Pace Law Review

Volume 40 | Issue 2 Article 5

July 2020

Judicial Reward Allocation for Asymmetric Secrets

Runhua Wang
Chicago-Kent College of Law, rwangkent@gmail.com

Recommended Citation
Runhua Wang, *Judicial Reward Allocation for Asymmetric Secrets*, 40 Pace L. Rev. 226 (2020)
DOI: https://doi.org/10.58948/2331-3528.2020
Available at: https://digitalcommons.pace.edu/plr/vol40/iss2/5

Judicial Reward Allocation for Asymmetric Secrets

Runhua Wang*

TABLE OF CONTENTS

* Empirical IP Fellow, Chicago-Kent College of Law. Thanks to Edward Lee, Mickie Piatt, and Jiubin Wang for their knowledge and ideas to develop and improve the work.

Abstract

Trade secret literature does not thoroughly consider information asymmetries between companies and employees. This Article visualizes the flows of technical information in and between companies and employees and categorizes two types of information asymmetries in the information transactions. The information asymmetries cannot be effectively governed by contracts and trade secret law. Companies employ covenants not to compete ("CNCs"), non-disclosure agreements ("NDAs"), and trade secret protection to shift the legal risks borne by employees from the disclosure risks borne by the companies, both restraining and aggravating the information asymmetries. The contracts and the law cannot increase employee loyalty to eliminate the information asymmetries. The risk shifting is not only costly to the companies, but it also harms innovation by employees and society due to the inevitable information asymmetries. Moreover, courts are inconsistent in enforcing the contracts and trade secret law for promoting innovation and other policy reasons. This Article revisits the literature that concerns the balance and the efficiency of the contracts and trade secret law for innovation. It argues that courts reward companies for training employees and investing in innovation by enforcing trade secrets and CNCs to supplement the ineffective NDAs used by companies. CNCs are less efficient for innovation than trade secret law. Thus, this Article suggests that courts rely on a strong trade secret regime when distributing training and innovation rewards. The strong trade secret regime adopts the inevitable disclosure doctrine and allows a broad scope of trade secret protection, rather than enforcing broad NDAs or CNCs, which are less efficient for innovation than trade secret law. At least, this regime should not impair employee loyalty.

I. Introduction

Waymo LLC ("Waymo"), Google's spin-off, repeatedly chased after its departing employees who joined its rival—Uber Techs., Inc. ("Uber")—through the arbitration system and the

judicial system for trade secret concerns.[1] In recent years, the most famous and influential disputes in Silicon Valley are the disputes between Waymo and Anthony Levandowski—a former Google employee, Waymo's co-founder, and star engineer in self-driving[2]—but spun out from Google and sold his spin-out startup Otto Trucking LLC ("Otto") to Uber.[3] In Waymo's legal claim of trade secret misappropriation against Uber and Levandowski, Waymo alleges that Levandowski downloaded over 14,000 confidential files from Waymo, which were improperly employed by Levandowski, Otto, and Uber.[4] Evidence of downloads were admitted by the court,[5] resulting in a settlement between Waymo and Uber to share Uber's self-driving business. However, Waymo continues to pursue rewards from Levandowski in arbitration proceedings and for criminal penalties against him under criminal trade secret doctrines.[6] If there is no civil trade secret misappropriation acknowledged by the court, how likely is it that a former employee will be prosecuted for trade secret theft? Levandowski had no plan to pay the rewards assigned by arbitrators and struggled against 33 counts of theft and attempted theft of trade secrets,[7] but recently pleaded guilty to stealing those 14,000 confidential files in exchange for federal prosecutors dropping the other 32

1 *See* Paresh Dave, *Waymo Secures Bigger Award Against Workers Who Went to Rival Uber*, REUTERS (Jan. 9, 2020 8:35 PM), https://www.reuters.com/article/us-waymo-uber/waymo-secures-bigger-award-against-workers-who-went-to-rival-uber-idUSKBN1Z904D (reporting that Uber arbitrated against two departing employees who joined Uber other than Anthony Levandowski).

2 *See generally* Burkhard Bilger, *Auto Correct: Has the Self-Driving Car at Last Arrived?,* NEW YORKER (Nov. 18, 2013), https://www.newyorker.com/magazine/2013/11/25/auto-correct (introducing the history and background of Google's self-driving project and the contribution made by Levandowski).

3 *See* Bernie Woodall, *Uber Buys Self-Driving Truck Startup Otto; Teams with Volvo*, REUTERS (Aug. 18, 2016 12:50 PM), https://www.reuters.com/article/us-uber-tech-volvo-otto-idUSKCN10T1TR.

4 Waymo LLC v. Uber Techs., Inc., No. C 17-00939, 2017 U.S. Dist. LEXIS 73843, at *3 (N.D. Cal. May 15, 2017).

5 *Id.* at *41–43.

6 Associated Press, *Ex-Google Engineer Anthony Levandowski Is Charged with Trade Secrets Theft*, L.A. TIMES (Aug. 27, 2019 4:02 PM), https://www.latimes.com/business/story/2019-08-27/ex-google-engineer-anthony-levandowski-is-charged-with-trade-secrets-theft.

7 *Id.*

counts.[8] It is also the hopeless eleventh year that Sergey Aleynikov, a former employee of Goldman Sachs ("Goldman"), is fighting his trade secret theft case, while there has been a civil decision exempting him from the civil claim of trade secret misappropriation.[9] Because of downloading confidential source code from Goldman and employing the code at his new employer, Aleynikov might have been liable for the civil claim if Goldman found the downloading earlier before the expiration of the statute of limitations.[10]

Besides the confidential information, are there any other losses that drive Waymo and Goldman Sachs mad after Waymo made a deal with Uber, and Goldman asserted no material losses?[11] After investing in research and development ("R&D") and training employees, companies face indefinable losses due to the departure of employees, which may be definable after a long time and uncompensable.[12] However, there are talented employees like Levandowski and Aleynikov, who are the inventors deploying the R&D investment, but are antipathetic to being trapped by a company. They may resign with some knowledge when they believe that they do not own any binding legal liabilities to the company.[13] Can companies investigate what the exact knowledge is within the statute of limitations? If they could, should courts assign the companies a full recovery

8 Nick Statt, *Self-Driving Car Engineer Anthony Levandowski Pleads Guilty to Stealing Google Trade Secrets*, THE VERGE (Mar 19, 2020, 8:26 PM), https://www.theverge.com/2020/3/19/21187651/anthony-levandowski-pleads-guilty-google-waymo-uber-trade-secret-theft-lawsuit.

9 *See* Peter J. Henning, *A Former Goldman Employee's Long, Strange Legal Odyssey*, N.Y. TIMES (Jan. 30, 2017), https://www.nytimes.com/2017/01/30/business/dealbook/a-former-goldman-employees-long-strange-legal-odyssey.html. Jonathan Stempel, *Former Goldman Programmer Fails, Again, to Toss Theft Conviction*, REUTERS (Oct. 8, 2019 3:40 PM), https://www.reuters.com/article/us-goldman-sachs-aleynikov/former-goldman-programmer-fails-again-to-toss-theft-conviction-idUSKBN1WN2AR (reporting that Aleynikov has been arrested twice since 2009 for the trade secret disputes between him and his former employer Goldman Sachs).

10 Aleynikov v. Goldman Sachs Grp., Inc., No. 12-5994, 2013 U.S. Dist. LEXIS 155137, at *7–8 (D.N.J. Oct. 29, 2013).

11 *Id.* at *2, 59 (finding that the claims of breach of contract and trade are barred for the statute of limitations).

