</sup> To be sure, some courts and scholars have suggested that modern standing doctrine could present considerable complications for the adjudication of trade secret cases.<sup>10</sup>

Imagine that an employee of Company X, a social media firm, is cleaning out her workstation after getting fired. On a whim, she grabs a thumb drive out of her backpack, plugs it into her work computer, and downloads some of the computer files onto the thumb drive. She takes the thumb drive out of the computer, puts it in her backpack, and exits the company building. Upon arrival home, she places the drive in her desk drawer and subsequently forgets about it.

During a routine security audit two weeks later, Company X's IT department discovers that the ex-employee downloaded sensitive data onto the thumb drive: a trade secret (an Excel

---

<sup>8</sup> See *infra* Part V.A.

<sup>9</sup> A few federal courts have briefly addressed whether certain trade secret violations amount to cognizable harms, although they did not do so using the familiar “injury-in-fact” standing language. See, e.g., *Vesta Corp. v. Amdocs Mgmt., Ltd.*, 2018 WL 4354301, at \*21 (D. Or. Sept. 12, 2018) (“The use of trade secret information in deciding whether to enter the market can be a cognizable harm.”); *Council on Am.-Islamic Rels. Action Network, Inc. v. Gaubatz*, 82 F. Supp. 3d 344, 361 (D.D.C. 2015) (holding that the court need not rule on whether the donor lists at issue are trade secrets because plaintiffs failed to identify “any cognizable harm to them or unjust enrichment of Defendants regarding these lists”).

<sup>10</sup> See *Chevron Corp. v. Donziger*, 974 F. Supp. 2d 362, 554 n.1257 (S.D.N.Y. 2014) (averring, prior to *TransUnion v. Ramirez*, 141 S. Ct. 2190 (2021), in dicta that the logic of *Clapper v. Amnesty Int'l USA*, 568 U.S. 398 (2013), should not apply to private disputes because such applications “could alter dramatically . . . the law governing preliminary injunctions in trade secret cases”); Daniel J. Solove & Danielle K. Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 101 B.U. L. REV. ONLINE 62, 65 (2021) (“If *Spokeo* and *TransUnion* are carried to their logical conclusion, common and longstanding private rights of action for countless laws, including copyright law, might no longer be viable in federal court.”); Christopher Morten, *TransUnion is a Double-Edged Sword*, L. & POL. ECON. PROJ. (Sept. 20, 2021) <https://perma.cc/576M-9D53> (“In various federal IP statutes, Congress has provided IP rights holders with additional rights to use federal courts for redress of contrived non-monetary injuries. Under *TransUnion*, these rights may no longer be enforceable.”); see also Sharon K. Sandeen, *Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort*, 19 MINN. J.L. SCI. & TECH. 373, 392–400 (2018) [hereinafter Sandeen, *Out of Thin Air*] (suggesting that it is unclear whether some trade secret violations result in cognizable harm and explaining that “[u]nder longstanding principles of tort law, ordinarily there can be no tort recovery without a wrongful act that causes cognizable injury”).

spreadsheet featuring a customer list constructed by the ex-employee and her team), as well as employee information, including some employees' Social Security numbers and driver's license information. Following the audit, Company X notifies the affected employees. Two lawsuits follow.

The first lawsuit is a class action brought by the employees against Company X for the data breach. The employees are understandably furious that Company X relinquished their sensitive data. They argue that it is common practice for companies to cut off former employees' network access and login credentials immediately upon termination, and Company X neglected to do so until well after the ex-employee's termination. Accordingly, the employees bring common law tort allegations against the company in federal court, seeking both damages and injunctive relief for various forms of harm: an increased risk of identity theft, time spent mitigating the increased risk of identity theft, and a loss of privacy.

While the employees' lawsuit might seem like enough to get through the courthouse doors, federal courts often dismiss similar cases for a lack of Article III standing.<sup>11</sup> Courts that do not find standing in such cases usually highlight that the plaintiffs cannot demonstrate a legally cognizable harm—a harm that federal courts are constitutionally authorized to hear—because none of the class's data has yet been misused; thus, any real-world harm alleged by the class members is thought to be too intangible and speculative for a court to reach the merits of the dispute.<sup>12</sup> The data breach surely increases the chance that the data *will* be misused, but increased risk is often held insufficient to form the basis of a lawsuit in federal court.<sup>13</sup>

---

<sup>11</sup> See, e.g., *Beck v. McDonald*, 848 F.3d 262, 274 (4th Cir. 2017) (holding that plaintiffs lacked standing for an increased risk of identity theft resulting from a data breach); see also *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332, 1343 (11th Cir. 2021) (rejecting standing in a data breach case for plaintiffs alleging harms of substantial risk of identity theft, mitigation costs, and conclusory allegations of unauthorized charges).

<sup>12</sup> See *Beck*, 848 F.3d at 274.

<sup>13</sup> See *McMorris v. Carlos Lopez & Assocs., LLC*, 995 F.3d 295, 303 (2d Cir. 2021) (holding that employees whose Social Security numbers were exposed did not have standing based on an increased risk of identity theft theory); see also *Reilly v. Ceridian Corp.*, 664 F.3d 38, 40–42 (3d Cir. 2011) (finding plaintiff-employees' increased risk of identity theft theory too speculative to establish a "certainly impending" injury-in-fact, and articulating that the employees "have not suffered any injury; there has been no misuse of the information, and thus, no harm"). Still, some courts have found standing for a risk of identity theft following a data breach because "determining standing is an inherently fact-specific inquiry." *McMorris*, 995 F.3d at 302. Courts that do find Article III

The second lawsuit is brought by Company X, which sues the former employee in federal court, alleging a violation of the DTSA. The DTSA added a federal civil claim to the Economic Espionage Act<sup>14</sup> (EEA) to protect companies from cyberespionage by bad actors including business competitors, foreign governments, and ex-employees.<sup>15</sup> The DTSA generally requires plaintiffs to plead three elements: (1) that they possessed a trade secret; (2) that the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce; and (3) that Defendants misappropriated or threatened to misappropriate that trade secret.<sup>16</sup> The plaintiff-company alleges that their ex-employee violated the DTSA insofar as she “misappropriated” their customer list, a trade secret, by acquiring it outside of the course of her employment and thus through “improper means.”<sup>17</sup> The company does not allege that the customer list has been disclosed or misused, nor do they allege surrounding circumstances that would make it seem likely that the customer list is about to be disclosed or misused.

Curiously, in contrast with the employee class action, the case law indicates that a federal court would not dismiss Company X’s DTSA lawsuit against their ex-employee for a lack of standing. Indeed, in DTSA cases similar to the above hypothetical, courts often skirt the issue of Article III standing

---

standing under an increased risk of identity theft theory generally require allegations regarding the data thief’s sophistication or bad intent, such that the injury becomes imminent. *See, e.g., Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157 (3d Cir. 2022) (finding standing where the asserted theory of injury is a risk of identity theft because “a sophisticated ransomware group” stole plaintiffs’ data with a clearly nefarious intent).

<sup>14</sup> *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488 (codified as amended at 18 U.S.C. §§ 1831–1839).

<sup>15</sup> *See* Press Release, Sen. Orrin Hatch, *Senator Coons, Hatch Applaud Committee Passage of Trade Secrets Legislation* (Jan. 28, 2016), <https://perma.cc/8F85-TT4M> [hereinafter Sen. Hatch Press Release] (“In today’s electronic age, trade secrets can be stolen with a few keystrokes, and increasingly, they are stolen at the direction of a foreign government or for the benefit of a foreign competitor.”).

<sup>16</sup> 18 U.S.C. § 1836(b)(1); *see, e.g., Oakwood Lab’s LLC v. Thanoo*, 999 F.3d 892, 905 (3d Cir. 2021).

<sup>17</sup> *See* 18 U.S.C. § 1836(b). Courts frequently accept the argument that customer lists are trade secrets. *See* 1 MELVIN F. JAGER, TRADE SECRETS LAW § 3:3 (2010). Indeed, disputes involving customer lists are a common variant of trade secret claims heard by federal courts. *See* Jeffrey Mordaunt, TRENDS IN TRADE SECRET LITIGATION REPORT 2020, at 9 (2020); *JetSmarter Inc. v. Benson*, 2018 WL 2694598, at \*5 (S.D. Fla. Apr. 6, 2018) (finding misappropriation plausibly pled where an employer alleged that a former employee improperly retained a customer list after termination).

completely.<sup>18</sup> Yet, it is well-settled that courts have an obligation to assess standing *sua sponte* before reaching the merits of a case.<sup>19</sup> That is, because standing is a jurisdictional requirement enshrined in Article III, federal courts are powerless to adjudicate a dispute unless a litigant “plausibly and clearly allege[s]” that they have met the requirements of standing at the pleading stage.<sup>20</sup>

The above hypothetical illustrates a divergence in Article III standing as applied to data breach and DTSA lawsuits, respectively. Data breach cases frequently result in dismissal for a lack of concrete or imminent injury, while federal courts uniformly confer Article III standing in DTSA cases alleging the mere improper acquisition or threatened misappropriation of trade secrets. There are important differences between data breach cases and DTSA cases,<sup>21</sup> and DTSA cases, by definition, rely on a federal statute, while data breach cases largely do not. However, insofar as both cases involve ephemeral harms—information theft—and need not involve any actual economic loss, it may be difficult to reconcile courts’ differing applications of standing requirements in the two types of cases.

This Comment argues that modern standing doctrine demands that DTSA plaintiffs demonstrate something beyond the improper acquisition or threatened misappropriation of trade

---

<sup>18</sup> See, e.g., *AUA Priv. Equity Partners, LLC v. Soto*, 2018 WL 1684339, at \*7 (S.D.N.Y. Apr. 5, 2018) (holding that a plaintiff sufficiently pled a DTSA claim based on the improper acquisition of a trade secret where confidential data was allegedly sent from the employee-defendant’s work laptop to their personal cloud-based storage, without undergoing standing analysis or considering whether the misappropriated trade secrets could conceivably be used to harm the plaintiff’s business); see also *HIRECounsel D.C., LLC v. Connolly*, 2021 WL 5998365, at \*5 (D.D.C. Dec. 20, 2021) (finding a sufficiently pled improper acquisition claim without undergoing standing analysis, where a plaintiff alleged that an employee took a screen shot of a confidential report and forwarded it to his personal email address).

<sup>19</sup> See, e.g., *Friends of the Earth v. Laidlaw*, 528 U.S. 167, 180–81 (2000) (highlighting the court’s “obligation to assure [itself] that [the plaintiff] had Article III standing at the outset of the litigation”).

<sup>20</sup> *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1621 (2020).

<sup>21</sup> For instance, plaintiffs are typically unable to identify the data thief in data breach cases, while trade secret actions often involve identifiable bad actors. *But see* David S. Almeling, Darin W. Snyder, Michael Sapoznikow, Whitney E. McCollum & Jill Weader, *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 302 (2010) (finding that, although rare, there are cases in which the identity of the alleged trade secret misappropriator is unknown). Moreover, as discussed, *infra*, in Part V.A., some states understand trade secrets as property rights, while personal data is typically not understood as such. See, e.g., Richard S. Murphy, *Property Rights in Personal Information*, 84 GEO. L. REV. 2381, 2393 (1996).

secrets, just as the doctrine demands that data breach plaintiffs show something more than the theft of sensitive data or a mere threat of identity theft. Trade secret plaintiffs, like data breach plaintiffs, should often be required to show more than mere acquisition or threat because—as will be shown below—neither improper acquisition nor threatened misappropriation of trade secrets are necessarily cognizable injuries.

The impact of this thesis is threefold. First, and most importantly, it illustrates that federal courts may be adjudicating trade secret cases that they do not actually have the constitutional power to hear. That is, when federal courts adjudicate cases alleging improper acquisition or threatened misappropriation of trade secrets without considering standing, they allow cases that do not plausibly allege a cognizable injury to slip through the cracks.

That federal courts may be deciding cases over which they do not have constitutional jurisdiction is enough reason to be concerned about whether certain DTSA violations are injuries-in-fact. Yet, in the trade secret context, ensuring that federal courts are only acting within their constitutional mandate will have the second benefit of preserving employee mobility in the marketplace: injunctions issued against employees impose limits on their mobility, trade secret litigation can chill employees from leaving, and employers may be unwilling to hire someone who has been sued for trade secret violations.<sup>22</sup>

Third, and finally, requiring plaintiff-companies to demonstrate actual injury in trade secret cases will ensure that federal trade secret law develops effectively. Indeed, a common justification for the injury-in-fact requirement is that actual injury increases litigants' incentive to present genuine issues to courts, such that courts can decide cases and create law through incremental and fact-specific determinations.<sup>23</sup> This justification

---

<sup>22</sup> See, e.g., ORLY LOBEL, *TALENT WANTS TO BE FREE: WHY WE SHOULD LEARN TO LOVE LEAKS, RAIDS, AND FREE RIDING* 52 (2013) (“Because employers cannot require their employees to stay in their current position, they must find other ways to prevent their ex-employees from competing with them.”); see also J. PATRICK HUSTON, *THE LAW OF TRADE SECRET LITIGATION* 442 (2020) (“Some courts have held that when plaintiff’s former employee misappropriates plaintiff’s trade secrets on leaving plaintiff, and the former employee joins another company, that other company can be liable for the former employee’s misappropriation under the doctrine of respondeat superior.”).

<sup>23</sup> See Eugene Kontorovich, *What Standing Is Good For*, 93 VA. L. REV. 1663, 1672 (2007); see also *Friends of the Earth*, 528 U.S. at 191 (“Standing doctrine functions to ensure, among other things, that the scarce resources of the federal courts are devoted to those disputes in which the parties have a concrete stake.”).



applies in the DTSA context because the DTSA is charting new territory through its federalization of an area that traditionally belonged to the states. To ensure that DTSA plaintiffs' claims are appropriate for adjudication in federal court, courts should force plaintiffs to precisely articulate in their complaints how a defendant's actions have caused them real-world harm.

This Comment proceeds in five Parts. Part I begins by elucidating modern Article III standing doctrine. Part II provides a background on trade secret law and the DTSA. Part III then advances a novel thesis: certain violations of the DTSA are not cognizable harms because they are neither concrete nor imminent injuries under modern standing doctrine. And Parts IV and V respond to Part III by offering two forceful objections and demonstrating three plausible, but potentially unsatisfying, paths for plaintiff companies to achieve standing in trade secret cases where standing may be questionable. Ultimately, this Comment contends that courts should more carefully evaluate standing for DTSA violations, even if strict evaluation of standing imposes an additional barrier for plaintiffs' entry into federal court.

## I. MODERN STANDING DOCTRINE

Standing doctrine is the crucial mechanism through which federal courts enforce the boundaries of cases that they have the power to adjudicate. It is rooted in Article III of the Constitution, which outlines various categories of "cases" and "controversies" that federal courts can address.<sup>24</sup> While the Constitution does not precisely explain the contours of "cases" and "controversies," since early U.S. history, the Supreme Court has understood the words to "defin[e] the judicial power of the United States."<sup>25</sup> Thus, the doctrine of standing has long been described as an "irreducible constitutional minimum" of Article III's case-or-controversy requirement.<sup>26</sup>

Modern standing doctrine requires plaintiffs to demonstrate three elements—*injury-in-fact*, *causation*, and *redressability*—

---

<sup>24</sup> See U.S. CONST. art. III, § 2, cl. 1.

<sup>25</sup> *Martin v. Hunter's Lessee*, 14 U.S. 304, 328 (1816); see also *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 102 (1998) (explaining that defining the terms "cases" and "controversies" requires looking to "common understanding of what activities are appropriate to legislatures, to executives, and to courts" (quoting *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 559–60 (1992))).