12 *See, e.g.*, *id.*

13 *See, e.g.*, *id.* at *21–23 (reciting Aleynikov's claim that he did not sign any confidential contracts).

for the employee departure with the knowledge under contract law and trade secret law? From a legal perspective and a law and economics perspective, this Article argues that the answer is no to both questions due to inevitable asymmetric information.

The United States ("U.S.") constantly strengthens its trade secret regime for social demand.[14] Technology develops faster than the development of law.[15] Patent protection by itself is never sufficient for protecting technical information.[16] Surveys show that U.S. companies, especially large companies, view trade secrets more important than patents.[17] However, it is common that companies are like Goldman, taking years to ascertain their loss of confidential information.[18] After the U.S. federal system adopted the Defend Trade Secrets Act ("DTSA") to set up the federal jurisdiction for hearing civil trade secret claims in 2016,[19] Senator Kamala Harris introduced a bill to revise the DTSA in 2019 by increasing the exemplary damages and extending the statute of limitations for trade secret misappropriations.[20] Can the current trade secret regime supplemented by such a bill reduce trade secret complaints and delight both the innovative companies, such as Waymo and

14 Katherine Linton, *The Importance of Trade Secrets: New Directions in International Trade Policy Making and Empirical Research*, U.S. INT'L TRADE COMMISSION J. INT'L COM. & ECON. 1, 5–6 (Sept. 2016), https://www.usitc.gov/publications/332/journals/katherine_linton_importance_of_trade_secrets_0.pdf.

15 David S. Almeling, *Seven Reasons Why Trade Secrets Are Increasingly Important*, 27 BERKELEY TECH. L. J. 1091, 1108 (2012).

16 *E.g.*, Alice Corp. Pty. Ltd. v. CLS Bank Int'l, 573 U.S. 208 (2014) (discussing ambiguities about the patentable subject matters). *See* Bronwyn Hall et al., *The Choice Between Formal and Informal Intellectual Property: A Review*, 52 J. ECON. LITERATURE 375, 418–19 (2014) (suggesting that trade secrets and patents are usually used as complements to each other).

17 *E.g.*, James J. Anton & Dennis A. Yao, *Little Patents and Big Secrets: Managing Intellectual Property*, 35 RAND J. ECON. 1, 1 n.1 (2004) (discussing how larger companies rely more on trade secrets than patents); Vincenzo Denicolo & Luigi Alberto Franzoni, *Patents, Secrets, and the First-Inventor Defense*, 13 J. ECON. & MGMT. STRATEGY 517, 520 (2004). *But see* Josh Lerner, *Using Litigation to Understand Trade Secrets: A Preliminary Exploration*, SSRN (Aug. 7, 2006), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=922520.

18 BRIAN T. YEH, CONG. RESEARCH SERV., R43714, PROTECTION OF TRADE SECRETS: OVERVIEW OF CURRENT LAW AND LEGISLATION, CONG. RESEARCH SERV. 13–14 (2016), https://fas.org/sgp/crs/secrecy/R43714.pdf (suggesting that firms spend years to realize the loss of trade secrets).

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

20 S. 1865, 116th Cong. § 1 (2019).

Goldman, and innovative employees, such as Levandowski and Aleynikov, for promoting innovation?

The literature, however, is controversial about the relationship between the strength of trade secret protection and innovation. Since the 1990's, legal scholars have seen the importance of discussing the efficiency of trade secret law.[21] Trade secret protection may suggest high social costs, including, but not limited to, the security costs required by the law and independent invention costs for the public.[22] However, scholars have not thoroughly discussed the efficiency of trade secret law.[23] Linton suggests that strengthening trade secret protection and innovation are positively related at the international level.[24] Some scholars believe that trade secrets promote innovation by reducing employee mobility[25] and knowledge spillovers to competitors.[26] If employees understand that they cannot bring the technical information learned from companies, they prefer to stay.[27] Moreover, Lemley believes that trade secret protection is more efficient than private investment in precaution against disclosing technical information to

21 *See* Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CAL. L. REV. 241, 264 (1998).

22 *See* David D. Friedman et al., *Some Economics of Trade Secret Law*, 5 J. ECON. PERSP. 61, 67 (1991).

23 *See id.* (omitting the cost discussion about trade secret law). *See also* Joshua Lerner, *The Importance of Patent Scope: An Empirical Analysis*, 25 RAND J. ECON. 319 (1994) (failing to prove the efficiency of trade secret law); Bone, *supra* note 21, at 265–69 (criticizing the failure of Lerner and Friedman et al. in efficiency study about trade secret law).

24 Linton, *supra* note 14, at 11.

25 *See* Sharon K. Sandeen & David S. Levine, *Trade Secrets and Climate Change: Uncovering Secret Solutions to the Problem of Greenhouse Gas Emissions*, *in* RESEARCH HANDBOOK ON INTELLECTUAL PROPERTY AND CLIMATE CHANGE 352, 359 (Joshua D. Sarnoff ed., 2016); I.P.L. Png, *Trade Secrets, Non-Competes, and Mobility of Engineers and Scientists: Empirical Evidence,* 2–3 (Aug. 2012), https://pdfs.semanticscholar.org/f749/68d6c888d3648222263e90889f4040f1a88b.pdf.

26 *See* Tobias Schmidt, *An Empirical Analysis of the Effects of Patents and Secrecy on Knowledge Spillovers*, CTR. EUR. ECON. RES. 10–11 (2006), https://poseidon01.ssrn.com/delivery.php?ID=698078116086095107084089109100080096030023066052042011074117101014072065004022108026016061018004029042019067116118074088092047039092028028115102075004123018010007007003006123075067006017081113081019116006075094023120118071023016107073024010127004&EXT=pdf.

27 *See* David S. Levine & Ted Sichelman, *Why Do Startups Use Trade Secrets?,* 94 NOTRE DAME L. REV. 751, 768 (2018).

employees.[28] By contrast, Schmidt reminded the importance of external knowledge (i.e., knowledge spillovers contributed by others) to innovation and company growth.[29] Contigiani et al. also suggest that employer-friendly trade secret law has adverse effects on innovation for undervaluing the innovation efforts made by employees.[30] Overall, scholars consistently suggest that trade secret protection should be balanced. Trade secrets under proper legal protection should promote innovation, stimulate clusters, and do not prohibit knowledge access.[31] By contrast, over-protection of trade secrets eliminates knowledge spillovers and reduces clusters.[32]

Granting injunctive relief without actual harm under the inevitable disclosure doctrine ("IDD")[33] or the DTSA confirms the control right of the fruits of R&D investment. However, lavishing injunctions conveys over-rewarded first-mover advantages.[34] In order to provide proper and balanced trade secret protection, courts have to decide the expiration of trade secrets because there is no legislative expiration date for trade secrets, while companies prefer trade secrets to patents for the perpetual protection of trade secrets.[35] The expiration of trade secrets implies terminating the first-mover advantages of trade secret owners and the spillover benefits of the public.[36] The difficulty for courts originates from their power to assign the benefits.

28 Mark A. Lemley, *The Surprising Virtues of Treating Trade Secrets as IP Rights*, 61 STAN. L. REV. 311, 334–35 (2008).

29 Schmidt, *supra* note 26.

30 Andrea Contigiani et al., *Trade Secrets and Innovation: Evidence from the "Inevitable Disclosure" Doctrine*, 39 STRATEGIC MGMT. J. 2921, 2924 (2018).