<sup>26</sup> *Lujan*, 504 U.S. at 560.

the first of which is at issue in this Comment.<sup>27</sup> The injury-in-fact element scrutinizes whether plaintiffs are alleging “real” harm. Said another way, the injury-in-fact element asks whether a plaintiff is plausibly alleging the type of injury that can be considered by federal courts under their constitutional mandate. Injury-in-fact is at issue in this Comment because certain violations of the DTSA may result in merely ephemeral or threatened injuries.

The other two elements of standing are not relevant here. The causation element of the doctrine only requires plaintiffs to demonstrate that their alleged injury is traceable to the defendant. Insofar as it is usually clear *who* allegedly committed the DTSA violations at issue—an employee, in the vast majority of cases<sup>28</sup>—causation is not in question. The redressability prong—which requires that the injury “will likely be redressed by a favorable decision”<sup>29</sup>—is also not at issue because DTSA plaintiffs’ alleged injuries can be mitigated through injunctive relief and money damages awarded by the court. In sum, while causation and redressability are factors that courts must consider in evaluating standing, the crucial element that courts currently overlook in this sphere is that certain DTSA claimants may be failing to adequately allege an injury-in-fact, and therefore seemingly lack standing.

#### A. Injury-in-Fact

This Section expands upon the injury-in-fact element, which has three sub-parts. To adequately plead an injury-in-fact, plaintiffs must plausibly allege that they have suffered a “concrete, particularized, and actual or imminent” injury.<sup>30</sup>

---

<sup>27</sup> See *id.* at 560–61. Standing doctrine has changed in recent decades. See Cass R. Sunstein, *What’s Standing After Lujan?*, 91 MICH. L. REV. 163, 169 (1992) (“The explosion of judicial interest in standing as a distinct body of constitutional law is an extraordinarily recent phenomenon.”); John A. Ferejohn & Larry D. Kramer, *Independent Judges, Dependent Judiciary: Institutionalizing Judicial Restraint*, 77 N.Y.U. L. REV. 962, 1009 (2002) (finding that “[t]here was no doctrine of standing prior to the middle of the twentieth century”). Prior to the modern development of standing doctrine, “a plaintiff’s right to bring suit was determined by reference to a particular common law, statutory, or constitutional right, or sometimes to a mixture of statutory or constitutional prohibitions and common law remedial principles.” William A. Fletcher, *The Structure of Standing*, 98 YALE L.J. 221, 224 (1988).

<sup>28</sup> See 1 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 5.01[1] (1996).

<sup>29</sup> *Clinton v. City of New York*, 524 U.S. 417, 435 (1998).

<sup>30</sup> *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2203 (2021).

Plaintiffs who do not meet this triumvirate of requirements cannot have their claim heard in federal court.

After elucidating the sub-parts of the injury-in-fact element of standing, this Comment will show in Part I.B how they have been applied to dismiss data breach plaintiffs' lawsuits. Finally, in Part I.C, this Comment will describe why standing arguments should similarly apply with particular force in DTSA cases.

### 1. Concrete.

For a plaintiff to gain access to federal court, they must demonstrate a concrete injury. The boundaries of concreteness are elusive. But a "concrete" injury must be 'de facto,' that is, it must actually exist.<sup>31</sup> The world of concrete injuries is far narrower than what a lay person might consider to be an injury or harm. For example, many forms of psychological harm do not constitute concrete injuries; likewise, many privacy harms fail to meet the concreteness threshold.<sup>32</sup> The Supreme Court most recently illuminated the concreteness requirement in two cases: *Spokeo, Inc. v. Robins*<sup>33</sup> and *TransUnion LLC v. Ramirez*.<sup>34</sup>

In *Spokeo*, plaintiff Thomas Robins sued Spokeo, a data aggregator, for wrongly informing users that Robins was married, affluent, and employed.<sup>35</sup> Robins alleged that the data aggregator put at risk his ability to find employment because the wrong information could make him seem overqualified to prospective employers.<sup>36</sup> He sued under the Fair Credit Reporting Act of 1970<sup>37</sup> (FCRA)—a statute that expressly authorized private suits

---

<sup>31</sup> *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016) (emphasis omitted).

<sup>32</sup> See Evan T. Lee & Josephine M. Ellis, *The Standing Doctrine's Dirty Little Secret*, 107 NW. U. L. REV. 169, 179 (2015) (collecting cases that show many noneconomic harms are not considered concrete injuries). Privacy harms are, in some ways, similar to trade secret harms. For instance, Professor Robert Post has persuasively argued that privacy torts are rooted in "social norms" and "safeguard[ ] rules of civility." See Robert C. Post, *The Social Foundations of Privacy*, 77 CAL. L. REV. 957, 959 (1989). Similarly, as discussed in Part II, a key underlying justification for trade secret law is the promotion of "commercial ethics." See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974). See generally Don Wiesner & Anita Cava, *Stealing Trade Secrets Ethically*, 47 MD. L. REV. 1076 (1988) (collecting cases that demonstrate trade secret law is a means of enforcing standards of commercial morality). Like privacy harms, trade secret harms are ephemeral and abstract. They appear to interfere with rights but need not involve setbacks to interests that one can easily see, like an actual loss of money or business.

<sup>33</sup> 578 U.S. 330 (2016).

<sup>34</sup> 141 S. Ct. 2190 (2021).

<sup>35</sup> *Spokeo*, 578 U.S. at 336.

<sup>36</sup> *Id.* at 350 (Ginsburg, J., dissenting).

<sup>37</sup> 84 Stat. 1127 (codified at 15 U.S.C. § 1681).

to enforce the law—arguing that the company failed to “assure maximum possible accuracy” in aggregating his personal information, as was required under the statute.<sup>38</sup>

The Court vacated and remanded Robins’s case because it found that he might not have alleged a concrete injury.<sup>39</sup> Robins lacked a clearly concrete injury because he could not identify a “real” injury that flowed from Spokeo’s statutory violation.<sup>40</sup> For instance, Robins did not allege that he had lost a specific job opportunity because of the statutory violation. The Court made clear that a “bare procedural violation” of a statute is not sufficient to establish a concrete injury as required under Article III.<sup>41</sup>

In remanding Robins’s case, the *Spokeo* Court appreciably expanded the concreteness requirement for the first time in its standing jurisprudence. It indicated that injuries with tangible physical or economic manifestations most cleanly fit into the Court’s conception of concrete injury.<sup>42</sup> However, intangible, ephemeral injuries could still be concrete if they have a “close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.”<sup>43</sup> Examples of intangible injuries that the Court has since endorsed as cleanly mapping onto the *Spokeo* common law analogy are those closely related to torts like defamation, libel, slander per se, disclosure of private information, and intrusion upon seclusion.<sup>44</sup>

The Court doubled down on *Spokeo* in *TransUnion*, one of its most recent standing cases. The *TransUnion* Court did not find a concrete injury for plaintiffs who alleged a risk of harm based on the presence of misleading Office of Foreign Assets Control (OFAC) alerts in their credit files, which branded the plaintiffs as “potential terrorists.”<sup>45</sup> The Court found that plaintiffs whose misleading credit files were not disseminated lacked a concrete

---

<sup>38</sup> *Spokeo*, 578 U.S. at 335.

<sup>39</sup> *Id.* at 341.

<sup>40</sup> *Id.* at 350.

<sup>41</sup> *Id.* at 342.

<sup>42</sup> *Id.*

<sup>43</sup> *Spokeo*, 578 U.S. at 341.

<sup>44</sup> See *TransUnion*, 141 S. Ct. at 2200–07. For reasons explained *infra*, in Part V.C, these common law torts, among others, fail to cleanly map onto the DTSA violations at issue in this Comment.

<sup>45</sup> *Id.* at 2203–07. *TransUnion* is a credit reporting agency that sells consumer reports on individuals’ creditworthiness. *Id.*

injury because the misleading information had not yet been distributed to creditors.<sup>46</sup>

Importantly, the misleading credit files amounted to a violation of the FCRA.<sup>47</sup> Nevertheless, again, the Court found that a bare statutory violation was not enough to confer standing.<sup>48</sup> While such a statutory violation *is* an injury in law, an “injury in law is not an injury in fact.”<sup>49</sup> The plaintiffs attempted to invoke the common law analog test from *Spokeo*, likening the misleading OFAC alerts to the historically recognized tort of defamation.<sup>50</sup> But their analogy was deemed inapposite because a key common law ingredient to defamation is dissemination of defamatory information, which many of the *TransUnion* plaintiffs did not allege.<sup>51</sup>

Put simply, the *TransUnion* plaintiffs whose misleading credit files were not disseminated had no standing because the presence of potentially damaging information in a database alone is not a concrete harm. Rather, it is an intangible, abstract, or ephemeral harm that is unlike any injury historically recognized as one that could form the basis of a lawsuit.<sup>52</sup> The inaccurate information in the litigants’ credit files was, to the *TransUnion* majority, like a defamatory letter that someone wrote and stored in a desk drawer: neither the letter nor the inaccurate credit files sitting in the database were likely to harm anyone, absent the actions of decisionmakers downstream, such as creditors who could use the information to inflict economic harm on the litigants.<sup>53</sup>

While concerns about the separation of powers motivate all three injury-in-fact requirements,<sup>54</sup> separation of powers concerns come to bear perhaps most conspicuously in the concreteness

---

<sup>46</sup> *Id.* at 2212.

<sup>47</sup> 84 Stat. 1127 (codified at 15 U.S.C. § 1681).

<sup>48</sup> *TransUnion*, 141 S. Ct. at 2207.

<sup>49</sup> *Id.* at 2205.

<sup>50</sup> *Id.* at 2208.

<sup>51</sup> *Id.* at 2209 (noting that the “remaining 6,332 class members are a different story” because “the parties stipulated that *TransUnion* did not provide those plaintiffs’ credit information to any potential creditors during the class period”).

<sup>52</sup> *See id.* at 2204. The Court held that the class members whose reports *were* disseminated to third parties suffered concrete harm analogous to reputational harm associated with the historically recognized tort of defamation. *TransUnion*, 141 S. Ct. at 2208.

<sup>53</sup> *See id.* at 2210.

<sup>54</sup> *Id.* at 2203–2207. *See generally* Heather Elliott, *The Functions of Standing*, 61 STAN. L. REV. 459, 461–63 (2008) (highlighting separation of powers justifications for standing doctrine).

requirement. The Court has reasoned that it is for the courts, not Congress, to decide when a violation of a statute is sufficient for standing. In declining to allow Congress to “enact an injury into existence” through statutory causes of action,<sup>55</sup> the Court ensures that Congress cannot “us[e] its lawmaking power” to encroach on the judiciary.<sup>56</sup>

To be sure, the Court has acknowledged that “Congress is well positioned to identify intangible harms that meet minimum Article III requirements.”<sup>57</sup> Nevertheless, the concreteness requirement establishes a “hard floor” that the Court has said cannot be removed by Congress via statute.<sup>58</sup> As Professor Gene Nichol has explained, “the assumption here is that there exists a universe of ‘de facto’ injuries that constitutes the outer boundary of federal jurisdiction. So long as Congress chooses from among the pool, Article III is not transgressed.”<sup>59</sup>

## 2. Actual or imminent.

The actual or imminent requirement is closely connected to the concreteness requirement. It ensures that litigants are alleging personal harm that is neither potential nor hypothetical. In other words, the plaintiff must show that they have “‘sustained or [are] immediately in danger of sustaining some direct injury’ as the result of the challenged [ ] conduct.”<sup>60</sup>

*Clapper v. Amnesty International USA*<sup>61</sup> is a key Supreme Court case that elucidates the imminence requirement of standing: it demonstrates that a risk of harm can be enough to establish standing only when injury is “certainly impending.”<sup>62</sup> *Clapper* involved a challenge to the Foreign Intelligence Services Act of 1978<sup>63</sup> (FISA), which authorizes the U.S. government to conduct surveillance on non-U.S. citizens outside of U.S.

---

<sup>55</sup> *TransUnion*, 141 S. Ct. at 2205.

<sup>56</sup> *Id.*

<sup>57</sup> *Spokeo*, 578 U.S. at 341.

<sup>58</sup> *Summers v. Earth Island Inst.*, 555 U.S. 488, 497 (2009); *see also TransUnion*, 141 S. Ct. at 2205 (“[W]e cannot treat an injury as ‘concrete’ for Article III purposes based only on Congress’s say-so.” (quoting *Trichell v. Midland Credit Mgmt., Inc.*, 964 F.3d 990, 999 n.2 (11th Cir. 2020))).

<sup>59</sup> *See* Gene R. Nichol, *The Impossibility of Lujan’s Project*, 11 DUKE ENVTL. L. & POL’Y F. 193, 203 (2001).

<sup>60</sup> *Los Angeles v. Lyons*, 461 U.S. 95, 102 (1983).

<sup>61</sup> 568 U.S. 398 (2013).

<sup>62</sup> *Id.* at 401.

<sup>63</sup> Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. § 1802).

borders.<sup>64</sup> The plaintiffs, Amnesty International lawyers, sued under the theory that there was an “objectively reasonable likelihood” that their sensitive communications with colleagues and clients located abroad would be recorded under FISA.<sup>65</sup> The Court held that the plaintiffs’ future injury—the possibility of recorded communications by the U.S. government—was not an injury-in-fact because it was not sufficiently imminent. A standard of an “objectively reasonable likelihood” was found to be “inconsistent with [the Court’s] requirement that ‘threatened injury must be certainly impending to constitute injury in fact.’”<sup>66</sup>

The Court also rejected the plaintiffs’ other theory of injury, which relied on the “costly and burdensome measures” they took to “protect the confidentiality of their international communications.”<sup>67</sup> The Court held that the prophylactic measures amounted to “manufacture[d] standing”<sup>68</sup> because they were “based on hypothetical future harm,” rather than “certainly impending” harm.<sup>69</sup>

Following *Clapper*, the actual or imminent requirement is most salient for plaintiffs seeking equitable relief because such claims are often necessarily based on harm that may not come to fruition.<sup>70</sup> Courts are generally skeptical of claims seeking prospective relief from threatened harms because such cases are essentially hypothetical disputes, the resolution of which are reserved for the political branches, not federal courts.<sup>71</sup>

### 3. Particularized.

A plaintiff must do more than plausibly allege a concrete and actual or imminent injury to get through the federal courthouse doors. They must also allege that they *personally* were injured. A “generally available grievance” against the government, for

---

<sup>64</sup> *Clapper*, 568 U.S. at 404.

<sup>65</sup> *Id.* at 407.

<sup>66</sup> *Id.* at 410 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The Court left open the possibility that a future injury could meet standing requirements if plaintiffs illustrate “substantial risk that the harm will occur.” *Id.* at 414 & n.5 (quotation marks and citations omitted).

<sup>67</sup> *Id.* at 402.

<sup>68</sup> *Clapper*, 568 U.S. at 402.

<sup>69</sup> *Id.*

<sup>70</sup> *See, e.g.*, *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014).

<sup>71</sup> *See generally* F. Andrew Hessick, *Probabilistic Standing*, 106 NW. U. L. REV. 55, 65 (2012) (illustrating that probabilistic injuries sometimes fail to satisfy Article III standing by recognizing, but critiquing, standing doctrine’s “minimum-risk requirement”).

example, is not a particularized injury.<sup>72</sup> But the particularization requirement is not at issue in this Comment because, unlike the other two injury-in-fact requirements, the particularization requirement does not scrutinize whether the nature of the injury—or the timing of the injury—is suitable for standing. Rather, it scrutinizes to whom the injury is inflicted. And DTSA plaintiffs—often business entities<sup>73</sup>—typically allege that their own trade secrets have been misappropriated, such that their injuries are particularized.<sup>74</sup>

## B. The Data Breach Cases

Data breach cases provide a possible lens through which to view the intersection of trade secret law and standing. Courts' skepticism that certain harms can establish an injury-in-fact for standing has been borne out in the data breach context: courts regularly use *Spokeo*, *TransUnion*, and *Clapper* to dismiss data breach cases that show ephemeral and threatened, rather than concrete and imminent, harm.<sup>75</sup> Plaintiffs who come to court alleging only that their data has been taken, rather than misused to inflict real-world economic injury, are routinely turned away for failure to plausibly allege an injury-in-fact because such plaintiffs are thought to lack both concrete and imminent injuries.<sup>76</sup>

For example, in *I.C. v. Zynga, Inc.*<sup>77</sup>—one of the dozens of data breach cases dismissed for a lack of standing in *Clapper*'s wake<sup>78</sup>—plaintiffs brought a class action against gaming company Zynga in connection with a data breach of players' information.<sup>79</sup> Plaintiffs sought both damages and injunctive relief for, inter

---

<sup>72</sup> See *Lujan*, 504 U.S. at 573.

<sup>73</sup> See Bailey, *supra* note 2.

<sup>74</sup> See Charles T. Graves, *Curiosities of Standing in Trade Secret Law*, 20 NW. J. TECH. & INTELL. PROP. 159, 173 (2023) (exploring standing in terms of what parties have the right to pursue trade secret violations in court).

<sup>75</sup> See, e.g., *Beck*, 848 F.3d at 274.

<sup>76</sup> *Legg v. Leaders Life Ins. Co.*, 574 F. Supp. 3d 985, 990 (W.D. Okla. 2021) (“[A]ll of the circuit court cases ‘conferring standing after a data breach based on an increased risk of theft or misuse included at least some allegations of actual misuse.’”).

<sup>77</sup> 600 F. Supp. 3d 1034 (N.D. Cal. 2022).

<sup>78</sup> See Thomas D. Haley, *Data Protection in Disarray*, 95 WASH. L. REV. 1193, 1220 (2020) (collecting cases and providing an empirical analysis of the more than 200 data breach cases in federal court that have litigated standing, nearly half of which cite *Clapper*, resulting in a relatively high rate of dismissal for a lack of standing).

<sup>79</sup> *Zynga*, 600 F. Supp. 3d at 1036–41.



alia, an increased risk of identity theft, costs to mitigate their risk of identity theft, emotional distress, and a loss of privacy.<sup>80</sup>

The district court relied on *TransUnion*, *Clapper*, and *Spokeo* to dismiss the suit for a lack of standing.<sup>81</sup> The court found that plaintiffs' theories of injury were insufficiently concrete because they were too dissimilar from the traditional intangible harms recognized by *Spokeo* as concrete.<sup>82</sup> Moreover, the court found that the injuries lacked sufficient imminence. Insofar as the data thieves had not misused any of the stolen information to commit identity theft, the court reasoned, "the risk of harm which caused the asserted costs and stress [was] too conjectural."<sup>83</sup>

In sum, as federal courts' recent data breach rulings illustrate, an injury-in-fact requires a showing of a real-world injury suffered—or about to be suffered—by the plaintiff themselves. Requirements like standing ensure that federal courts are only hearing cases that they are constitutionally authorized to hear: those involving real injuries, rather than speculative or generalized grievances. That is, the doctrine is grounded in both constitutional and prudential considerations; it maintains the separation of powers, restricts courts to adjudicating only those disputes within their purview, and lends itself to the sort of adversarial process that "sharpens the presentation of issues."<sup>84</sup>

### C. Standing and the DTSA

Simply put, if improper acquisition and threatened misappropriation—both statutory violations of the DTSA—are not per se injuries-in-fact, then many courts risk adjudicating cases that they do not have the constitutional power to hear. Of course, it is critical to ensure in every matter that federal courts are adjudicating exclusively those cases that plausibly allege an injury-in-fact because the Supreme Court—the final arbiter of constitutional meaning—has understood Article III to require it.<sup>85</sup>

---

<sup>80</sup> *Id.* at 1052.

<sup>81</sup> *Id.* at 1046–48.

<sup>82</sup> *Id.* at 1048.

<sup>83</sup> *Id.* at 1052.

<sup>84</sup> *Baker v. Carr*, 369 U.S. 186, 204 (1962).

<sup>85</sup> Modern standing doctrine has no shortage of critics. See, e.g., *Sierra v. City of Hallandale Beach*, 996 F.3d 1110, 1132 (11th Cir. 2021) (Newsom, J., concurring) (averring that standing "is incoherent in theory and easily manipulable in practice"); see also ERWIN CHEMERINSKY, *CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES* 61 (6th ed. 2019) ("The Court has not consistently articulated a test for standing. . . . Moreover, many

Indeed, the Court has repeatedly highlighted the importance of strictly policing the boundaries of judicial power in its precedents.<sup>86</sup> Thus, ensuring that federal courts hear exclusively the types of disputes that they have the constitutional power to decide is, in itself, enough reason to scrutinize standing in DTSA cases.

But a lack of standing analysis in DTSA cases elicits particular concern for at least two reasons. First, a lack of standing scrutiny in DTSA cases undermines the quality of federal trade secret law; and second, a lack of standing scrutiny allows private litigants to improperly leverage federal courts to curb employee mobility and competition.

Adjudication of only injuries-in-fact promotes sound judicial decision-making and encourages the creation of quality precedent.<sup>87</sup> This applies with particular force in the context of the DTSA because the DTSA, enacted in 2016, is a relatively new statute, and it concerns an area of law that has traditionally been the province of the states.<sup>88</sup> As such, there is not a wide body of federal trade secret case law.<sup>89</sup> The creation of judicial opinions only when an actual injury has been—or is about to be—inflicted will allow federal trade secret law to progress most effectively.<sup>90</sup>

Second, ensuring a showing of an injury-in-fact protects defendants from plaintiff-employer overreach vis à vis the federal judiciary.<sup>91</sup> Courts are obligated to prevent private parties from using the judiciary to assert their will against others who have

---

commentators believe that the Court has manipulated standing rules based on its views of the merits of particular cases.”). Such critiques are beyond the scope of this Comment, which has the relatively narrow purpose of cohering trade secret lawsuits with modern standing doctrine.

<sup>86</sup> See *Valley Forge Christian Coll. v. Am. United for Separation of Church & State, Inc.*, 454 U.S. 464, 489 (1982) (explaining the importance of refusing to “convert standing into a requirement that must be observed only when satisfied”); see also Martin H. Redish & Sopan Joshi, *Litigating Article III Standing: A Proposed Solution to the Serious (But Unrecognized) Separation of Powers Problem*, 162 U. PA. L. REV. 1373, 1375 (2014).

<sup>87</sup> See F. Andrew Hessick, *Standing, Injury in Facts, and Private Rights*, 93 CORNELL L. REV. 275, 321 (2008) (“Courts and commentators often state . . . that a factual injury provides context for a court’s decision, both making the case more ‘real’ and increasing the chance of a sound decision by forcing the court to be aware of the impact of its decision.”).

<sup>88</sup> See JAGER, *supra* note 17, at § 2:1.

<sup>89</sup> See *Houser v. Feldman*, 569 F. Supp. 3d 216, 224 (E.D. Pa. 2021) (observing the lack of federal trade secret law).

<sup>90</sup> See Hessick, *Standing, Injury in Facts, and Private Rights*, *supra* note 87, at 321.

<sup>91</sup> Trade secret plaintiffs may use litigation to “strategically harass[] potential competitors, threaten[] litigation to deter a star employee from leaving, or act[] on a desire to prevent the leakage of embarrassing facts.” Hrды, *supra* note 7, at 561.

not yet caused any real damage.<sup>92</sup> This is an important limiting principle in the trade secret context because standing can be a bulwark against overreaching by employers and marketplace competitors. As Professor Deepa Varadarajan observes, “[t]rade secret law can profoundly impact employees’ ability to move between jobs and take their knowledge and skills with them without fear of reprisal from former employers.”<sup>93</sup> Employers may have a tendency to sue employees—despite an absence of concrete or imminent damage—in order to chill them from exiting the firm, especially to go work for competitors. Similarly, employers may aim to weaponize trade secret claims with no showing of an injury-in-fact because their lawsuits can chill *other* companies, who can be liable for wrongs by the ex-employees they hire, from hiring their departed employees.<sup>94</sup> Marketplace competitors who have not been injured will similarly be incentivized to overreach in the trade secret context because they wish to quash competing companies through gratuitous lawsuits.<sup>95</sup> The mere existence of a lawsuit in federal court could exert pressure on both employees and competitors to settle cases that should otherwise be dismissed for a lack of standing.<sup>96</sup>

The upshot is that while courts ostensibly assume that injury has been inflicted because a trade secret violation has occurred, analysis should instead go back to first principles and ask precisely how—and, more boldly, whether—federal trade secret law fits into modern standing doctrine. The doctrine means little if it is ignored in borderline cases.

## II. THE DEFEND TRADE SECRETS ACT (DTSA)

This Part briefly discusses the history of trade secret law before introducing the violations of the DTSA at issue in this Comment: acquisition of a trade secret through a breach of a duty

---

<sup>92</sup> See Redish & Joshi, *supra* note 86, at 1377–78 (“To the extent that the federal courts coercively impact the lives of citizens in a manner not incident to the resolution of live disputes, they have exceeded their legitimate role in a democratic society and seriously undermined our constitutionally dictated system of separation of powers.”).

<sup>93</sup> Deepa Varadarajan, *Trade Secret Precautions, Possession, and Notice*, 68 HASTINGS L.J. 357, 360 (2017).

<sup>94</sup> See Huston, *supra* note 22, at 442.

<sup>95</sup> Professors David Levine and Sharon Sandeen have recently highlighted anticompetitive practices by so-called “trade secret trolls,” who aim to use frivolous trade secret litigation as a means of extracting settlement. David S. Levine & Sharon K. Sandeen, *Here Come the Trade Secret Trolls*, 71 WASH. & LEE L. REV. ONLINE 230 (2015).

<sup>96</sup> See, e.g., Redish & Joshi, *supra* note 86, at 1377.

to maintain secrecy, acquisition through espionage, and threatened misappropriation. The trade secret violations described below will be considered in the shadow of modern standing doctrine in Parts III, IV, and V.

#### A. An Overview of Trade Secret Law

Trade secret law is sometimes described as a sort of “intellectual property,”<sup>97</sup> but it is fundamentally separate from patent, copyright, and trademark law; it is an “anomaly” because it is based “on the breach of relationally specific duties.”<sup>98</sup> Trade secret law generally aims to protect trade secret holders from those who wrongly acquire, use, or disseminate their trade secrets, or threaten to do so. Meanwhile, trade secret law aspires to both promote innovation and encourage good faith in business.<sup>99</sup> These aims are often at odds with employee mobility insofar as trade secret plaintiffs frequently seek injunctions ordering defendant-employees not to compete against them.<sup>100</sup> A successful trade secret claim typically requires plaintiffs to demonstrate three basic elements: first, that the information for which protection is sought is a trade secret;<sup>101</sup> second, that the trade secret holder took reasonable measures to protect their information;<sup>102</sup> and third, that the defendant “misappropriated”<sup>103</sup> the trade secret.

While traditional forms of trade secrets include a “formula for a chemical compound, a process of manufacturing . . . or a list of

---

<sup>97</sup> See Amy Kapczynski, *The Public History of Trade Secrets*, 55 U.C. DAVIS L. REV. 1367, 1390 (2022).

<sup>98</sup> The DTSA states that the Act “shall not be construed to be a law pertaining to intellectual property for purposes of any other Act of Congress.” § 1836 2(g). See Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 243–44 (1998); see also JAGER, *supra* note 17, at § 3:11 (highlighting that “unlike a patent owner, a person who possesses a trade secret does not have an exclusive right to the information”).

<sup>99</sup> See, e.g., *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974).

<sup>100</sup> See *SI Handling Sys. v. Heisley*, 753 F.2d 1244, 1266–69 (3d Cir. 1985) (discussing the tendency of trade secret law to limit employee mobility); see also Edmund Kitch, *The Expansion of Trade Secrecy Protection and the Mobility of Management Employees*, 45 S.C. L. REV. 659, 665 (1996).

<sup>101</sup> In order to qualify as a trade secret, the information must have “independent economic value, actual or potential,” and it cannot be “generally known” by those in the relevant industry. See 18 U.S.C. § 1839(3).

<sup>102</sup> See 18 U.S.C. § 1839(3).

<sup>103</sup> Misappropriation includes improper acquisition, use, or disclosure of a trade secret. 18 U.S.C. § 1839(5). The DTSA also provides injunctive relief for “threatened misappropriation.” 18 U.S.C. § 1839(5).

customers,”<sup>104</sup> trade secrets are amorphous and defined broadly to include virtually any type of information that derives value from secrecy.<sup>105</sup> In recent years, trade secrets have become increasingly expansive.<sup>106</sup> For example, the Supreme Court of Washington recently found that data comprised of customer zip codes compiled by Lyft, the rideshare company, are trade secrets, largely because they are used by the company as a spatial indicator of revenue generation and for marketing new products.<sup>107</sup> Other courts have found that a company’s diversity strategies and initiatives are trade secrets.<sup>108</sup>

Trade secret law has a complex history and is derived from a variety of sources. Until the recent passage of the DTSA, trade secret law was considered the province of the states, although trade secret cases could be adjudicated by federal courts through means like diversity jurisdiction.<sup>109</sup> Early trade secret law developed in the common law as a form of unfair competition resulting from a breach of confidence.<sup>110</sup> In 1939, the American Law Institute published a summary of trade secret law in the Restatement (First) of Torts.<sup>111</sup> Many courts relied on the Restatement, which helped standardize trade secret law across states.<sup>112</sup>

However, trade secret law continued to develop inconsistently across the states and, as a response, the highly influential Uniform Trade Secrets Act<sup>113</sup> (UTSA), a model state statute, was published in 1979.<sup>114</sup> Forty-eight states have adopted a version of the UTSA.<sup>115</sup> Because of the scattered common law

---

<sup>104</sup> RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

<sup>105</sup> See 18 U.S.C. § 1839(5).

<sup>106</sup> See Kapczynski, *supra* note 97, at 1395; 3 RUDOLF CALLMANN, LAW OF UNFAIR COMPETITION, TRADEMARKS AND MONOPOLIES § 14:14 (4th ed. 2020) (“Almost any subject matter may be a trade secret.”).

<sup>107</sup> L/R’s Lyft, Inc. v. City of Seattle, 190 Wash. 2d 769, 774–83 (2018).

<sup>108</sup> See Jamillah Williams, *Diversity as a Trade Secret*, 107 GEO. L.J. 1685, 1697–98 (2019); see also Assessment Techs. Inst., LLC v. Parkes, 588 F. Supp. 3d 1178, 1194 (D. Kan. 2022) (finding that proctored nursing exams are trade secrets under the DTSA and KTSA).

<sup>109</sup> See JAGER, *supra* note 17, at § 2:1 (explaining that state courts developed trade secret law under different common law theories of injury: breach of contract, tort of breach of confidence, or infringement of property rights).

<sup>110</sup> *Id.*

<sup>111</sup> See RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

<sup>112</sup> JAGER, *supra* note 17, at § 3:1.

<sup>113</sup> UNIF. TRADE SECRETS ACT (UNIF. L. COMM’N 1979) (amended 1985).