31 *See id.* at 2922 (suggesting that trade secret protection needs to be balanced for promoting innovation); Andrea Fosfuri & Thomas Ronde, *High-Tech Clusters, Technology Spillovers, and Trade Secret Laws*, 22 INT'L J. INDUS. ORG. 45, 45 (2004); Andrew A. Schwartz, *The Corporate Preference for Trade Secret,* 74 OHIO ST. L. J. 623, 633–34 (2013); Sandeen & Levine, *supra* note 25, at 352.

32 Fosfuri & Ronde, *supra* note 31, at 45.

33 *See*, *e.g.*, PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).

34 *See infra* Sections V.B, V.C.

35 *See* Sudipto Bhattacharya & Sergei Guriev, *Patents vs. Trade Secrets: Knowledge Licensing and Spillover*, 4 J. EUR. ECON. ASS'N. 1112, 1116 (2006); Schwartz, *supra* note 31, at 647.

36 Levine & Sichelman, *supra* note 27, at 811 (emphasizing the importance of first-mover benefits given by trade secret protection to companies).

Based on the U.S. trade secret law, this Article explores the efficiency and the balance of enforcing trade secret protection by courts in civil cases for promoting innovation. The contribution of this Article is that it traces and maps the process of technical information formation and the information transactions between companies and employees. Employees can be either the originators of valuable technical information or the agents of deploying the information in business, or both.[37] Accordingly, this Article highlights two types of inevitable information asymmetries: first, employees may self-teach some technical information held by the company; second, employees may not disclose the innovative technical information originated by them to the company.[38] The two types of information asymmetries result in moral-hazard problems and suggests increased probable deadweight losses to companies after investing in R&D.

In order to explore the balance of governing technical information disclosure, this Article focuses on three primary trade secret protection measures against technical information disclosure by employees: (1) covenants of not to compete ("CNCs"); (2) non-disclosure agreements ("NDAs"); and (3) the trade secret legal doctrines under the Uniform Trade Secret Act ("UTSA")[39] and the DTSA. NDAs, or confidentiality agreements, prohibit employees from unauthorized disclosure of the employer's confidential information.[40] CNCs regulate that employees shall not compete with the employer "in the employer's existing or contemplated businesses for a designated period of time (e.g., three to five years) in a specified geographical region that corresponds to the market in which the employer participates" after the termination of employment.[41] However, all of those legal measures have uncertainties and shortcomings to eliminate the information asymmetries,

37 *See infra* Part II.

38 *See infra* Section II.C.

39 UNIF. TRADE SECRET ACT (UNIF. LAW COMM'N 1985).

40 *See* Miles J. Feldman, *Toward a Clearer Standard of Protectable Information: Trade Secrets and the Employment Relationship*, 9 BERKLEY TECH. L. J. 151, 179 (1994). Stuart J. H. Graham & Ted Sichelman, *Why Do Start-Ups Patent?*, 23 BERKELEY TECH. L. J. 1063, 1082 (2008).

41 Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 602–03 (1999).

resulting in inefficiency in promoting innovation. Thus, this Article revisits the literature concerning the efficiency and the inefficiency of the contracts and trade secret law under the track of the information flows between companies and employees, and explores the balance of enforcing them for courts.

This Article argues that CNCs and trade secret law are conditional rewards for companies to supplement NDAs. Instead of lavishly enforcing NDAs, a more efficient combination for innovation is to narrowly enforce NDAs but broadly recognize trade secrets. While both CNCs and the IDD under trade secret law can restrict employee mobility, they are not equivalent.[42] The rewards given by enforcing CNCs are cheaper but less efficient than trade secret law (including the IDD) in terms of encouraging innovation.[43] Contracts and trade secret law convert the disclosure risks borne by companies to legal risks borne by employees.[44] This Article suggests that under the fiduciary duties imposed by contracts or law, employee loyalty is still important but cannot be effectively increased by the discussed legal measures.[45] The risk-shifting by legal security measures may place innovation conducted by employees opposite to R&D invested by companies.[46] Courts should not send signals to disregard employee loyalty in civil cases, regardless of whether courts can improve employee ethics and prevent trade secret thefts by enforcing criminal doctrines.[47]

Part II maps the information transactions between a company and its employees, and visualizes the two types of information asymmetries in the transactions. Part III introduces how contracts (i.e., CNCs and NDAs) and trade secret law govern the technical information disclosure by employees. Part IV analyzes the risks of the disclosure under legal security measures, the ineffectiveness of the legal security measures which exaggerates the risks, and innovation impacted by the risks. Part V discusses the efficiency of enforcing the contracts and trade secret law on innovation.

42 *See infra* Section V.B.
43 *See infra* Sections V.B, V.C.
44 *See infra* Section IV.D
45 *See infra* Sections IV.B, IV.C, IV.D, V.D.
46 *See infra* Section IV.D.
47 *See infra* Section V.D.

II. Internal Technical Information Transactions

Innovation, R&D, production, and marketing need to exchange and use technical information. Figure 1 depicts a decision tree, which shows how a unit of technical information is deployed by companies and employees after the information is independently created and held by either side of them. Both a company and employees can control the technical information produced by the company's investment, depending on who is the direct creator of the information.[48] When holding control, the company and employee inventors have the choice to disclose the information to each other or outsiders. Phase I knowledge transactions from companies to employees constitute employee training, exchanging for Phase II knowledge transactions from employees to employers. On the one hand, the strength of the control dynamically varies between the company and employees in the internal knowledge transactions. On the other hand, continuous R&D also happens in the transactions of information between companies and employees.

In Figure 1, "root" is the root of the decision tree is a unit of creative technical information (T). "Target nodes," represented by the circle nodes at the end of each path of the decision tree, describe the possible existing forms of the creative technical information from the perspective of the employer. When the company controls the information, it can become a part of a patent (P_1), be placed in the public domain (D), or be treated as a trade secret and be used in the current/1st-generation product or producing process (P_2), in the second generation product or producing process (P_3), to send signals to competitors, consumers, or investors (P_4), or with no specific goals (P_5). When an employee inventor controls the information, the information can be transferred to the company and achieve the above targets or be remained with the employee as information asymmetries. The employee can retain control of the information in the form of deadweight loss (L) or transfer the information to others. The employer's direct competitors can use the information as the company's homogeneous product (H_1). The company's non-direct competitors can use the information as the company's

[48] *See* JEAN TIROLE, THE THEORY OF CORPORATE FINANCE 389 (2006) (discussing the allocation of control rights of shares between outsiders and insiders).

heterogeneous product (H_2). Finally, "decision nodes," represented by the rectangles in Figure 1, represent uncertainties to be explored by the company and decisions to be made by the company or the employee inventor. When the company and the employee explore legal uncertainties or make transaction decisions, there are costs posted. The costs vary with *T*, the company's intellectual property (IP) management, the employment contracts, and the employee's education, knowledge, experience, and skills.