<sup>114</sup> *Id.*

<sup>115</sup> See H.R. REP. NO. 114-529, at 198 (2016).

development of trade secret law, states have different conceptions of trade secrets.<sup>116</sup> Yet, many states' shared adoption of the UTSA has led to similar statutes.<sup>117</sup>

The DTSA borrowed heavily from the UTSA and expanded the protection of trade secrets by creating, for the first time, a federal private right of action for the "misappropriation" and "threatened misappropriation" of a trade secret.<sup>118</sup> While the DTSA aspired to create a uniform standard of trade secret protection,<sup>119</sup> federal courts interpret the DTSA coextensively with the jurisdiction's state-level trade secret law.<sup>120</sup> One reason for such treatment is that both the DTSA and state statutes borrow from the USTA, and the DTSA has a provision explicitly noting that it does not preempt state law.<sup>121</sup> Thus, state trade secret law often informs courts' understanding of the DTSA, and plaintiffs can bring claims under both the DTSA and state law in the same action.<sup>122</sup>

There are three forms of misappropriation at issue in this Comment, all of which are violations of the DTSA: acquisition of a trade secret through a breach of a duty to maintain secrecy, acquisition through espionage, and "threatened" misappropriation, which is typically thought to occur where a fact finder believes someone intends to misappropriate a trade secret. It will become clear in Part III that these statutory violations may not necessarily entail cognizable factual injuries. Insofar as these violations are not cognizable injuries-in-fact, many federal courts—by failing to closely scrutinize whether plaintiffs are

---

<sup>116</sup> *Id.*

<sup>117</sup> Compare ALA. CODE § 8-27-3 (2020) (adopting a version of the UTSA but requiring misuse or disclosure for liability to attach) with 6 DEL. CODE ANN. §§ 2001-2009 (attaching liability to improper acquisition, use, and disclosure). New York did not adopt a version of the UTSA and does not have a civil trade secret statute. Its common law requires use or disclosure for liability. See, e.g., *Paz Sys., Inc. v. Dakota Grp. Corp.*, 514 F. Supp. 2d 402, 407 (E.D.N.Y. 2007).

<sup>118</sup> 18 U.S.C. § 1839(5); see *Houser*, 569 F. Supp. 3d at 224 (providing history on the DTSA).

<sup>119</sup> *Houser*, 569 F. Supp. 3d at 224.

<sup>120</sup> See *id.* ("Interpreting the DTSA poses unique problems because there is relatively little guidance and existing cases may have inadvertently adopted a state's unique approach to trade secrets for the DTSA.")

<sup>121</sup> 18 U.S.C. § 1836(f) (noting that the amendments should not be construed to "preempt any other provision of law").

<sup>122</sup> See, e.g., *Complete Logistical Servs., LLC v. Rulh*, 350 F. Supp. 3d 512, 518 (E.D. La. 2018) (quoting *Source Prod. & Equip. Co. v. Schehr*, 2017 WL 3721543, at \*2 (E.D. La. Aug. 29, 2017)) ("[E]xisting state law on trade secrets informs the Court's application of the DTSA.")

alleging more than a bare violation of the DTSA—are abdicating their obligation to assure themselves of Article III standing at the outset of litigation.<sup>123</sup>

## B. Improper Means of Acquisition Is a Form of Misappropriation

While misappropriation under the DTSA includes the use and disclosure of trade secrets,<sup>124</sup> the statute permits an injunction against employees for a type of misappropriation commonly referred to as “improper acquisition.”<sup>125</sup> Improper acquisition is, to some extent, reminiscent of data theft: it involves the acquisition of a trade secret—intangible information—through “improper means.” While “acquisition” is not defined by the DTSA, it has been interpreted by courts as taking, downloading, copying, or memorizing a trade secret.<sup>126</sup> “Improper means” is defined in the DTSA to include both (1) a “breach or inducement of a duty to maintain secrecy” and (2) “espionage.”<sup>127</sup> The two variants are explored below.

### 1. Breach of a duty to maintain secrecy.

Courts recognize that a duty to maintain secrecy can flow from the employer-employee relationship.<sup>128</sup> In cases alleging trade secret misappropriation against current or former employees, courts sometimes interpret a breach of secrecy to be mere activity involving trade secrets beyond what is typical of an employee in their position.<sup>129</sup> To ground a broad view of employees’ duty to maintain secrecy, courts often point to standardized employment agreements, confidentiality

---

<sup>123</sup> See *Friends of the Earth*, 528 U.S. at 180–81.

<sup>124</sup> 18 U.S.C. § 1839(5).

<sup>125</sup> See 18 U.S.C. § 1839(6); see also, e.g., *Oakwood Lab’ys LLC v. Thanoo*, 999 F.3d 892, 905 (3d Cir. 2021).

<sup>126</sup> See, e.g., *RKI, Inc. v. Grimes*, 177 F. Supp. 2d 859, 875 (N.D. Ill. 2001).

<sup>127</sup> See 18 U.S.C. § 1839(6).

<sup>128</sup> See 18 U.S.C. § 1839(5); 1 ROGER M. MILGRIM, *supra* note 28, at § 5.01[1] (“The great majority of reported trade secret cases arise in the context of the employer-employee relationship.”).

<sup>129</sup> See, e.g., *Molon Motor & Coil Corp. v. Nidec Motor Corp.*, 2017 WL 1954531, at \*5 (N.D. Ill. May 11, 2017) (finding improper acquisition where an employee downloaded protected information onto a thumb drive and “use of the thumb drive was not part of the normal course” of business).

agreements, or internal policies signed by employees.<sup>130</sup> But courts also find that employees have a “duty to maintain secrecy” without such formal agreements, so long as there is evidence of a past or present employment relationship or a mutual understanding that the alleged trade secrets would be kept secure.<sup>131</sup>

Thus, a duty to maintain secrecy may be described as part of an implied contract between employer and employee or ex-employee,<sup>132</sup> and virtually any employee who acquires a trade secret outside of the course of normal business activities could be found by a court to have breached a duty to maintain secrecy. Because trade secret acquisition by an actor who breaches a duty to maintain secrecy is itself actionable under the DTSA, federal courts have readily adjudicated cases alleging little more than bare allegations of improper acquisition.<sup>133</sup>

An oft-litigated version of improper acquisition—which promises to become increasingly common in the “work from home” age—occurs where an employer alleges that an employee failed to return documents and emails after departing under suspicious circumstances. For instance, in *API Americas Inc. v. Miller*,<sup>134</sup> the court found an employee liable under the DTSA after the employee “transmitted multiple emails containing Plaintiff’s trade secrets from his business email account to his personal account, without Plaintiff’s permission.”<sup>135</sup>

## 2. Espionage.

“[E]spionage” is another type of improper acquisition recognized by the Act.<sup>136</sup> Espionage is typically understood as “surreptitious surveillance for the purpose of discovering a businessman’s secrets.”<sup>137</sup> While espionage may involve the

---

<sup>130</sup> See, e.g., *United States v. Olgado*, 2022 WL 2356996, at \*7 (N.D. Cal. June 30, 2022) (finding an employee breached a duty to maintain secrecy because they “violated [ ] internal policies” by downloading trade secrets onto a storage device).

<sup>131</sup> See JAGER, *supra* note 17, at § 3:31.

<sup>132</sup> See MILGRIM, *supra* note 28, at § 5.02.

<sup>133</sup> See, e.g., *MMR Constructors, Inc. v. JB Grp. of LA, LLC*, 2022 WL 1223919, at \*2 (M.D. La. Apr. 26, 2022) (granting injunctive relief after a plaintiff alleged that their former employee downloaded “hundreds of files believed to contain [the company’s] trade secrets and confidential business information” in the month before resigning).

<sup>134</sup> 380 F. Supp. 3d 1141, 1147 (D. Kan. 2019).

<sup>135</sup> *Id.* at 1149.

<sup>136</sup> 18 U.S.C. § 1839(6).

<sup>137</sup> T.K. Bell, Comment, *Industrial Espionage: Piracy of Secret Scientific and Technical Information*, 14 U.C.L.A. L. REV. 911, 911 (1967).



acquisition of trade secrets through criminal conduct, such as trespass, someone can improperly acquire a trade secret without committing an independent wrong.

*E.I. DuPont deNemours & Co. v. Christopher*,<sup>138</sup> for instance, features one oft-cited, pre-DTSA example of “espionage” without an independent wrong. The Fifth Circuit in *Christopher* recognized a cause of action against a non-employee who took an aerial photograph of a secret factory.<sup>139</sup> The photographer was found not to have trespassed and was not in privity with the company from which he misappropriated the trade secret. Yet, he was found liable for improper acquisition because his activity fell “below the generally accepted standards of commercial morality.”<sup>140</sup>

There is considerable judicial discretion in determining what constitutes activities that fall below such standards, but *Christopher* remains an exemplar for trade secret cases involving both espionage and improper acquisition by an employee.<sup>141</sup> This is because, at bottom, trade secret law is about policing commercial morality. Accordingly, courts look to *Christopher* to deem improper any acquisition of trade secrets that, like the photographer’s activity, falls below “generally accepted standards.”<sup>142</sup>

### C. Threatened Misappropriation and Inevitable Disclosure

While improper acquisition is a form of actual misappropriation, the DTSA also permits a court to grant an injunction “to prevent any . . . threatened misappropriation.”<sup>143</sup> Threatened misappropriation differs from improper acquisition because it focuses on whether the defendant seems *likely* to wrongly use or disclose a trade secret and need not involve actual misappropriation.

#### 1. “Threatened misappropriation” and its unclear

---

<sup>138</sup> 431 F.2d 1012 (5th Cir. 1970).

<sup>139</sup> *Id.* at 1015.

<sup>140</sup> *Id.* at 1016.

<sup>141</sup> See *Compulife Software Inc. v. Newman*, 959 F.3d 1288, 1311 (11th Cir. 2020).

<sup>142</sup> See, e.g., *HIRECounsel*, 2021 WL 5998365, at \*6 (referencing *Christopher* for the proposition that “‘improper means’ has been defined as those means that ‘fall below the generally accepted standards of commercial morality and reasonable conduct’” (quoting *Christopher*, 431 F.2d at 1016)).

<sup>143</sup> See 18 U.S.C. § 1836(b)(3)(A)(i); see also, e.g., *Fres-co Sys. USA, Inc. v. Hawkins*, 690 F. App’x 72, 76 (3d Cir. 2017).

boundaries.

Threatened misappropriation lacks a clear doctrine. Courts sometimes find threatened misappropriation where it seems that a bad actor intends to use or disclose a trade secret at some point in the future.<sup>144</sup> Evidence of an employee's bad-faith intent or motive is the most common means through which plaintiffs demonstrate threatened misappropriation.<sup>145</sup> In some cases, however, a mere lack of care or lack of assurance by an employee could be enough to constitute threatened misappropriation.<sup>146</sup>

For instance, in *Khazai v. Watlow Electric Manufacturing Co.*,<sup>147</sup> the court found threatened misappropriation adequately pled where an ex-employee refused to sign documents that would confirm that his former employer owned certain trade secrets.<sup>148</sup> The ex-employee's activity was deemed by the court as creating a "sufficient probability that[ ] wrongful disclosure by plaintiff of defendants' trade secrets [would] occur."<sup>149</sup>

## 2. Inevitable disclosure as a form of threatened misappropriation under the DTSA.

The inevitable disclosure doctrine is a common law doctrine that arises where an employer alleges that a departing employee's industry knowledge cannot be separated from the employer's trade secrets such that disclosure or use of the employer's trade secrets is "inevitable" in the course of future employment.<sup>150</sup> Inevitable disclosure is understood by some jurisdictions as a sort of "threatened misappropriation."<sup>151</sup> And because threatened misappropriation is explicitly listed as a cause of action in the DTSA, some federal courts have understood

---

<sup>144</sup> See, e.g., *Gene Codes Corp. v. Thomson*, 2011 WL 611957, at \*5 (E.D. Mich. Feb. 11, 2011) ("To establish threatened misappropriation, a party must specifically identify the trade secret likely to be misappropriated and must convince the court of the former employee's 'duplicitous' by proffering evidence indicating a significant lack of candor or willingness to misuse trade secrets.").

<sup>145</sup> See, e.g., *Edward D. Jones & Co., L.P. v. Kerr*, 415 F. Supp. 3d 861, 867 n.4 (S.D. Ind. 2019).

<sup>146</sup> See *Jazz Pharms., Inc. v. Synchrony Grp., LLC*, 343 F. Supp. 3d 434, 443 (E.D. Pa. 2018).

<sup>147</sup> 201 F. Supp. 2d 967, 968 (E.D. Mo. 2001).

<sup>148</sup> *Id.* at 974.

<sup>149</sup> *Id.*

<sup>150</sup> See *PepsiCo, Inc. v. Redmond*, 54 F.3d 1262, 1268 (7th Cir. 1995).

<sup>151</sup> See, e.g., *Barilla Am., Inc. v. Wright*, 2002 WL 31165069, at \*8–9 (S.D. Iowa July 5, 2002) (finding that inevitable disclosure is a variation of threatened disclosure).

the DTSA to permit a cause of action under the inevitable disclosure doctrine.<sup>152</sup>

However, the DTSA contains language that ostensibly forecloses use of the inevitable disclosure doctrine: it does not permit injunctive relief that “prevent[s] a person from entering into an employment relationship” based “merely on the information the person knows.”<sup>153</sup> Despite such language, the inevitable disclosure doctrine has been accepted under the DTSA in many jurisdictions.<sup>154</sup> The doctrine is sometimes accepted under the DTSA because—as noted above—federal courts interpret the DTSA coextensively with the jurisdiction’s state-level trade secret law, and many states permit the inevitable disclosure doctrine.

Inevitable disclosure is theoretically different from threatened misappropriation insofar as a defendant’s intentions do not matter if disclosure is truly “inevitable.” Notwithstanding this theoretical difference, many courts undertake mixed analysis, analyzing a defendant’s intentions while determining the applicability of the inevitable disclosure doctrine.<sup>155</sup> In other words, some courts look for evidence of bad faith in both inevitable disclosure and threatened misappropriation cases.<sup>156</sup>

### III. IMPROPER ACQUISITION AND THREATENED MISAPPROPRIATION: COGNIZABLE HARMS?

---

<sup>152</sup> See, e.g., *Gen. Elec. Co. v. Uptake Techs., Inc.*, 394 F. Supp. 3d 815, 832–34 (N.D. Ill. 2019).

<sup>153</sup> 18 U.S.C. § 1836(b)(3)(A)(i)(I); see *Defend Trade Secrets Act of 2016*, S. REP. NO. 114-220, 114th Cong., 2d Sess., 12 n.12 (2016) (“[L]imitations on injunctive relief were included to protect employee mobility.”); see also M. Claire Flowers, Comment, *Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016*, 75 WASH. & LEE L. REV. 2207, 2230–31 (2018) (arguing that the DTSA aimed to foreclose the inevitable disclosure doctrine).

<sup>154</sup> See, e.g., *Packaging Corp. of Am., Inc. v. Croner*, 419 F. Supp. 3d 1059, 1069 (N.D. Ill. 2020); *Phoseon Tech., Inc. v. Heathcote*, 2019 WL 7282497, at \*11 (D. Or. Dec. 27, 2019) (“Seventeen states appear to have adopted the inevitable disclosure doctrine.”).

<sup>155</sup> See, e.g., *Triumph Packaging Grp. v. Ward*, 834 F. Supp. 2d 796, 813 (N.D. Ill. 2011).

<sup>156</sup> *Sonoco Prods. Co. v. Johnson*, 2000 WL 35501037, at \*72 (D. Colo. Jan. 31, 2000) (finding the defendant might misappropriate his former employer’s trade secrets because the defendant was untrustworthy and holding that, “[u]nder these circumstances, the Court may issue a permanent injunction to prevent inevitable disclosure of the trade secrets”).

The following Parts will explain how the violations described above should be analyzed under the standing analysis laid out in Part I. If a trade secret “falls” into the wrong hands—or there is a threat of misappropriation—“does it make a sound?”<sup>157</sup> That is, does improper acquisition or threat necessarily inflict injury? This Part argues that improper acquisition and threatened misappropriation may not be per se injuries-in-fact because they sometimes fail to constitute either concrete or imminent injuries. It is crucial to determine whether these statutory violations amount to concrete or imminent injuries because, if they do not, then it is striking that courts are not conducting standing analysis in these cases—as they do in the data breach context<sup>158</sup>—to ensure that they have the constitutional power to hear them. Moreover, and similarly, if these DTSA violations are not per se injuries-in-fact, then plaintiffs should be required in their complaints to explain precisely how they have been harmed, instead of merely outlining that their trade secrets have been taken or threatened.

As explained in Part II, both improper acquisition and threatened misappropriation are violations of the DTSA. But merely asserting a violation of the DTSA without connecting the violation to any concrete injury, impending harm, or substantial risk of harm is—at first blush—not enough to meet modern standing requirements under *TransUnion* and *Spokeo*. Indeed, both cases underscored that the mere fact that a defendant has run afoul of a statute is insufficient to confer standing. They referred to statutory violations that lack real-world injury as “bare procedural violations”<sup>159</sup> that are “divorced from any concrete harm” such that they do not inflict actual injury.<sup>160</sup> This Part will make clear that improper acquisition and threatened misappropriation may be analogous to “bare procedural violations”; they run afoul of the DTSA in ways that *could*, but need not, inflict concrete and imminent damage.

#### A. Improper Acquisition and Threatened Misappropriation:

---

<sup>157</sup> See *Owner-Operator Indep. Drivers Assn., Inc. v. U.S. Dept. of Transp.*, 879 F.3d 339, 344 (D.C. Cir. 2018) (“[I]f inaccurate information falls into a government database, does it make a sound?”).

<sup>158</sup> See *supra* Part I.B.

<sup>159</sup> *Spokeo*, 578 U.S. at 342.

<sup>160</sup> *Id.*

## Per Se Injuries?

Of course, one could argue that improper acquisition and threatened misappropriation are inherently injurious. Indeed, many courts have ostensibly concluded that improper acquisition and threatened misappropriation are cognizable harms, without conducting in-depth standing analysis, for this reason.<sup>161</sup> The Third Circuit, for example, recently declared that “[b]y statutory definition, trade secret misappropriation *is* harm.”<sup>162</sup> However, it is difficult to reconcile the Third Circuit’s pronouncement with *TransUnion* and the separation of powers concerns underlying the decision. Although Congress’s judgment on what constitutes a concrete and actual harm is instructive,<sup>163</sup> it is decidedly not dispositive. Standing requirements would be hollow if Congress could simply define injuries within statutes to evade the demands of Article III.<sup>164</sup>

If, indeed, factual concrete injuries occur at the moment of improper acquisition or threatened misappropriation, it is difficult to put the harm into words. These trade secret harms might be best described as breaches of trust or transgressions of commercial morality.<sup>165</sup> The resultant injuries—if they are injuries—are, like data breach and other privacy harms, ephemeral. Yet data breach and privacy harms, but not trade secret harms, have been closely scrutinized and frequently dispensed by courts as insufficient for standing.<sup>166</sup>

It can be similarly difficult to see how improper acquisition inflicts real-world harm, at least until a trade secret is used by the person or entity that misappropriates. While trade secret owners might argue that misappropriation has inherent economic harms, instances of threatened misappropriation or improper acquisition need not make a trade secret more difficult for a

---

<sup>161</sup> See *supra* text accompanying note 18.

<sup>162</sup> *Oakwood Lab’s LLC v. Thanoo*, 999 F.3d 892, 905 (3d Cir. 2021) (emphasis in original); see also *Monster Energy Co. v. Vital Pharms., Inc.*, 2019 WL 2619666, at \*10 (C.D. Cal. May 20, 2019) (finding “[a]llegations that Monster owned the stolen or misappropriated trade secrets and that it derived economic value from the lack of disclosure of those trade secrets prior to their misappropriation are sufficient to allege concrete injury for these claims”).

<sup>163</sup> *Spokeo*, 578 U.S. at 340.

<sup>164</sup> See *TransUnion*, 141 S. Ct. at 2207 (“A regime where Congress could freely authorize *unharm*ed plaintiffs to sue defendants who violate federal law not only would violate Article III but also would infringe on the Executive Branch’s Article II authority.” (emphasis in original)).

<sup>165</sup> See *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 481 (1974).

<sup>166</sup> See *supra* text accompanying note 11.

company to derive value from. An improperly acquired customer list, for example, can often be used by its owner in the same way it was used before the improper acquisition. By its nature, information can be held by many people at one time.<sup>167</sup> That is, improper acquisition or threat alone need not render the trade secret unavailable for use. That improper acquisition is intuitively not harmful until use or disclosure may be why—until the last several years—many states refused to recognize liability for the mere improper acquisition of a trade secret.<sup>168</sup>

Threatened misappropriation is, by its very nature, an example of risk-based harm. The reason the DTSA permits equitable relief in these circumstances is to prevent misappropriation that *might* occur. Even assuming that misappropriation itself is a per se concrete injury, the doctrine demands that plaintiffs show “certainly impending”—not merely “threatened”—harm for standing.<sup>169</sup> An “objectively reasonable likelihood” of harm will not suffice to meet the “certainly impending” harm requirement.<sup>170</sup>

Yet some courts appear to ignore *Clapper*’s demand for impending harm in threatened misappropriation cases, electing instead to ask whether misappropriation *might* or *could* happen in the future.<sup>171</sup> In one case, for example, a federal court entered a preliminary injunction against an employee who was alleged to have uploaded “some portion” of his employer’s confidential information onto a personal hard drive.<sup>172</sup> There was evidence demonstrating the defendant’s “propensity for making

---

<sup>167</sup> Also consider cases in which an employee knows that they have taken a trade secret but does not understand the trade secret they have taken. In such cases, it seems far less likely that the trade secret will be misused because the employee might not know how to misuse it. Yet, the case law indicates that their acquisition of the trade secret might be a per se injury sufficient for standing.

<sup>168</sup> See, e.g., *Iconics, Inc. v. Massaro*, 266 F. Supp. 3d 449, 452 (D. Mass. 2017) (summarizing, in a pre-UTSA case, Massachusetts trade secret law and explaining that misappropriation requires plaintiffs to show use or disclosure).

<sup>169</sup> See *Clapper*, 568 U.S. at 404; see also *Greenstein v. Noblr Reciprocal Exch.*, 585 F. Supp. 3d 1220, 1228 (N.D. Cal. 2022) (finding no standing because there was no evidence of a “credible risk of imminent harm”).

<sup>170</sup> *Clapper*, 568 U.S. at 407.

<sup>171</sup> See, e.g., *Power Integrations, Inc. v. De Lara*, 2020 WL 1467406, at \*20 (S.D. Cal. Mar. 26, 2020) (stating that a claim of threatened misappropriation could be pled where a former employee was alleged to have lied about his employment with a competitor while in possession of plaintiff’s confidential information without discussing standing).

<sup>172</sup> *Engility Corp. v. Daniels*, 2016 WL 7034976, at \*11 (D. Colo. Dec. 2, 2016).

surreptitious copies of the relevant data.”<sup>173</sup> A case could be made that harm was certainly impending because the ex-employee is untrustworthy. Nevertheless, it is surprising that the court did not conduct standing analysis to find a sufficiently impending harm because “deciding whether a given risk of harm meets the materiality threshold is an independent responsibility of federal courts.”<sup>174</sup> Since the “improper means” standard indicates that “trade secret law is potentially capable of reaching any conduct that strikes a judge as unethical,”<sup>175</sup> it is important that courts ensure the existence of impending harm before conferring standing. As in the data breach cases, courts might look to focus on how much effort the trade secret misappropriator expended as a proxy for whether harm is impending.<sup>176</sup> In any case, it is not obvious that an employee who wrongly retains a customer list or merely displays a lack of candor has inflicted real or impending harm on their former employer.

An absence of impending harm analysis is also noticeable in applications of the inevitable disclosure doctrine—at least where courts do not require truly “inevitable” disclosure to impart liability on departing employees.<sup>177</sup> A lack of impending harm analysis allows companies to benefit from judgments by federal courts that impose injunctions on ex-employees, without requiring those same companies to meet the requirements for entry into court: a plausible allegation of an injury-in-fact.

#### B. Mitigation Costs as Injuries Sufficient for Standing

To be sure, trade secrets derive their value from secrecy, and both improper acquisition and threatened misappropriation might marginally decrease their secrecy or put their secrecy at risk. And after each instance of improper acquisition or threat, the benefit to the trade secret holder might remain the same as it

---

<sup>173</sup> *Id.*; see also *Prot. Techs., Inc. v. Ribler*, 2017 WL 923912, at \*2 (D. Nev. Mar. 8, 2017) (omitting standing analysis and issuing a TRO based on threatened misappropriation where an employee downloaded trade secret information to a private drive and emailed the information from his company email account to a personal email). *But see Teradyne v. Clear Commc’ns Corp.*, 707 F. Supp. 353, 357 (N.D. Ill. 1989) (holding, without analyzing standing, that under Illinois’s trade secret statute, plaintiffs “do not state a claim of threatened misappropriation. All 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.”).

<sup>174</sup> *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917, 933 (11th Cir. 2020).

<sup>175</sup> *Bone*, *supra* note 98, at 250.

<sup>176</sup> See, e.g., *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 155–57 (3d Cir. 2022).

<sup>177</sup> See *supra* Part II.B.

did before the improper acquisition or threat, but the cost of keeping the trade secret a secret could increase. After an employee improperly acquires or threatens a trade secret, the trade secret owner might be compelled to take potentially costly measures to prevent misuse or disclosure.

But insofar as the trade secret holder does not allege any facts that make misuse or disclosure seem imminent, as in the data breach cases, their claims for mitigation costs could amount to “manufacture[d] standing” under *Clapper*.<sup>178</sup> Further, while trade secrets do derive value from secrecy, more precisely, they derive value from *general* secrecy; absolute secrecy is not required for a trade secret to maintain its status.<sup>179</sup> Moreover, at least in the case of improper acquisition or threatened misappropriation by an employee—rather than a competitor or third party—the employee might have already been exposed to the trade secret. That is, an act of misappropriation by an employee who has already been exposed to a trade secret does not obviously make a trade secret less secret.

Of course, in some circumstances, a company whose trade secret has been improperly acquired or threatened could be forced to take steps to ensure the trade secret is not disseminated or used in a way that *will* harm the company or extinguish the trade secret’s status as a trade secret. In such a scenario, the company should be required to plead facts to show that it actually took such prophylactic steps, and that subsequent dissemination, misuse, or other financial harm was impending. Such a pleading requirement might be onerous, but it is what the modern standing doctrine requires.<sup>180</sup>

### C. Decreased Secrecy as Cognizable Harm

Even assuming *arguendo* that certain cases of improper acquisition or threatened misappropriation *do* make the trade secret at issue marginally less secret, it is difficult to see the

---

<sup>178</sup> *Clapper*, 568 U.S. at 416. Objections to this point are acknowledged, *infra*, in Part IV.

<sup>179</sup> See UNIF. TRADE SECRETS ACT § 1(4)(ii) (UNIF. L. COMM’N 1985). Definitionally, trade secrets “derive[] independent economic value . . . from not being *generally* known.” 18 U.S.C.A. § 1839(3) (emphasis added).

<sup>180</sup> See *TransUnion*, 141 S. Ct. at 2207 (rejecting the argument that the concrete-harm requirement should be “ditched altogether” because it is at times inconvenient, inefficient, and difficult to apply).



cognizable harm in marginally decreased secrecy.<sup>181</sup> This is especially true because modern courts have significantly expanded the boundaries of what is considered a trade secret, in part, by loosening the need for a trade secret to derive “actual or potential” value from secrecy.<sup>182</sup> Since modern courts sometimes do not thoroughly scrutinize whether trade secrets actually derive value from secrecy,<sup>183</sup> one should wonder whether a single instance of improper acquisition or threat can actually be said to devalue a trade secret. Courts readily adjudicate cases in which trade secrets have been abandoned by the company and subsequently misappropriated, for example.<sup>184</sup> In such cases, it is difficult to believe that injury resulting from mere improper acquisition or threat is felt by the company in any “real” sense.

While a company might respond that individual instances of acquisition or threat would make a trade secret command less in a hypothetical sale, such an argument is likely too speculative to support standing. The company’s harm may fail to meet *Clapper*’s “certainly impending” injury standard because it would necessarily lack both the identification of a potential buyer and an explanation of precisely how the misappropriation “in any way

---

<sup>181</sup> Exposing more employees to a given trade secret, or licensing a trade secret to another company, would also seem to marginally decrease secrecy, at least insofar as such actions increase the risk that a trade secret will be misused or disclosed. But no one could seriously argue that there is cognizable harm—in and of itself—from either exposing employees to a trade secret or licensing a trade secret.

<sup>182</sup> See, e.g., Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 27–41 (2021) (collecting cases and demonstrating that some modern trade secret cases are adjudicated without any showing that the trade secrets at issue actually derive actual or potential value from secrecy); see also Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERK. TECH. L.J. 829, 906 (2017) (highlighting that the “‘independent economic value’ requirement . . . has not been applied satisfactorily in many cases”); *Earthbound Corp. v. MiTek USA, Inc.*, 2016 WL 4418013, at \*10 (W.D. Wash. Aug. 19, 2016) (“The EEA defines trade secrets similarly to but even more broadly than the UTSA.”).

<sup>183</sup> See *Mallet & Co. Inc. v. Lacayo*, 16 F.4th 364, 385 (3d Cir. 2021) (explaining that plaintiffs need “to demonstrate . . . a ‘significantly better than *negligible*’ chance” of the existence of a trade secret to plead misappropriation) (emphasis added) (citing *Reilly v. City of Harrisburg*, 858 F.3d 173, 179 (3d Cir. 2017)); see also *Bar Method Franchisor LLC v. Henderhiser LLC*, 580 F. Supp. 3d 979, 996 (D. Colo. 2022) (finding that exercise training methods are likely trade secrets and holding that plaintiff’s methods may be protected even though customers routinely observed the training methods) (citing *Core Progression Franchise LLC v. O’Hare*, 2021 WL 1222768, at \*9 (D. Colo. 2021)).

<sup>184</sup> See Hrdy & Lemley, *supra* note 182, at 25 (citing cases and explaining that modern trade secret law, including the DTSA, “deliberately eliminated any requirement that a trade secret be used in one’s business”).

diminished the value” of its trade secret.<sup>185</sup> In any case, assuming a trade secret holder *could* demonstrate a concrete injury through a loss of hypothetical resale value as a result of improper acquisition or threat, the trade secret holder should have to plausibly allege such an injury in their complaint.<sup>186</sup> It could be difficult for some plaintiffs to plausibly make such an allegation because a trade secret from which a company derives value, or subjectively believes has “potential” value, is not necessarily valuable to others in the marketplace.<sup>187</sup> It may also be difficult for some to plausibly allege a loss of value because, in practice, the fact that a legitimate trade secret exists can be difficult to determine at the pleading stage.

Indeed, the thumb drive taken by the employee in the introductory hypothetical is like the defamatory letter described in *TransUnion*.<sup>188</sup> The thumb drive, like the letter, is an unrealized risk that has not yet ripened into a real-world injury. The thumb drive—like any improperly acquired or threatened trade secret—has the *potential* to cause the company harm through its use or disclosure. But so does personally identifying information in the wrong hands. And, again, many courts have found that plaintiffs alleging their data has been merely acquired by a bad actor—rather than misused—lack standing.<sup>189</sup>

While it is certainly distressing for a company to lose security of its trade secret, it is also distressing for a consumer or employee to lose security of personally identifying information. Many courts have been unmoved by emotional injuries in both the data breach context<sup>190</sup> and beyond.<sup>191</sup> Any loss

---

<sup>185</sup> See *Pena v. British Airways, PLC (UK)*, 2020 WL 3989055 at \*3 (E.D.N.Y. Mar. 30, 2020) (finding no concrete injury based on alleged diminution in value where plaintiff “ha[d] not alleged that he was offered or forewent any opportunity to profit from the sale of his personal information”).