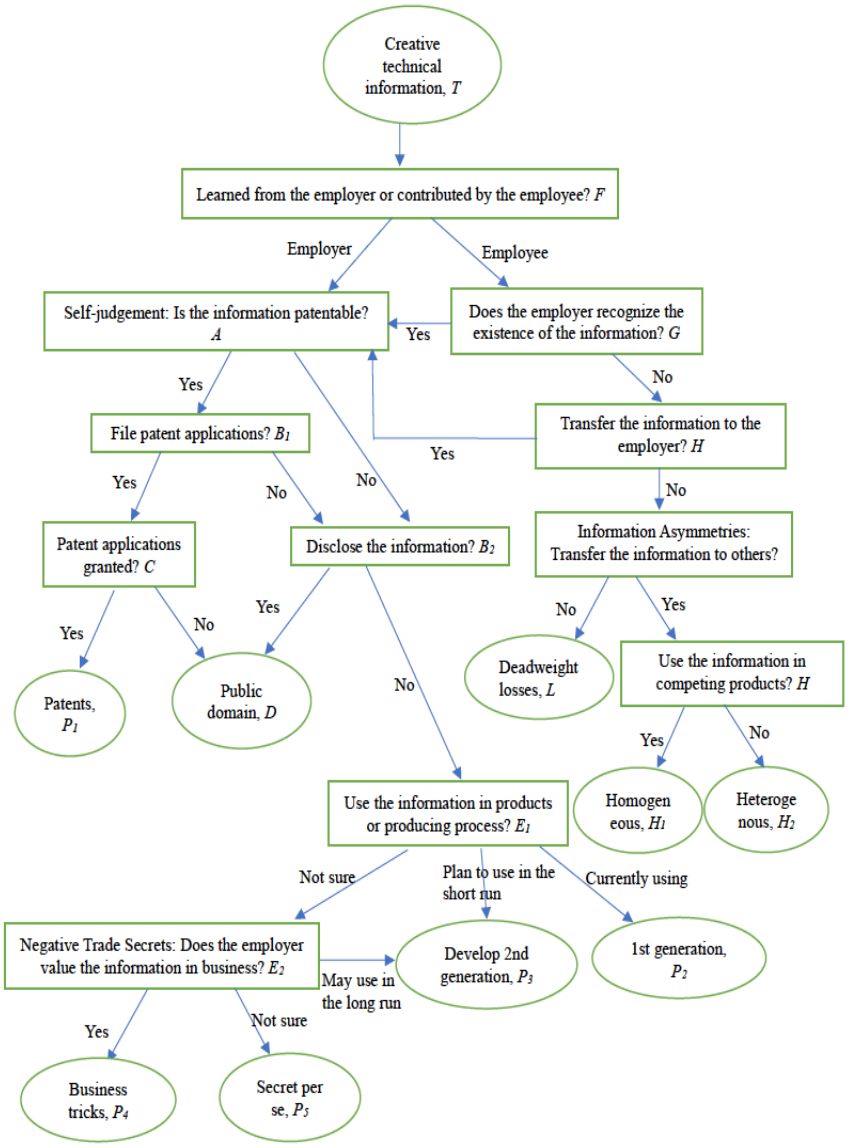

Figure 1. Technical Information Transactions Between the Company and Employee Inventors.[49]

[49] The logic of this theoretical figure is originated by the author and expressed in a serious of studies. This figure focuses on the flow of information transactions and is another expression of the information accessibility by the public, which is expressed in Figure 1 in Runhua Wang, Information Asymmetry and the Inefficiency of Informal IP Strategies Within Employment Relationships 15 (May 20, 2020) (unpublished manuscript) (on file with author).

A. Phase I Knowledge Transactions: from Companies to Employees

The internal transactions of technical information from companies to employees who do not create the information are a process of training. Companies have the incentives to disclose the technical information to these employees to use in production or marketing or further develop the information in R&D.[50] In internal transactions, the information control held by companies is not stable, depending on the information's existing forms. If a company holds the information, and the information exists in a patent or in the public domain, the company has absolute control of the information.[51] When employees can access or learn the information that is not publicly available, the company has relative control over the information because of the risks of unauthorized information leakage by employees.[52] The company considers disclosure risks in its translations of technical information with its employees.

1. Public Information

Companies have control over the public technical information only when the information is under patent protection.[53] Filing patent applications is the primary way that an information holder discloses its technical information.[54] A reasonable information holder maximizes his income received from the information.[55] Thus, the information holder is hardly able to disclose its information for free.[56] Patent law allows patent holders to be compensated from the market and provides patent holders at least first-mover advantages.[57] When patent applications are rejected, or patents have expired, the technical information embedded in the patent

50 *See* Lemley, *supra* note 28 at 332.

51 *See* 35 U.S.C. § 261 (2020).

52 *See* Png, *supra* note 25, at 1–3.

53 *See* 35 U.S.C. § 261.

54 *See* WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 359-363 (2003).

55 ROBERT COOTER & THOMAS ULEN, LAW AND ECONOMICS 12–13 (6th ed. 2012).

56 *See* Bhattacharya & Guriew, *supra* note 35, at 1115 (suggesting the nature of knowledge in business is to sell the knowledge). *But see* Schmidt, *supra* note 26 (suggesting the benefits of a marketing stunt after open innovation).

57 *See* Levine & Sichelman, *supra* note 27, at 755.

applications or patents drops in the public domain passively.[58] The information holder then loses its control of the information.

Companies do not prohibit, but rather encourage, internal transactions of their technical information if the information is under patent protection.[59] Employees need to use the information when conducting their work, which gives companies incentives to reduce the learning costs of the information for employees. Moreover, it is a common strategy for companies to protect their technical information against employees by filing patent applications.[60] Regardless if outsiders learn the information through employees, the company that is a patent holder can protect the information by suing for patent infringement.[61]

Patents, however, are a limited exiting form of much technical information. First, the technical information should be qualified as patentable subject matter; it must be within the scope of "process, machine, manufacture, or composition of matter."[62] However, besides this fundamental barrier, the scope of patent protection is not clear.[63] Second, patents are expensive in application, maintenance, and litigation.[64] If a patent cannot bring enough revenue or investment to offset the costs of patent application and maintenance, small businesses hesitate to file patent applications but prefer trade secrets to patents.[65] Third, companies do not

58 *See* 35 U.S.C. §§ 122, 371.

59 *See* Lemley, *supra* note 28.

60 April M. Franco & Matthew F. Mitchell, *Covenants Not to Compete, Labor Mobility, and Industry Dynamics*, 17 J. ECON. & MGMT. STRATEGY 581, 603 (2008).

61 35 U.S.C. § 271.

62 35 U.S.C. § 101 (1952). The European Patent Office ("EPO") does not provide patent protection for discoveries; scientific theories; mathematical methods; aesthetic creations; schemes; rules and methods for performing mental acts; playing games or doing business, and programs for computers; and presentations of information if patent applications do not have other technical features. *See* The European Patent Convention, art. 52, June 2016, Eur. Patent Conv. *See also* 2019 Revised Patent Subject Matter Eligibility Guidance, 84 Fed. Reg. 50, 52 & 57 (Jan. 7, 2019) (defining mathematical concepts, certain methods of organizing human activity, and mental processes as "abstract ideas," which are hardly subjective to patent eligibility).

63 *See* Lerner, *supra* note 17, at 7. *See generally* Alice Corp. v. CLS Bank Int'l, 573 U.S. 208 (2014) (blurring the boundaries of patentable subject matters by vague language in the court decision).

64 *See* Suzanne Scotchmer & Jerry Green, *Novelty and Disclosure in Patent Law*, 21 RAND J. ECON. 131 (1990). *See also* Douglas C. Lippoldt & Mark F. Schultz, *Uncovering Trade Secrets - An Empirical Assessment of Economic Implications of Protection for Undisclosed Data* 9 (OECD Trade Policy Papers No. 167, 2014); Almeling, *supra* note 15, at 1116; Lerner, *supra* note 17, at 5.