<sup>186</sup> *Muransky*, 979 F.3d at 924–25 (“We will not ‘imagine or piece together an injury sufficient to give [a] plaintiff standing when it has demonstrated none.’” (quoting *Micosukee Tribe of Indians of Fla. v. Fla. State Athletic Comm’n*, 226 F.3d 1226, 1229 (11th Cir. 2000))).

<sup>187</sup> See *Hrdy & Lemley*, *supra* note 182, at 38 (collecting cases to show that, in practice, federal courts do not require plaintiffs to show that their trade secrets have actual or potential value: “so long as someone, somewhere, might ‘potentially’ think the secret is worth paying for, it . . . satisf[ies] the independent economic value requirement”).

<sup>188</sup> See *supra* Part I.A.

<sup>189</sup> See, e.g., *Reilly*, 664 F.3d at 45.

<sup>190</sup> *Id.* at 44.

<sup>191</sup> See *Hein v. Freedom from Religion Found., Inc.*, 551 U.S. 587, 619 (2007) (Scalia, J., concurring) (explaining that “mental displeasure” is not sufficient to form the basis of an injury-in-fact in at least some circumstances).

of peace of mind resulting from the above-described trade secret violations does not seem cognizable.

#### D. Comparison to Data Breach Harms

As in the data breach cases, it often seems as if decisionmakers downstream would need to take certain actions for an improperly acquired or threatened trade secret—including the thumb drive in the introductory hypothetical—to harm the entity that lost its trade secret.<sup>192</sup> Following the thumb drive example, the ex-employee would need to take the customer list on the thumb drive to a competitor, or use it herself, and the ex-employee or the competitor would need to use the list in a way that harms her former company’s business or ability to use its client list.<sup>193</sup> This might not be so probable, at least unless there is a credible chance that clients on the list will actually take their business elsewhere. Thus, without the inclusion of certain facts—such as whether the clients on a customer list could conceivably bring their business to another company, whether there is a ready market for the customer list, or whether the acquirer of the list appears likely to imminently disclose its contents—an allegation of improper acquisition or threatened misappropriation tends to resemble the risk-based theories of harm rejected by the Court in *Clapper* and *TransUnion*. Said another way, current trade secret doctrine seems to underappreciate its own reliance on risk-based harm. And the account described above illuminates some separation between what courts tend to see as real-world harms and certain trade secret violations.

The state of the world post-improper acquisition or threat is undoubtedly worse for a trade secret owner than it was prior to the acquisition or threat. Surely an owner would rather not have had its trade secret threatened or improperly acquired, but so too would a consumer rather not lose private data to a hacker. Being

---

<sup>192</sup> *Clapper*, 568 U.S. at 410 (rejecting standing for a theory of harm that relies on an “attenuated chain of possibilities”).

<sup>193</sup> *See Reilly*, 664 F.3d at 43 (declining to find standing because the court could not describe the alleged injury “without beginning [its] explanation with the word ‘if’: *if* the hacker read, copied, and understood the hacked information, and *if* the hacker attempts to use the information, and *if* he does so successfully, only then will Appellants have suffered an injury” (emphasis in original)).

put in a marginally worse position is simply not enough to meet the demands of Article III.<sup>194</sup>

Insofar as certain violations of the DTSA present, at best, borderline cases of standing, it is crucial that courts fulfill their mandate to scrutinize whether the plaintiff has plausibly alleged an injury-in-fact. Without such scrutiny, DTSA cases that courts do not have the constitutional power to hear will slip through the cracks.

#### IV. TWO OBJECTIONS

Part III suggested that there is some intuitive attraction to the idea that certain violations of the DTSA need not inflict real-world, factual damage on certain plaintiffs. This Section moves forward to suggest, and respond to, objections that plaintiffs, courts, and commentators alike may have to the above discussion.

##### A. Reasonable Measures and Standing

At this point, critics might have two responses to the above arguments, both meritorious but ultimately unavailing. First, one might argue that claims for mitigation costs taken to protect a trade secret following any act of misappropriation would *not* amount to “manufacture[d] standing”<sup>195</sup> under *Clapper* because maintaining a trade secret requires a holder to take “reasonable measures to keep [the] information secret.”<sup>196</sup> Thus, the argument would continue, a trade secret holder who fails to mitigate risk by, for example, initiating litigation against one who wrongly acquires their trade secret should lose the trade secret status of their information. Perhaps a trade secret holder who fails to make a costly response to misappropriation has necessarily failed to undertake “reasonable measures.” And it might follow that, since the loss of a trade secret’s trade secret status is a concrete harm, mitigation costs like the costs of bringing a lawsuit should suffice to confer standing.

This argument has appeal, but it probably fails in most cases because an owner need not bring a lawsuit nor take costly mitigation measures after misappropriation occurs to maintain a

---

<sup>194</sup> *Thorne v. Pep Boys Manny Moe & Jack Inc.*, 980 F.3d 879, 894 (3d Cir. 2020) (explaining that the creation of a “new non-zero risk” is too speculative to support standing (citing *Thole v. U.S. Bank N.A.*, 140 S. Ct. 1615, 1621 (2020))).

<sup>195</sup> *Clapper*, 568 U.S. at 416.

<sup>196</sup> *See* 18 U.S.C. § 1839(3)(A).

trade secret's status. The reasonable secrecy precautions required by courts have not been so demanding.<sup>197</sup> Indeed, the case law reveals that in cases involving employee misappropriation, reasonable efforts typically hinge on whether an employer “adequately informed its employees of the identity of its claimed trade secrets” before misappropriation occurred.<sup>198</sup> One empirical review of federal trade secret cases finds that confidentiality agreements with employees in place at the time of misappropriation are key to demonstrating that a trade secret holder took “reasonable measures.”<sup>199</sup> Other commentators find that in many cases, valid nondisclosure agreements, with “very little else,” sufficiently support a conclusion of “reasonable efforts.”<sup>200</sup>

The justification for a relatively lenient rule is clear. “If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention.”<sup>201</sup> A court would be asking a plaintiff to do too much if it was to cite the owner's failure to bring a lawsuit or take mitigation efforts following a past instance of misappropriation as reason not to view something as a trade secret. Therefore, the mitigation costs argument likely fails.

This argument would also be an odd place for a plaintiff to hang their hat for standing because whether a plaintiff adequately protected their trade secret is a question of fact that courts often decline to resolve at the pleading stage.<sup>202</sup> It is thus

---

<sup>197</sup> See, e.g., *Electro-Craft Corp. v. Controlled Motion, Inc.*, 332 N.W.2d 890, 901 (Minn. 1983) (explaining that trade secret holders must make “some effort to keep the information secret” (emphasis added)).

<sup>198</sup> ELIZABETH A. ROWE & SHARON K. SANDEEN, *CASES AND MATERIALS ON TRADE SECRET LAW* 170 (2012).

<sup>199</sup> Almeling et al., *supra* note 21, at 321; see also Alan J. Tracey, *The Contract in the Trade Secret Ballroom—A Forgotten Dance Partner?*, 16 TEX. INTELL. PROP. L.J. 47, 63 (2007) (“One of the most commonly used and well-recognized approaches to safeguarding the access of trade secret information is a confidentiality agreement.”).

<sup>200</sup> James H.A. Pooley, Mark A. Lemley & Peter J. Toren, *Understanding the Economic Espionage Act of 1996*, 5 TEX. INTELL. PROP. L.J. 177, 218 (1997) (citing *Surgidev Corp. v. Eye Tech., Inc.*, 828 F.2d 452, 455 (8th Cir. 1987)).

<sup>201</sup> *Rockwell Graphic Sys., Inc. v. DEV Indus., Inc.*, 925 F.2d 174, 180 (7th Cir. 1991).

<sup>202</sup> See, e.g., *Xavian Ins. Co. v. Marsh & McLennan Cos.*, 2019 WL 1620754, at \*6 (S.D.N.Y. Apr. 16, 2019). *But see* *Gov't Emps. Ins. Co. v. Nealey*, 262 F. Supp. 3d 153, 167 (E.D. Pa. 2017) (“While it may be true that courts often do not resolve this issue at the pleadings stage, this does not mean it is improper to do so in certain circumstances—or that it is never done.”).

difficult to imagine that courts would be willing or able to adjudicate whether cognizable harm results from threatening plaintiffs' *future* "reasonable measures" arguments.

It is important to acknowledge that this argument might work for a particularly valuable trade secret because the reasonable measures requirement mandates consideration of what is reasonable under the circumstances.<sup>203</sup> Perhaps failing to improve security measures—even after an act of improper acquisition that does not seem to involve impending disclosure or use—would be unreasonable to certain courts and fact finders. If a plaintiff can make the case that they were forced to take action at some economic cost because a misappropriator raised the bar of what a future fact finder was to consider "reasonable measures," then it might be enough for standing. Yet, it is difficult to believe that such a chain of inferences would be accepted in most cases.

#### B. Congressional Judgment

Second, critics might point out that, while not dispositive, Congress's judgment is instructive in determining what kinds of intangible harms are "real" enough for standing.<sup>204</sup> In enacting the DTSA, which designates improper acquisition and threatened misappropriation as clear statutory violations, Congress may have signaled its belief that these trade secret violations are inherently injurious. Courts might be persuaded to view improper acquisition and threatened misappropriation as inherently injurious because Congress seems to think they are. The question, then, is whether improper acquisition and threatened misappropriation are in the "pool" of "de facto" injuries from which Congress can choose.<sup>205</sup> The answer is unclear, and modern trade secret violations, to some degree, resemble their historic counterparts.<sup>206</sup> But, there is undoubtedly tension between this argument and the Court's statements about standing setting a "hard floor" that cannot be removed via congressional statute.<sup>207</sup>

And even assuming *arguendo* that Congress's judgment *was* dispositive despite the case law to the contrary, Congress's recognition of improper acquisition or threatened

---

<sup>203</sup> See UNIF. TRADE SECRETS ACT § 1(4) (UNIF. L. COMM'N 1985).

<sup>204</sup> See *supra* text accompanying note 57.

<sup>205</sup> See Nichol, *supra* note 59, at 203.

<sup>206</sup> See *infra* Part V.B.

<sup>207</sup> *Summers*, 555 U.S. at 497.

misappropriation as violations of the DTSA need not reflect a judgment that such activity is inherently injurious. Rather, prohibitions against improper acquisition and threatened misappropriation may be preventative. That is, these statutory violations may represent attempts to decrease the chance that actual harm—trade secret use and disclosure—will occur in the future.<sup>208</sup> Under modern standing doctrine, many courts have rejected standing for plaintiffs invoking violations of statutes that attempt to decrease individuals' risk of downstream harm.<sup>209</sup>

An alternative argument in line with the above is that Congress's elevation of improper acquisition and threatened misappropriation as injuries sufficient for standing does not warrant separation-of-powers concerns because *states* had previously provided relief for such actions under statutes modeled after the UTSA. This might provide a creative workaround, but it seems to be uncharted territory. “*Spokeo* speaks only to the judgment of the United States Congress that a harm should be cognizable before federal courts. So it is unclear what role (if any) state legislatures play in the *Spokeo* framework.”<sup>210</sup> It would be surprising if Congress could authorize unharmed plaintiffs to sue where states had also done so.

## V. THREE (POTENTIAL) PATHS TO STANDING

Part III illustrated that plaintiff-employers should be required to allege sufficient facts to demonstrate a concrete or imminent harm from improper acquisition or threatened misappropriation to prove they have standing. Beyond meeting *Clapper's* demanding “certainly impending” injury requirement,<sup>211</sup> this Part demonstrates that there are at least three convincing paths to standing in cases alleging improper acquisition or threatened misappropriation. First, a trade secret

---

<sup>208</sup> Much of the DTSA and EEA's legislative histories focus on the downstream revenue and job losses that result from wrongful trade secret use and disclosure. *See, e.g.*, Sen. Hatch Press Release, *supra* note 15 (“American businesses continue losing significant revenue and American jobs to trade secret theft.”).

<sup>209</sup> *See, e.g.*, *Kamal v. J. Crew Grp.*, 918 F.3d 102, 117 (3d Cir. 2019); *Braitberg v. Charter Commc'ns, Inc.*, 836 F.3d 925, 930 (8th Cir. 2016) (denying standing for a failure to destroy data in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e)); *see also* Elizabeth E. Beske, *Charting a Course Past Spokeo and TransUnion*, 29 GEO. MASON L. REV. 729, 775 (2021) (“The Court's standing requirements . . . constrain[] Congress to a reactive or nearly reactive approach, thereby curbing its options in responding to big societal problems.”).

<sup>210</sup> *Garland v. Orleans, PC*, 999 F.3d 432, 438 n.2 (6th Cir. 2021).

<sup>211</sup> *See Clapper*, 568 U.S. at 401.

might be a property right, the invasion of which inflicts a concrete injury and thus confers standing. Second, improper acquisition and threatened misappropriation might be concrete injuries because they have common law analogs. And third, improper acquisition and threatened misappropriation may invariably result in independent concrete injuries sufficient for standing. The first two paths are unsatisfying because (1) many states do not clearly recognize trade secrets as property and (2) the closest common law analogs to trade secret actions are likely inapposite. The final path—that these DTSA violations result in independent harms—is likely to be successful, but it requires the presence of certain facts accompanied by specific plausible allegations of harm in a complaint. The lack of a satisfying path to standing may indicate that some courts are abdicating their constitutionally required obligation to ensure standing, while wrongly exerting their power against employees and marketplace competitors.

#### A. Are Trade Secrets a Property Right?

If a trade secret is a property right, then the improper acquisition of a trade secret—though not necessarily threatened misappropriation—likely confers standing: *TransUnion* instructed that a lawsuit can proceed where “the plaintiff has suffered concrete harm to her property.”<sup>212</sup> However, whether a trade secret is a property right is a close, open question in many states.<sup>213</sup> There are two competing theories regarding the underpinnings of trade secret law: one that relies on a conception of trade secrets as property and another that relies on a theory of trade secrets as reliant on relational duties, which sound in

---

<sup>212</sup> See *TransUnion*, 141 S. Ct. at 2206. Improper acquisition would likely amount to trespass of a chattel or conversion, both concrete harms. See, e.g., *Mey v. Got Warranty*, 193 F. Supp. 3d 641, 647 (N.D. W. Va. 2016). Threatened misappropriation, however, might not confer standing *even if* trade secrets are recognized as property. Threatening a property right is likely not enough for standing under the modern doctrine.

<sup>213</sup> Charles T. Graves, *Trade Secrets as Property: Theory and Consequences*, 15 J. INTELL. PROP. 39, 41 (2007) (recognizing the “persistent philosophical debate” concerning whether trade secrets are property); see also *id.* at 63 (“[T]he fact that a court may in passing describe trade secrets as property rights or duties of confidence does not tell the reader whether the court is speaking as a result of sustained philosophical reflection on the subject.”). To be sure, it is rare that state courts need to expressly decide whether a trade secret entails a property right. CALLMANN, *supra* note 106, § 14:14 (“It is only in exceptional cases that the protection of the property right in a trade secret furnishes the theoretical basis for protecting the owner of the secret against the unlawful use of confidential knowledge.”).



tort.<sup>214</sup> Some states have endorsed the property theory, some have endorsed the relational view, and many—perhaps most—have been silent or ambiguous on the question.<sup>215</sup> Because it is unclear in many states whether trade secrets are property rights, this path to standing will sometimes fall short.