65 *See* Anthony Arundel, *The Relative Effectiveness of Patents and Secrecy*

use patents to protect valuable inventions for not disclosing the inventions.[66] Most advanced technologies are protected under trade secrets.[67] Moreover, survey data suggest that companies use trade secrets more often than patents.[68]

2. Unpublished Technical Information

When the technical information held by a company is not publicly available, the company treats it as trade secrets.[69] The company can affirmatively use the technical information in its first-generation products, the production of the first-generation products (P_2), or the development of the second-generation products (P_3). Alternatively, the technical information can be deployed as negative trade secrets, advertised as business tricks (P_4), or deposited as a secret per se (P_5) by the employer.[70] Even though negative trade secrets are not activated by the information holder in its products or production, business tricks deter competitors or

for Appropriation, 30 RES. POL'Y 611, 613 (2001); Nishant Dass et al., *Intellectual Property Protection and Financial Markets: Patenting vs. Secrecy* 4 (May 19, 2015), http://www.law.northwestern.edu/research-faculty/clbe/events/innovation/documents/DassNandaXiao.pdf; Levine & Sichelman, *supra* note 27, at 763–64; Lemley, *supra* note 28, at 331. *But see* Josh Lerner, *Patenting in the Shadow of Competitors*, 38 J. L. & ECON. 563 (1995); Lerner, *supra* note 17, at 4; Anton & Yao, *supra* note 17, at 3 (arguing that small innovations should be all protected under patents).

66 *See* Bhattacharya & Guriev, *supra* note 35, at 1117, 1142.

67 Sandeen & Levine, *supra* note 25, at 352–53.

68 *See* John Kitching & Robert Blackburn, *Intellectual Property Management in the Small and Medium Enterprise (SME)*, 5 J. SMALL BUS. & ENTERPRISE DEV. 327, 329–32 (1998) (showing British SMEs prefer trade secrets to patents by survey data); Linton, *supra* note 14, at 6. *See*, *e.g.*, Trade, Investment, & Industrial Policies in India: Effects on the U.S. Economy, Inv. No. 332-543, USITC Pub. 4501, at *140 (Dec. 2014) (showing that trade secrets are more important to US "internationally-engaged" companies than patents, copyrights, and trademarks by survey data); Stuart J. H. Graham et al., *High Technology Entrepreneurs and the Patent System: Results of the 2008 Berkeley Patent Survey*, 24 BERKELEY TECH. L.J. 1255, 1310 (finding that one-third of people do not file patent applications for preventing technology disclosure).

69 *See* Lippoldt & Schultz, *supra* note 64, at 6 (categorizing three types of trade secrets, including technical information, confidential business information, and know-how). Know-how is considered as a type of technical information in this research. *Id.*

70 *See* Bhattacharya & Guriev, *supra* note 35, at 1115 (suggesting no incentives for companies to disclose their knowledge for free). *See also* Michael A. Epstein & Stuart D. Levi, *Protecting Trade Secret Information: A Plan for Proactive Strategy*, 43 BUS. LAW. 887, 887–88 (May 1988) (categorizing trade secrets as trade secrets used in business, trade secrets providing a competitive advantage, or trade secrets as secrets per se).

suggest values to competitors or alliances.[71] By contrast, the deposited secrets per se sleep and do not suggest any imminent economic value.[72] Overall, keeping the technical information in secret may maximize the net present value of the technical information.[73]

The transaction of unpublished technical information from companies to employees who do not create the information is a process of training regardless of whether this process has the value of R&D, production, or marketing. Employees cannot learn technical information that is a trade secret unless the company trains them. On the one hand, employees have incentives to learn the knowledge and reduce the training costs for companies.[74] On the other hand, the training costs are not zero due to the costs of opaque information and increase as the company increases the opacity and keeps the information secret.[75]

The concerns about spillovers of unpublished technical information prevent companies from training employees with unpublished technical information. After employees have access to technical information, knowledge spillovers are reducible but inevitable due to the difficulties and high costs in keeping knowledge in secrets.[76] Employee mobility and employee-involved external communications may trigger knowledge spillovers.[77] Spillovers create potential competitors[78] and are losses to companies.[79] Survey data show that departing employees are

71 *See* Dass et al., *supra* note 65, at 22 (criticizing the inefficient information asymmetry resulted from trade secrets).

72 *See* Michael Risch, *Why Do We Have Trade Secrets?*, 11 MARQ. INTELL. PROP. L. REV. 1, 22, 32 (2007) (suggesting that secret information itself as secrecy has value).

73 *See* Schwartz, *supra* note 31, at 664 (reasoning from the perpetuity of trade secrets and corporations).

74 *See* Png, *supra* note 25, at 20 (suggesting that employees make tradeoffs between low wages and training in their early-career stages).

75 *See* Dass et al., *supra* note 65, at 1 (suggesting the costs of opacity and the costs of trade secrets).

76 *See* Schmidt, *supra* note 26, at 6.

77 *See* Png, *supra* note 25, at 1–3 (suggesting less employee mobility equals fewer knowledge spillovers between employers).

78 *See* Paavo Ritala et al., *Knowledge Sharing, Knowledge Leaking and Relative Innovation Performance: An Empirical Study*, 35 TECHNOVATION 22, 24 (2015) ("[Knowledge leakage]. . .creates new competitors for the original knowledge owner."). *See also* C. Christopher Baughn et al., *Protecting Intellectual Capital in International Alliances*, 32 J. WORLD BUS. 103, 104 (1997) ("Uncontrolled information disclosure . . . possibly help[s] to create a future competitor.").

79 *See* Bhattacharya & Guriev, *supra* note 35, at 1115 (suggesting spillovers are against trade secrets and business principles of maximizing profits).

"the biggest threat of loss" to British companies.[80] Therefore, training or information disclosure to employees increases the risks of spillovers and opportunity costs.[81] As a result, employers may overinvest in secrecy and block their unpublished technical information from their employees.[82]

B. Phase II Knowledge Transactions: from Employees to Companies

Besides being a receiver of knowledge trained by a company, an employee is also a creator of knowledge and technical information. Regardless of the controversial question of who owns the technical information produced by an employee during employment,[83] the employee has the absolute control of the technical information before its disclosure to the company.[84] Strategically, the employee can either transfer the technical information to the company or outsiders, or not disclose it at all, which is a deadweight loss to society (*L*).

If the technical information can be exchanged for value, a reasonable employee should have incentives to transfer it to his employer or outsiders (i.e., another employer or a start-up), rather than keep it as a deadweight loss (i.e., *L*). Employees expect internal and external career advancement by being innovative and producing valuable technical information.[85] After an employee has disclosed the technical information

80 *See* Levine & Sichelman, *supra* note 27, at 780; Kitching & Blackburn, *supra* note 68, at 329.

81 *See* Gilson, *supra* note 41, at 601 ("[T]he earlier in the invention process an employee must make the decision to undertake a start-up, the riskier is the employee's human capital investment in the venture.").

82 *See* Lemley, *supra* note 28, at 334 (discussing overinvestment in secrecy by companies without trade secret law). *See also* Friedman et al., *supra* note 22, at 68 (balancing the public and private costs of precautions against theft of trade secrets).

83 *See generally* JOHN LOCKE, TWO TREATISES OF GOVERNMENT (1689). Locke's labor theory suggests that laborers own the property rights of what they produce and should be able to control the fruits of their labor. *See id.* IP scholars criticize this theory and believe that IP law is utilitarian and preempts the personal interests of the laborers. *See* Wendy J. Gordon, *A Property Right in Self-Expression: Equality and Individualism in the Natural Law of Intellectual Property*, 102 YALE L. J. 1533, 1540, 1608 (1993); Bone, *supra* note 21, at 283–88.

84 *See* James J. Anton & Dennis A. Yao, *Expropriation and Inventions: Appropriable Rents in the Absence of Property Rights*, 84 AM. ECON. REV. 190, 191 (1994) (suggesting that only inventors know the value of their inventions). Even though technical information is more than an idea, it is not practical for employers to monitor and react to every word that employees write on notebooks or save on computers.

85 *See* Contigiani et al., *supra* note 30, at 2938 (stating "[career

to his employer, there are litigation risks (e.g., trade secret misappropriations) if the employee transfers the technical information to others. Therefore, in theory, an employee should have stronger incentives to transfer the technical information to his employer rather than to outsiders.

Employees, however, have limited incentives to transfer the technical information produced by them to their employers. Employees make tradeoffs between learning or receiving economic and reputational payments from companies.[86] They learn from companies in the early career stage and accept low payments as the investment to the learning.[87] After learning in Phase I transactions, they look for better payments for their knowledge or the technical information produced by them from companies or outsiders.[88] Companies can incentivize employees to transfer knowledge to companies by increasing the compensation employees receive.[89] However, companies may not increase the compensation because of the investment in training the employees in Phase I transactions.[90] As a result, employees have few incentives to produce valuable technological information when they encounter both low payments and few external opportunities.[91]

It is problematic that many companies do not realize the importance of Phase II transactions of technical information from employees to employers.[92] Large companies with a big pool of knowledge do not rely on the knowledge contributed by particular employees.[93]

advancement] . . . may depend on both internal-to-the firm and external career paths").

86 *See* Png, *supra* note 25, at 19.

87 *See* Jarle Moen, *Is Mobility of Technical Personnel a Source of R&D Spillovers?*, 23 J. LAB. ECON. 1, 2 (2000) (showing "the youngest workers appear to invest most heavily in on-the-job learning" by empirical evidence).

88 *Id.* at 20. *See also* Fosfuri & Ronde, *supra* note 31, at 47–48 (suggesting that high-value information and high wage offered from externalities increase mobility).

89 *See* Png, *supra* note 25, at 20 ("By reducing such outside opportunities, trade secrets law might force employers to increase compensation.").

90 *See* Jonathan M. Barnett & Ted M. Sichelman, *Revisiting Labor Mobility in Innovation Markets* 3 (Univ. S. Cal. L. Sch. Legal Studies Research Papers Series, Paper No. 207, 2016), https://pdfs.semanticscholar.org/df2e/ca68c18dfcde41c754697de86e00f1f822c7.pdf (showing that low wages are paid to employees for the training costs of employers).

91 *See* Png, *supra* note 25, at 19–20 (suggesting that employees invest them less if they would have fewer external opportunities).

92 *See id.* at 19 (arguing that companies do not understand the importance of human capital investment on their R&D).

93 *See id.*

Small companies may not be able to produce valuable R&D.[94] However, a company itself does not produce any technical information, which is all transferred from its employees.[95] The technical information transferred from employees to companies reflects the innovation efforts produced by the employees, which are expected by companies.

C. Problems of Information Asymmetries

Information asymmetries always exist in Phase I and Phase II information transactions between companies and employees.[96] First, when a company controls a unit of technical information and trains its employees with the information, the company is incapable of knowing how much the employees actually learn.[97] Second, the company is incapable of knowing how valuable the information originated from employees will be.[98] When information is originated from employee inventors, the company is passive to access that information.[99]

The first type of information asymmetries result in direct losses or deadweight losses to the company if the employee inventor discloses the information to others without authorization from the company. The unauthorized information disclosure results in a direct loss when others use the information and produces products or services competing with the company's first and second-generation products or services. The disclosure results in deadweight losses to the company if others profit from the information in other ways.

The second type of information asymmetries is deadweight losses to the company. If the employee inventor does not disclose the information to outsiders (i.e., *L*), the information is treated as a deadweight loss to society. If the information could be valuable to the company and

94 *See id.* at 20.

95 *See* Bhattacharya & Guriev, *supra* note 35, at 1116 (suggesting that knowledge buyers do not produce ideas).

96 Michael C. Jensen & William H. Meckling, *Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*, 3 J. FIN. ECON. 305, 308 (1976) (stating information asymmetry exists in agency relationships, which are contracts "under which one or more persons (the principal(s)) engage another person (the agent) to perform some service on their behalf which involves delegating some decision -making authority to the agent.").

97 *See* Franco & Mitchell, *supra* note 60, at 583.

98 *See* Png, *supra* note 25, at 9 (suggesting that employers can never understand the value of the inventions of employees the same way the employees do).

99 *See* Schwartz, *supra* note 31, at 666 (suggesting that the nature of secret information is information asymmetry in the transactions between the information holder and its investors).

protected under patents P_1[100] or used in the company's first/second-generation products or producing the products (i.e., P_2 or P_3), the adverse-selection problem arises. Alternatively, the employee inventor may transfer the information to outsiders, such as a spin-out startup,[101] new employers, or other companies. Homogenous products H_1 and heterogeneous products H_2 produced by using the information result in a loss to the company because it could be profited from the products (i.e., H_1 and H_2). Between the two types of loss, the loss of the technical information producing homogenous products H_1 is larger due to the harm on the company's current market share. The lost profits caused by transferring the technical information to outsiders suggest a moral-hazard problem resulting from information asymmetries.[102]

With respect to this moral-hazard problem, employees have both abilities and motivations to transfer their creative technical information to outsiders,[103] even though employers expect loyalty from employees.[104] A piece of technical information resulting from an employee's intelligence has an unbalanced value to the employee inventor and his employer. First, the employee values the technical information produced by him higher than the company.[105] Second, the information can be undervalued by the

100 Franco & Mitchell, *supra* note 60, at 585 (arguing that there are companies that file patent applications to protect information and prevent information disclosure by employees).

101 Spin-out startups are formed by employees based on their own decisions; employees form spin-off startups as a choice of employers. *See id.* at 582.

102 *See generally* Drew Fudenberg & Jean Tirole, *Moral Hazard and Renegotiation in Agency Contracts*, 58 ECONOMETRICA J. ECON. SOC'Y 1279 (1990).

103 *See* Manuel Trajtenberg & Roy Shalem, *Software Patents, Inventors and Mobility*, SSRN 101, 145 (2009), https://poseidon01.ssrn.com/delivery.php?ID=454026098004121084018109106090015093000085002012023032095093074109069087095002119006057018122039107109012091107120022029068078025094036037013093100072097072104005067012046083067009071127121086124028095115098007112004004016027004112119102096006086084&EXT=pdf (suggesting that asymmetric information is the main incentive for job mobility of inventors); YEH, *supra* note 18, at 15 (listing the motivations of trade secret thefts, which include personal financial gain).