1. An understanding of trade secrets as premised on a property conception has been adopted by some courts.

Proponents of the argument that trade secrets are property generally start with the contention that trade secrets have many property-like traits: trade secrets are assignable, they can be passed down in a trust, and they can pass to a trustee in bankruptcy.<sup>216</sup> The Supreme Court in *Ruckleshaus v. Monsanto*<sup>217</sup> observed the “property-like” nature of trade secrets and held that trade secrets are property under Missouri law for the purposes of a Fifth Amendment Takings Clause<sup>218</sup> analysis.<sup>219</sup> While observant commentators have recognized the limitations of *Ruckleshaus*,<sup>220</sup> some courts have cited the case to suggest that trade secrets *are*, in fact, property.<sup>221</sup>

---

<sup>214</sup> See, e.g., *Deerpoint Grp., Inc. v. Agrigenix, LLC*, 400 F. Supp. 3d 988, 997 (E.D. Cal. 2019) (explaining that the “property approach” to trade secrets “is the alternative to the ‘relationship approach’”); see also *N. Petrochemical Co. v. Tomlinson*, 484 F.2d 1057, 1060 (7th Cir. 1973) (finding that “[a] suit to redress the theft of a secret is one grounded in tort”).

<sup>215</sup> See, e.g., *Grow Co. v. Chokshi*, 403 N.J. Super. 443, 469 (App. Div. 2008) (finding that it “is not entirely clear where New Jersey law stands” on whether trade secrets are property rights); *Progressive Prods. v. Swartz*, 292 Kan. 947, 954 (2011) (observing that “trade secret law creates a property right that is defined by the extent to which the owner of the secret protects that interest from disclosure to others” under Kansas law); *Valco Cincinnati, Inc. v. N & D Machining Serv., Inc.*, 492 N.E.2d 814, 817–18 (Ohio 1986) (“The employer who has discovered or developed trade secrets is protected against unauthorized disclosure or use, not because he has a property interest in the trade secrets but because the trade secrets were made known to the employee in a confidential relationship.”).

<sup>216</sup> *Ruckleshaus v. Monsanto*, 467 U.S. 986, 1002 (1984).

<sup>217</sup> *Id.*

<sup>218</sup> U.S. CONST. amend. V.

<sup>219</sup> *Ruckleshaus*, 467 U.S. at 1001–02.

<sup>220</sup> *Kapczynski*, *supra* note 97, at 1416 (“The Missouri cases cited by the court also did not conclude clearly that trade secrets were property under state law. Instead of paying close attention to state law, the Court gestured at Blackstone and Locke.”). There is reason to be skeptical of using Supreme Court cases to argue for *or* against the view that trade secrets are property because, as attorney Charles Graves observes, “[t]rade secret law does not develop from landmark federal cases in the same manner that, say, copyright or patent law does. The U.S. Supreme Court does not provide final authority on state law questions of trade secret law, except where they collide with federal law.” Graves, *supra* note 213, at 70 n.96.

<sup>221</sup> See, e.g., *Oakwood Lab’s LLC v. Thanoo*, 999 F.3d 892, 914 (3d Cir. 2021).

It is important not to overread *Ruckleshaus*. *Ruckleshaus* did not declare that a trade secret is absolutely a property right; rather, it interpreted Missouri common law to view a trade secret as a property right.<sup>222</sup> As discussed above, states have varied understandings of trade secret law. And, in any case, the precedential value of *Ruckleshaus* should be limited to the takings context.

Still, there is support for the property view of trade secrets beyond *Ruckleshaus*. Property interests “are created and their dimensions are defined by existing rules or understandings that stem from an independent source such as state law,”<sup>223</sup> and some states clearly recognize trade secrets as property rights.<sup>224</sup> Likewise, scholars have recognized the use of property-like terminology dating back to early trade secret cases, notwithstanding that “[t]he property view of trade secrets often evokes more conceptual heat than light.”<sup>225</sup> This could be dispositive in DTSA cases in which standing is litigated because, as discussed above, federal courts interpret the statute coextensively with the jurisdiction’s state-level law.

2. An alternative understanding of trade secrets views them as dependent on relational duties rather than property rights.

In contrast, the Supreme Court’s decision in *E. I. DuPont de Nemours Powder Co. v. Masland*<sup>226</sup> is sometimes cited to illustrate that trade secrets are rooted in relational duties rather than property rights.<sup>227</sup> Justice Oliver Wendell Holmes wrote in

---

<sup>222</sup> *Ruckleshaus*, 467 U.S. at 1001–02.

<sup>223</sup> *Bd. of Regents of State Colls. v. Roth*, 408 U.S. 564, 577 (1972).

<sup>224</sup> States that appear to have clearly endorsed the property view include Alaska, California, Georgia, Hawaii, Indiana, Kansas, Minnesota, Tennessee, and Utah. See 2 BRIAN M. MALSBERGER, *TRADE SECRETS: A STATE-BY-STATE SURVEY* 55 (Alaska), 264 (California), 806 (Georgia), 883 (Hawaii), 1121 (Indiana), 1297 (Kansas), 1688 (Michigan), 1774 (Minnesota), 2975 (Tennessee), 3127 (Utah) (7th ed. 2018). *But see* *Sec. People, Inc. v. Medeco Sec. Locks, Inc.*, 59 F. Supp. 2d 1040, 1043 (N.D. Cal. 1999), *aff’d*, 243 F.3d 555 (Fed. Cir. 2000) (“The decision to focus on the relationship, and not to treat trade secrets as ‘property,’ reflects a policy choice by California in which the interests in promoting the free use of new ideas is elevated over the interests in rewarding holders of economically significant secrets.”).

<sup>225</sup> See MILGRIM, *supra* note 28, § 2.01 (“Rights in a trade secret are in the nature of property rights.”).

<sup>226</sup> 244 U.S. 100 (1917).

<sup>227</sup> See, e.g., *Kubik, Inc. v. Hull*, 56 Mich. App. 335, 357 (1974) (interpreting *Masland* to understand trade secrets as reliant on relational duties, not property rights); see also

*Masland* that the starting point for trade secret law “is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs.”<sup>228</sup> Although the all-important text is arguably dicta, *Masland* suggests that the use of property-like terminology in early trade secret cases is an “unanalyzed expression” that does not necessarily place trade secrets in the property domain.<sup>229</sup> Breaches of confidentiality—not violations of a property interest—might undergird liability for trade secret misappropriation.

While some scholars—and the Supreme Court itself—have minimized the importance of *Masland* in certain contexts,<sup>230</sup> other courts and scholars have found it dispositive.<sup>231</sup> Further, because property rights are generally defined by states,<sup>232</sup> notwithstanding the Supreme Court’s interpretation of *Masland*, some states still endorse the relational theory over the property theory, and many more have been unclear on the question.<sup>233</sup> Moreover, aside from *Masland*, there is significant legal support for the relational view of trade secrets. For instance, the influential 1939 Restatement (First) of Torts avers that a property theory of trade secrets “has been frequently advanced and rejected.”<sup>234</sup> The Restatement noted that “good faith” is the

---

In re Educ. Comput. Corp., 199 U.S.P.Q. 178, 185 (Armed Serv. Bd. Contract App. 1977) (citing *Masland* to cast doubt on the property conception).

<sup>228</sup> *Masland*, 244 U.S. at 102.

<sup>229</sup> *Id.*; see Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 316 (2008) (“In the nineteenth century, courts periodically spoke of trade secrets as property rights, though it is not clear that they meant by that term what we mean today.”).

<sup>230</sup> See, e.g., MILGRIM, *supra* note 28, § 2.01; Graves, *supra* note 213, at 70 n.96; *Ruckleshaus*, 467 U.S. at 1004 n.9 (averring that *Masland* did not foreclose the property view).

<sup>231</sup> See, e.g., *Law Kendall Holdings, Ltd. v. Eden Cryogenics, LLC*, 2010 WL 3894166, at \*1 (S.D. Ohio Sept. 29, 2010); see also Pamela Samuelson, *Principles for Resolving Conflicts Between Trade Secrets and the First Amendment*, 58 HASTINGS L.J. 777, 807 (2007).

<sup>232</sup> See *Roth*, 408 U.S. at 577.

<sup>233</sup> States that ostensibly endorse the relational view and lean away from the property view include Oregon, Rhode Island, and Texas. See MALSBERGER, *supra* note 224, at 2643 (Oregon), 2812–13 (Rhode Island), 3036 (Texas). See, e.g., *Justin Belt Co. v. Yost*, 502 S.W.2d 681, 685 (Tex. 1973); *Stimson Lumber Co. v. Laurence-David, Inc.*, 224 Or. 447, 452 (1960). States that are ambiguous on their view of trade secrets as property include Delaware, Illinois, New Jersey, and New York. See MALSBERGER, *supra* note 224, at 589 (Delaware), 965 (Illinois), 2115 (New Jersey), 2219 (New York).

<sup>234</sup> See RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

underlying policy rationale that justifies the law, implying that the Restatement instead endorsed the relational view.<sup>235</sup>

Importantly, trade secrets are fundamentally different from what courts usually consider to be property. The boundaries of a given trade secret are not well-defined, at least until the start of litigation, whereas property and its accompanying right to exclude generally appears to require a fixed boundary.<sup>236</sup> Trade secrets—just like other forms of information—are not truly “in rem”;<sup>237</sup> they are not rights against the rest of the world because the law does not prevent anyone from reverse engineering a trade secret or discovering a trade secret independently.<sup>238</sup>

Just like the Supreme Court in *Ruckleshaus*, federal courts should look to state common law to determine whether trade secrets should be considered property or relational rights. Courts already look to state law to determine the applicability of the inevitable disclosure doctrine.<sup>239</sup> And in cases outside of the trade secret context, federal courts are sometimes called to evaluate what constitutes a property injury in the state in which the federal court sits to ensure standing; in these cases, there is no standing if there is not recognition of a property right.<sup>240</sup> Just the same, if an employee is alleged to have misappropriated a trade secret in one of the many states that does not clearly recognize trade secrets as property rights, then standing should be questioned. Insofar as most states have an ambiguous view or clearly do not view trade secrets as property, improper acquisition should not amount to an invasion of a property right in most states, leading to questionable standing.

---

<sup>235</sup> *Id.*; see also Bone, *supra* note 98, at 245 (rejecting the property view).

<sup>236</sup> See *ILG Indus., Inc. v. Scott*, 49 Ill. 2d 88, 97 (1971); see also *Vacco v. Van den Berg*, 6 Cal. Rptr. 2d 602, 612 n.16 (1991).

<sup>237</sup> See *Coll. Sav. Bank v. Fla. Prepaid Postsecondary Educ. Expense Bd.*, 527 U.S. 666, 667 (1999) (“The hallmark of a protected property interest is the right to exclude others. That is ‘one of the most essential sticks in the bundle of rights that are commonly characterized as property.’”).

<sup>238</sup> See *Franke v. Wiltschek*, 209 F.2d 493, 495 (2d Cir. 1953) (“Plaintiffs do not assert, indeed cannot assert, a property right in their development such as would entitle them to exclusive enjoyment against the world. Theirs is not a patent, but a trade secret.”).

<sup>239</sup> See, e.g., *Phoseon Tech., Inc. v. Heathcote*, 2019 WL 7282497, at \*11 (D. Or. Dec. 27, 2019).

<sup>240</sup> See, e.g., *United States v. Timley*, 507 F.3d 1125, 1129–30 (8th Cir. 2007) (forfeiture) (looking to the “law of the jurisdiction that created the property right to determine whether the claimant has a valid interest”); *O’Neil v. Peak*, 2010 WL 55865, at \*3 (W.D. Wash. Jan. 5, 2010) (civil RICO) (“[I]n order to achieve standing under [the civil RICO statute] a plaintiff must show harms to a state-created property interest.”).

## B. Are Improper Acquisition or Threatened Misappropriation Traditionally Recognized Injuries?

Perhaps the next best path to standing is to argue that improper acquisition and threatened misappropriation are intangible yet concrete injuries because they each have “a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts.”<sup>241</sup> It is difficult to determine what sort of pedigree satisfies the “traditionality” test,<sup>242</sup> but applications of *Spokeo* appear to require a harm that has been consistently<sup>243</sup> recognized as a basis of a lawsuit for well over a century.<sup>244</sup>

Before embarking on a search for a related common law analog, it is first important to establish that improper acquisition and threatened acquisition—as they are understood today—were not traditionally actionable at common law. If the violations at issue in this Comment *have* long been actionable, then it would be difficult to argue that Congress is overstepping its bounds by providing a cause of action for these DTSA violations; if these forms of misappropriation have always been actionable, then the DTSA would merely be an example of Congress codifying long-recognized cognizable injuries.<sup>245</sup> This Section illustrates, first, that improper acquisition was not traditionally actionable and, second, that just *some* forms of threatened misappropriation were actionable.

First, improper acquisition was not traditionally actionable. This suggests that it may not have a traditional common law analog under *Spokeo*. The UTSA, penned in 1979, recognized a cause of action for mere improper acquisition, but the UTSA

---

<sup>241</sup> *Spokeo*, 578 U.S. at 341.

<sup>242</sup> See *Muransky*, 979 F.3d at 931 (questioning what constitutes a “sufficiently ancient” cause of action).

<sup>243</sup> See, e.g., *TransUnion*, 141 S. Ct. at 2204.

<sup>244</sup> See *infra* text accompanying note 266.

<sup>245</sup> To be sure, *even if* violations of the DTSA are akin to long-recognized cognizable injuries, a mere violation of the statute may not confer standing. The Seventh Circuit recently interpreted *TransUnion* to distinguish

between (1) the cause of action giving a plaintiff the right to sue over a defendant’s legal infraction and (2) the injury, if any, that he suffered as a result.

To sue in federal court, a plaintiff must have both; a suitable cause of action cannot save a plaintiff’s case if he has suffered no harm.

*Dinerstein v. Google, LLC*, 73 F.4th 502, 519 (7th Cir. 2023). The court went on to add that “*Spokeo* and *TransUnion* put an end to federal courts hearing claims premised on nonexistent injuries—regardless of historical pedigree.” *Id.* at 521.

almost surely does not have a sufficiently ancient pedigree to meet the traditionality test.<sup>246</sup> Just a few years before the creation of the UTSA, the Supreme Court surveyed trade secret law in *Kewanee Oil Co. v. Bicron Corp.*<sup>247</sup> and did not recognize improper acquisition as violative of the common law;<sup>248</sup> the Court only recognized the availability of a cause of action where a trade secret was both improperly acquired *and* subsequently used or disclosed.<sup>249</sup> The Restatement (First) is also instructive, and it does not find that a cause of action is available for mere acquisition: the Restatement recognizes only misuse and disclosure as actionable.<sup>250</sup>

One case frequently cited as marking the birth of American trade secret law<sup>251</sup> is the 1868 case *Peabody v. Norfolk*.<sup>252</sup> The case did not involve mere acquisition insofar as Norfolk, the defendant employee, was specifically alleged to have been in the process of taking information about his former employer's textiles process *to a market competitor*.<sup>253</sup> The dispute was actionable not because of the improper acquisition itself, but because there was impending use or disclosure of the secret that followed the acquisition.<sup>254</sup> *Peabody* is typical of early trade secret cases insofar as it involved actual competition with the plaintiff in the marketplace.<sup>255</sup> That is, acquisition itself was likely not considered a cognizable injury under state common law unless the acquisition was paired with allegations suggesting impending use or disclosure that would harm the plaintiff's business.<sup>256</sup>

---

<sup>246</sup> See *Muransky*, 979 F.3d at 931.

<sup>247</sup> 416 U.S. 470 (1974).

<sup>248</sup> *Id.* at 475.

<sup>249</sup> *Id.*

<sup>250</sup> See MILGRIM, *supra* note 28, § 1.01[1]; see also Sandeen, *Out of Thin Air*, *supra* note 10, at 385 (“[T]he recognition of a claim of acquisition by improper means, not followed by a subsequent disclosure or use, did not officially occur until 1979 when the UTSA was adopted.”).

<sup>251</sup> JAGER, *supra* note 17, § 2:3 (collecting early U.S. trade secret cases).

<sup>252</sup> 98 Mass. 452 (1868).

<sup>253</sup> *Id.* at 453–54.

<sup>254</sup> See, e.g., *Massaro*, 266 F. Supp. 3d at 452 (summarizing Massachusetts trade secret law before the state's adoption of the UTSA, and explaining that misappropriation requires plaintiffs to show use or disclosure).

<sup>255</sup> See CATHERINE L. FISK, *WORKING KNOWLEDGE: EMPLOYEE INNOVATION AND THE RISE OF CORPORATE INTELLECTUAL PROPERTY, 1800–1930*, at 175 (2009).

<sup>256</sup> 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 MITCHELL HAMLIN L. REV. 493, 499 (2010); see also Kapczynski, *supra* note 97, at 1382 (observing that “courts [were] hostile to contracts aiming to restrict the mobility or uses of information by skilled employees through the early nineteenth century”).

Second, threatened misappropriation as we currently understand it was often not actionable under the common law.<sup>257</sup> Historic threatened misappropriation cases have limited usefulness because they were confined to instances involving the actual threat of competition in the market, rather than a general threat of downstream trade secret use or disclosure.<sup>258</sup> While threatened misappropriation that involved impending or actual departure to a competing company was surely recognized at common law,<sup>259</sup> modern threatened misappropriation does not demand anything close to a showing that the alleged acquirer of the trade secret is—or could be—an injurious competitor in the marketplace.<sup>260</sup> Thus, while some forms of threatened misappropriation might satisfy the common law analog test from *Spokeo* because the Court instructed that “*Spokeo* does not require an exact duplicate in American history and tradition,”<sup>261</sup> the sorts of threatened misappropriation recognized by the DTSA likely do not analogize. This is because allegations of injurious *unfair competition*, rather than mere and amorphous threat, were key to threatened misappropriation claims.<sup>262</sup>

This history reveals that, while trade secret law has always been understood to regulate commercial morality, improper acquisition and many forms of threatened misappropriation are of relatively new import, and therefore may not meet the *Spokeo* traditionality test on their own.

### C. Potential Common Law Analogs

That mere improper acquisition and some forms of threatened misappropriation were not historically actionable indicates that they might lack a traditional common law analog. An exhaustive review of every potential common law analog is impossible. Thus, this Comment focuses on the three best candidates available for courts searching for a common law

---

<sup>257</sup> See Fisk, *supra* note 255, at 175 (“If the employee was permitted to acquire, and did acquire, a full knowledge of the trade secret to enable him to perform his duties, the employer could not afterward restrain him from using any knowledge so acquired or any secret so disclosed.” (quotation marks omitted)).

<sup>258</sup> See *supra* text accompanying note 171; see also Timothy E. Murphy, *Memorizing Trade Secrets*, 57 U. RICH. L. REV. 533, 571 (2023) (collecting cases, and finding that “early courts were often reluctant to grant injunctions upon speculative future disclosures”).

<sup>259</sup> See Fisk, *supra* note 255, at 177.

<sup>260</sup> See *supra* text accompanying note 184.

<sup>261</sup> *TransUnion*, 141 S. Ct. at 2204.

<sup>262</sup> Sandeen, *Out of Thin Air*, *supra* note 10, at 382.

analog to satisfy *Spokeo*'s traditionality test:<sup>263</sup> breach of confidence, intrusion upon seclusion, and breach of express or implied contract.

Ultimately, these analogs are likely unsuitable to meet *Spokeo*'s demand. Breach of confidence fails as a common law comparator because it requires third-party disclosure, whereas the DTSA violations at issue do not. Intrusion upon seclusion is inapposite because a key component of the tort is highly offensive conduct toward an individual and such an element is absent from trade secret violations. And implied breach of contract likely falls flat because contracts are legal rights that may not inflict "real" harm when breached. Because these three paths to standing likely fail, courts cannot turn to them to confer standing for plaintiffs who allege bare improper acquisition or threatened misappropriation.

1. Threatened misappropriation and improper acquisition likely fail to map onto a breach of confidence.

Breach of confidence is a common law tort that protects private information conveyed in confidence.<sup>264</sup> Improper acquisition through a violation of a duty to maintain secrecy seems, at first blush, similar to the tort of a breach of confidence. Threatened misappropriation can also be analogized to a breach of confidence insofar as the defendant is threatening to act in bad faith against their employer's interests by intending to disseminate their confidential information.

Indeed, trade secret law was "originally conceived of as an act of unfair competition resulting from a breach of confidence."<sup>265</sup> While a breach of confidence *might*<sup>266</sup> have the pedigree required

---

<sup>263</sup> The author considered analogizing to several other common law causes of action, including breach of a fiduciary duty and unjust enrichment. Breach of a fiduciary duty plainly fails to align with the trade secret actions at issue because while trade secret violations do not require a separate harm, a breach of fiduciary duty requires the plaintiff to show some actual, independent "harm resulting from [the] breach of duty." RESTATEMENT (SECOND) OF TORTS § 874 (1979). Unjust enrichment similarly fails as a comparator because unjust enrichment would require that the defendant *used* the trade secret to enrich themselves and, of course, the trade secret actions at issue necessarily do not entail use. See RESTATEMENT (FIRST) OF RESTITUTION § 136 (1937) ("A person who has tortiously *used* a . . . trade secret . . . is under a duty to restitution for the value of the benefit thereby received." (emphasis added)).

<sup>264</sup> See *Kamal*, 918 F.3d at 114.

<sup>265</sup> Sandeen, *Out of Thin Air*, *supra* note 10, at 382.

<sup>266</sup> *Muransky*, 979 F.3d at 931–32 (finding that it is unclear whether breach of confidence can be regarded as a "traditional" tort under *Spokeo*).



by *Spokeo*, this path to standing almost surely falls short because a breach of confidence traditionally required “disclosure to a third party.”<sup>267</sup> Of course, neither improper acquisition nor threatened misappropriation requires actual disclosure. And the Supreme Court in *TransUnion* instructed that when an element “essential to liability” at common law is absent from an alleged harm, the common-law comparator is insufficient to form the basis of a concrete harm.<sup>268</sup>

2. Intrusion upon seclusion likely falls short in most cases.

The tort of intrusion upon seclusion occurs where someone invades the solitude of another in a way that would be “highly offensive to a reasonable person.”<sup>269</sup> The Court explicitly cited “inclusion upon seclusion” as a “traditional” harm, fit for the *Spokeo* inquiry.<sup>270</sup> The trade secret actions at issue in this Comment may analogize to intrusion upon seclusion, but they map awkwardly onto this tort for two reasons.

First, the tort definitionally requires that the intrusion be “highly offensive” to a reasonable person.<sup>271</sup> The Eleventh Circuit described intrusion upon seclusion as requiring “universally condemnable” intrusion, “objectively intense interference.”<sup>272</sup> For example, persistent harassment through phone calls would constitute intrusion upon seclusion.<sup>273</sup> In contrast, it seems difficult to argue that the activity described by courts as giving rise to liability for improper acquisition or threatened misappropriation is “highly offensive” or “objectively intense.” Rather, the activity—such as one instance of downloading trade secrets onto an external drive—is more properly described as “isolated, momentary, and ephemeral.”<sup>274</sup>

Second, both courts and scholars have recognized the tort of intrusion upon seclusion as being concerned with *individuals’*

---

<sup>267</sup> See *Kamal*, 918 F.3d at 118 (“[W]e do not believe a breach of confidence action is sufficiently analogous absent third-party disclosure.”); see also *Muransky*, 979 F.3d at 926 (same).

<sup>268</sup> See *TransUnion*, 141 S. Ct. at 2209–10.

<sup>269</sup> *Salcedo v. Hanna*, 936 F.3d 1162, 1171 (11th Cir. 2019) (quoting RESTATEMENT (SECOND) OF TORTS § 652B).

<sup>270</sup> *TransUnion*, 141 S. Ct. at 2204.

<sup>271</sup> RESTATEMENT (SECOND) OF TORTS § 652B.

<sup>272</sup> *Salcedo*, 936 F.3d at 1171.

<sup>273</sup> See RESTATEMENT (SECOND) OF TORTS § 652B cmt. d.

<sup>274</sup> *Salcedo*, 936 F.3d at 1171.

privacy, dignity, and protection from embarrassment.<sup>275</sup> A classic example is someone spying on another in their home. Such activity is likely actionable under the tort because it is an invasion of an individual's personal affairs.<sup>276</sup> The Supreme Court of California has understood the tort to require a "plaintiff [to] show the defendant penetrated some zone of physical or sensory privacy surrounding, or obtained unwanted access to data about, the plaintiff."<sup>277</sup> While the trade secret actions at issue in this Comment typically involve some sort of unwanted intrusion, trade secret actions have nothing to do with individuals' privacy, dignity, or protection from embarrassment.

To be sure, some instances of improper acquisition through espionage may fall under this tort because spying on a business to obtain private information seems similar to intrusion upon seclusion. However, an instance of flying a plane over a factory to take photographs,<sup>278</sup> for example, seems ephemeral, momentary, and hardly "highly offensive."

3. Breach of express or implied contract is likely the best analogy, but it might not be the sort of analog accepted by courts.

Courts might also look to the history of trade secrets and recognize that, at least as far as the employer-employee relationship is concerned, trade secret rights can stem from an express or implied contract between the two parties. Thus, improper acquisition or threatened misappropriation might amount to a breach of contract,<sup>279</sup> which could be a traditionally recognized injury.

Yet courts and commentators alike have suggested that a mere breach of a contract—divorced from harm—likely does not constitute a concrete injury under *Spokeo* either.<sup>280</sup> As Professors

---

<sup>275</sup> See Edward Bloustein, *Privacy as an Aspect of Human Dignity*, 39 N.Y.U. L. REV. 962, 971 (1964).

<sup>276</sup> See, e.g., *Kohler v. City of Wapakoneta*, 381 F. Supp. 2d 692, 704 (N.D. Ohio 2005).

<sup>277</sup> *Shulman v. Grp. W Prods., Inc.*, 955 P.2d 469, 490 (Cal. 1998).

<sup>278</sup> *Christopher*, 431 F.2d at 1013.

<sup>279</sup> Because an express or implied contract requires some relationship between the parties, improper acquisition through espionage will not analogize.

<sup>280</sup> See F. Andrew Hessick, *Standing and Contracts*, 89 GEO. WASH. L. REV. 298, 313 (2021) (arguing that because contracts simply create legal rights, a breach of contract should not in itself support standing under *Spokeo*); see also, e.g., *Dinerstein*, 73 F.4th at 522 ("[A] breach of contract alone—without any actual harm—is purely an injury in law, not an injury in fact. And it therefore falls short of the Article III requirements for a suit in federal court."); *Svenson v. Google Inc.*, 2016 WL 8943301, at \*10 (N.D. Cal. Dec. 21,

Danielle Citron and Daniel Solove observe, “[f]ailing to fulfill promises . . . and thus betraying people’s expectations has not counted as a cognizable harm.”<sup>281</sup> Further, the line of cases that find a lack of standing for data breaches may foreclose the argument that a breach of an implied contract, without more, is a cognizable injury. Employees and customers whose data was lost can often be said to have an implied contract—through privacy policies or otherwise—with the entity that held their data.<sup>282</sup> In such cases, the implied contract argument has been rejected.<sup>283</sup>

#### D. Do Improper Acquisition or Threatened Misappropriation Result in Other Concrete Harms?

*TransUnion* instructs that a risk of harm can be actionable when it causes an independent concrete harm.<sup>284</sup> DTSA plaintiffs might find a better path to standing by averring that improper acquisition and threatened misappropriation necessarily lead to concrete harms.

For instance, courts could surely find concrete harm based on a theory involving the actual devaluation of a trade secret. If the trade secret at issue is being actively licensed<sup>285</sup> and has a readily available market, the plaintiff may be able to show that an instance of improper acquisition decreased its licensing value, so long as the plaintiff plausibly pleads facts to show that their economic harm is real, rather than speculative or conjectural.<sup>286</sup>

---

2016) (finding that a breach-of-contract plaintiff “must show the *fact* of injury” for Article III standing (emphasis in original)). *But see* *Dinerstein v. Google, LLC*, 484 F. Supp. 3d 561, 571 (N.D. Ill. 2020) (“Whether alleging breach of contract—without actual damages—is enough to confer standing is a close call. There is authority on both sides of the issue, but the court concludes that Plaintiff has the better argument.”).

<sup>281</sup> Danielle K. Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830–61 (2022).

<sup>282</sup> *See, e.g., Svenson*, 2016 WL 8943301, at \*10.

<sup>283</sup> *Id.*

<sup>284</sup> *See TransUnion*, 141 S. Ct. at 2211.

<sup>285</sup> A company that licenses a trade secret to others sells the right to derive value from the trade secret. *See, e.g., NOVA Chems., Inc. v. Sekisui Plastics Co.*, 579 F.3d 319, 327–28 (3d Cir. 2009).

<sup>286</sup> Some courts have accepted this argument in the personal data domain after plaintiffs whose data was stolen—but not misused—sought standing for the devaluation of their data. *See, e.g., In re Marriott Int’l, Inc., Customer Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 460–62 (D. Md. 2020) (conferring standing for the “loss of value of property” in plaintiffs’ personal identifying information). *But see Chambliss v. Carefirst, Inc.*, 189 F. Supp. 3d 564, 572 (D. Md. 2016) (rejecting standing, and holding that the court “need not decide whether such personal information has a monetary value, as Plaintiffs have not

The devaluation theory seems unlikely to work if there is not a likely buyer or licensee for the trade secret at issue.<sup>287</sup> Similarly, the devaluation theory should fail under the modern doctrine where a company has abandoned its trade secret. A company cannot claim to be damaged for losing exclusive access to something from which it never materially benefitted.

Courts might also accept the argument that trade secret misappropriation necessarily decreases the value of the company that holds it, *even* if the misappropriation does not devalue the trade secret. Consider a case in which investors discover that a trade secret has been improperly acquired or threatened; investors might think that the company is devalued, even if it has not actually lost the ability to tap the value of its trade secret. A subsequent loss of stock price, for example, would certainly be enough to show concrete harm,<sup>288</sup> if the price hit could be connected to the trade secret theft. This may establish standing, but again, federal courts have an obligation to require plaintiffs to actually plead the above injuries. Conclusory allegations involving hypothetical investors who might find out about an instance of improper acquisition or threat should not suffice to get through the courthouse doors.

#### CONCLUSION

This Comment highlights one area that standing doctrine has inexplicably not yet touched: federal trade secret law. Federal courts have routinely shut data breach plaintiffs out of court for failing to demonstrate concrete or imminent injuries. Yet courts uniformly confer standing for plaintiffs alleging improper acquisition and threatened misappropriation, violations of the DTSA that may similarly fail to represent concrete or imminent injuries.

Indeed, federal courts' adjudication of DTSA cases that allege bare violations of the statute provides plaintiffs the benefit of pleading traditionally state law claims in federal court without

---

alleged that they have attempted to sell their personal information or that, if they have, the data breach forced them to accept a decreased price for that information”).

<sup>287</sup> See *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 784 (N.D. Cal. 2019) (holding that a hypothetical loss of value is insufficient to confer standing).

<sup>288</sup> Empirical literature reveals that companies that suffer from data breaches sometimes experience a loss in market value. See, e.g., Daniel Schatz & Rabih Bashroush, *The Impact of Repeated Data Breach Events on Organisations' Market Value*, 24 *INFO. & CYBER SEC.* 73, 87 (2016).

requiring those same plaintiffs to pay the cost of entry: a heightened Article III standing requirement.<sup>289</sup> By closely scrutinizing DTSA cases that might lack plausible allegations of an injury-in-fact, federal courts can both ensure that they are acting within their constitutional limits and protect employee mobility.

---

<sup>289</sup> See *TransUnion*, 141 S. Ct. at 2224 n.9 (Thomas, J., dissenting) (noting that state courts are not bound by Article III).