104 Lemley, *supra* note 28, at 335.

105 An information holder values its information higher than the buyers of the information. In the training story, an employer is the information holder and values their training more than the contributions and efforts done by its employees. In the information asymmetry story, an employee values his or her intelligence higher than how much the employer compensates him or her for producing the technical information. *See* Risch, *supra* note 72, at 35 (suggesting that people overvalue what they produce or own).

company before information disclosure.[106] Because of the costs of training employees, the company pays relatively lower compensation to employees compared to the value that the employees contribute to the company.[107] Third, employees can be compensated more from outsiders than the company.[108] The value of the technical information received from employees also depends on how the company manipulates and deploys the information in business.[109]

The moral-hazard problem can also result in the problem of reverse selection.[110] When the negotiation power of employees is weak against the company, employees are less likely to disclose and transfer the technical information produced by them on the employment position to the company.[111] During their employment, they may not transfer the information to outsiders; the information is treated as a deadweight loss to the society (i.e., *L*).[112] After their mobility, they may use the information with a new employer or a spin-out startup, exposing the moral-hazard problems.[113]

III. Trade Secret Protection Governed by Contracts and Trade Secret Law

The primary measures of trade secret protection include physical restrictions, contracts, and trade secret law. The literature suggests that trade secret protection enables companies to disclose knowledge and secret technologies to employees.[114] Physical security measures are costly and prohibit technical information disclosure from companies to

106 *See* Png, *supra* note 25, at 9.

107 *See* Barnett & Sichelman, *supra* note 90, at 3.

108 *See* Bhattacharya & Guriev, *supra* note 35, at 1113 (suggesting the value of knowledge spillovers to innovation).

109 *See* Lemley, *supra* note 28, at 336 (arguing that secret information can be developed to have a higher value by externalities under Arrow's Paradox).

110 S*ee generally* Jean-Jacques Laffont & Jean Tirole, *Adverse Selection and Renegotiation in Procurement*, 57 REV. ECON. STUD. 597, 597 (1990).

111 Anton & Yao, *supra* note 84, at 192 (arguing that the inventor's weak negotiation power results in non-disclosure of his or her invention or spin-out startups).

112 *See* Lemley, *supra* note 28, at 335–36.

113 *See* YEH, *supra* note 18, at 14.

114 *See generally* Lemley, *supra* note 28, at 319–20.

employees.[115] By contrast, the other two approaches of trade secret protection reduce the social costs of information disclosure.[116]

The primary civil law dealing with trade secret misappropriations is contract law (e.g., the law about enforcing CNCs and NDAs), the Restatement (First) of Torts, the Restatement (Third) of Unfair Competition, and trade secret law (i.e., the UTSA, the DTSA, and relevant common law doctrines).[117] In general, scholars agree that trade secret protection under trade secret law can spur R&D.[118] Empirical evidence supports that the enactment of the UTSA and strong enforcement of trade secret law are positively related to R&D investment by large businesses, especially in high-tech industries.[119] This Part introduces the trade secret statutory law and the common law supplementing the statutes in trade secret protection and discusses their uncertainties.

A. Employment Contracts

There are mainly two types of employment contracts governing the security of technical information. One type is CNCs, and the other type is NDAs. Both types of contracts can prevent knowledge spillovers caused by employee mobility. Before the beginning of developing trade secret-specific law in common law in the late-nineteenth century, companies and courts relied only on these two types of agreements to protect trade secrets.[120] These agreements are still used by companies to

115 *See* Epstein & Levi, *supra* note 70, at 897–98 (listing common "affirmative steps" to keep information secret, such as locking gates, using security orders to distinguish employees, marking employees by asking them to wear security badges).

116 See Lemley, *supra* note 28, at 335; Lippoldt & Schultz, *supra* note 64, at 7–8 (suggesting that trade secret protection increases R&D investment).

117 *See* Almeling, *supra* note 15, at 1106 (suggesting that even though trade secret law varies by states and the federal level, the UTSA is a template for the various trade secret laws). *But see* 18 U.S.C. § 1836 (West 2016); RESTATEMENT (FIRST) OF TORTS §§ 757–59 (Am. Law Inst. 1939); RESTATEMENT (THIRD) OF UNFAIR COMPETITION §§ 39–45 (Am. Law Inst. 1995); Christopher Rebel J. Pace, *The Case for a Federal Trade Secrets Act*, 8 HARV. J. L. & TECH. 427, 428 (1995) (arguing that trade secrets should be subject to property law, rather than tort law); LANDES & POSNER, *supra* note 54, at 355 (arguing that trade secret law is not independent of the liabilities under contract law and tort law).

118 Lemley, *supra* note 28, at 326.

119 *See generally* I.P.L. Png, *Law and Innovation: Evidence from State Trade Secrets Laws*, 99 REV. ECON. & STAT. 167 (2017).

120 *See* Bone, *supra* note 21, at 251–52 (citing Peabody v. Norfolk, 98 Mass. 452 (Mass. 1868)) (highlighting Peabody v. Norfolk as the starting point of having trade secret common law).

secure technical information and complement or supplement the protection under trade secret law. CNCs are employee-based, and NDAs are information-based to restrict employee mobility and secure technical information transactions within a company. These two types of contracts are primarily governed by common law but are also governed by state statutes.[121]

1. Covenants Not to Compete

CNCs encourage Phase I transactions of technical information from companies to employees.[122] Employee mobility is the primary reason for knowledge spillovers.[123] Even though CNCs may not directly address confidential information, employers can use CNCs to retain valued employees and reduce employee mobility.[124] Furthermore, CNCs can reduce the risks of spillovers and prevent the losses and opportunity costs resulting from information transfers from employees to outsiders.[125] By preventing spin-outs, CNCs are used to prevent competition by startups.

Courts allow the enforcement of CNCs restrictively under two elements: (1) the necessity of enforcing the CNC; and (2) the reasonableness of the restraints in the CNC.[126] The enforcement of CNCs should be necessary to protect the legitimate business interests of employers,[127] which specifically refer to trade secrets, confidential information, and goodwill.[128] With respect to the reasonableness, courts usually consider the restrictions on time and geographical scope in CNCs.[129] For example, Texas courts require consideration for

121 Png, *supra* note 25, at 8.

122 *See* Barnett & Sichelman, *supra* note 90, at 3 (suggesting that CNCs promote training employees by employers).

123 Epstein & Levi, *supra* note 70, at 890.

124 Procter & Gamble Co. v. Stoneham, 747 N.E.2d 268, 276 (Ohio Ct. App. 2000) ("The [trial] court also stated that the non-competition covenant was 'not being used to protect confidential information, but it is used as a measure to retain valued employees.'").

125 Gilson, *supra* note 41, at 602–03.

126 *See, e.g.*, Boulanger v. Dunkin' Donuts Inc., 815 N.E.2d 572, 576–77 (Mass. 2004).

127 *Id*. at 576–77 ("A covenant not to compete is enforceable only if it is necessary to protect a legitimate business interest, reasonably limited in time and space, and consonant with the public interest.").

128 *See* Marine Contractors Co. v. Hurley, 310 N.E.2d 915, 920 (Mass. 1974).

129 *E.g.*, *Boulanger*, 815 N.E. at 576–77.

establishing reasonableness[130]; New York courts weigh the losses of employers against the restraints on employees, which should not be higher than the former[131]; and Georgia law adds that CNCs are only restricted to "key employees."[132] As a typical example, an enforceable CNC in Wisconsin is as follows:

> Upon termination of this Agreement, [employee] shall not participate in any way, directly or indirectly, either through direct or indirect ownership, employment or otherwise, in any business which deals with or relates to products or services which are the same or similar to those manufactured and/or sold by [employer] *in the field of fine chemistry, pharmaceuticals and electronic components, for a period of one year in the American continents and Japan*. In addition, [employee] shall cease all contacts with any existing or prospective customers of [employer] as well as with its suppliers, provided that [employee] may maintain such contacts in the pursuit of business not competing, whether directly or indirectly, with that of [employer].[133]

While the above examples show that CNCs are unlikely to be unconditionally enforceable, CNCs are not consistently enforceable in the U.S., either. PBC News Hour reports that about 40% of Americans have signed CNCs, but only about 20% of the CNCs are binding.[134] Some states that have "anti-CNC" statutes to govern unfair competition and the freedom of employment disfavor or constrict the use of CNCs,[135] such as

130 *See generally* Powerhouse Prods. v. Scott, 260 S.W.3d 693 (Tex. App. 2008).

131 *See* BDO Seidman v. Hirshberg,712 N.E.2d 1220, 1223 (N.Y. 1999) ("A restraint is reasonable only if it: (1) is no greater than is required for the protection of the legitimate interest of the employer, (2) does not impose undue hardship on the employee, and (3) is not injurious to the public.").

132 GA. CODE ANN. § 13-8-50 (West 2011).

133 La Calhene, Inc. v. Spolyar, 938 F. Supp. 523, 526 (1996).

134 Kristen Doerer, *What You Should Know About Noncompete Agreements*, PBS (July 14, 2016 6:11 PM), https://www.pbs.org/newshour/economy/know-non-compete-agreements.

135 *Noncompete Reform Continues in New England: Maine, New Hampshire, and Rhode Island All Pass New Laws*, FISHER PHILLIPS: NON-COMPETE & TRADE SECRETS BLOG (July 17, 2019), https://www.fisherphillips.com/Non-Compete-and-Trade-Secrets/noncompete-reform-continues-in-new-england-maine (reporting that Massachusetts, Maine, New Hampshire, and Rohde Island recently passed laws to prohibit

California,[136] Illinois,[137] and Oregon.[138] It does not mean that CNCs are strictly voided in these states,[139] but rather less likely enforceable. By contrast, some states have "pro-CNC" statutes that authorize the use of CNCs, such as Massachusetts,[140] Michigan,[141] North Carolina,[142] and Texas.[143] However, these statutes set restrictions in drafting CNCs[144] or do not guarantee the enforceability of CNCs in courts.[145] Moreover, despite the statutes that protect employers in Michigan, Michigan state courts disfavor CNCs.[146] In other states (e.g., New York) without statutes to void CNCs, the courts may still reject CNCs for the considerations of public policies.[147]

2. Non-Disclosure Agreements

enforcing CNCs against low-wage employees). *See also* Barnett & Sichelman, *supra* note 90, at 3 ("[S]everal state legislatures have enacted laws or are considering enacting laws to prohibit or restrict noncompetes.").

136 *See*, *e.g.*, CAL. BUS. & PROF. CODE. §16600 (West 2020) ("Except as provided in this chapter, every contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."); CAL. LAB. CODE § 2802 (West 2016); Ixchel Pharma, LLC v. Biogen Inc., Civ. No. 2:17-00715, 2018 U.S. Dist. LEXIS 13548, at *12–13 (Jan 25, 2018) (prohibiting non-compete agreements for unfair competition under antitrust law).

137 *See* 820 ILL. COMP. STAT. 90/10 (2017).

138 *See* OR. REV. STAT § 653.295 (2019).

139 *See*, *e.g.*, Edwards v. Arthur Andersen LLP, 189 P.3d 285, 289–90 (Cal. 2008) (permitting CNCs as exceptions of §16600 if reasonableness is established). *See also* Gilson, *supra* note 41, at 607–09 (noting that there could be cases allowing CNCs in California, even though CNCs are commonly not applicable in California).

140 MASS. GEN. LAWS. ch. 149 § 24L (2018).

141 MICH. COMP. LAWS ANN. § 445.774a (West 1985).

142 N.C. GEN. STAT. ANN. § 75-4 (West 2005).

143 TEX. BUS. & COM. CODE ANN. § 15.50 (West 2009).

144 *See*, *e.g.*, MASS. GEN. LAWS ANN. ch.149, § 24L (West 2018). The statutes in Massachusetts establish minimum standards for valid and enforceable CNCs.

145 For example, Massachusetts courts do not consistently enforce CNCs. *See* Gilson, *supra* note 41, at 603–07 (discussing the inconsistent application of CNCs in Massachusetts, where the courts favor CNCs in general).

146 *See*, *e.g.*, Huron Tech. Corp. v. Sparling, No. 316133, 2014 Mich. App. LEXIS 1675, at *6 (Mich. App. Sep. 11, 2014) (rejecting enforcement of the CNC because it is unreasonably broad).

147 *See*, *e.g.*, Shearson Lehman Bros. Holdings, Inc. v. Schmertzler, 500 N.Y.S.2d 512, 513 (N.Y. App. Div. 1986) ("[A] covenant given by an employee that he will not compete with his employer has been regarded much more strictly because of the powerful considerations of public policy which militate against sanctioning the loss of a man's livelihood . . . .").

In addition to CNCs, NDAs are another common measure to prevent and deter employees from disclosing confidential information to outsiders.[148] In employment relationships, NDAs—or confidentiality agreements—establish confidential responsibilities. Today, employment contracts usually include confidential provisions.[149] In other words, NDAs are usually signed at the beginning of establishing employment relationships. As a result, if the research is conducted during the employment, research results are confidential under NDAs regardless of when a research idea is generated.

Similar to CNCs on prohibiting employee mobility, NDAs are also a double-edged sword in innovation. On the one hand, NDAs crush startup competitors and deter competitors from hiring their employees or acquiring their confidential information.[150] On the other hand, NDAs deter companies from hiring talented employees from their competitors.[151]

Compared to CNCs, NDAs are more closely related to trade secret law. The foundation of trade secret protection in trade secret law is the privacy or confidentiality of trade secrets.[152] Holmes suggested that if a company cannot contain its technical information secret, trade secret law does not prohibit employees from revealing the information to others.[153] Samuelson followed Holmes and suggested that the nature of trade secret law is about "breach of confidence or use of improper means to obtain a trade secret."[154]

NDAs, however, do not necessarily create enforceable trade secrets.[155] First, NDAs may not be binding if the confidential information

148 Epstein & Levi, *supra* note 70, at 905.

149 Orly Lobel, *Symposium Keynote: The DTSA and the New Secrecy Ecology*, 1 BUS. ENTREPRENEURSHIP & TAX L. REV. 369, 377 (2017).

150 *Id.*

151 *Id.*

152 *See*, *e.g.*, E. I. du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012, 1014–17 (5th Cir. 1970) (excluding a concern of breach of confidence for policy reasons, such as promoting innovation). *See also* Bone, *supra* note 21, at 297.

153 E. I. Du Pont De Nemours Powder Co. v. Masland, 244 U.S. 100, 102–03 (1917).

154 Pamela Samuelson, *Information as Property: Do Ruckelshaus and Carpenter Signal a Changing Direction in Intellectual Property Law?,* 38 CATH. U. L. REV. 365, 374–75 (1989).

155 *See* Sharon K. Sandeen, *A Contract by Any Other Name Is Still a Contract: Examining the Effectiveness of Trade Secret Clauses to Protect Databases*, 45 IDEA 119, 124 (2005) ("A trade secret cannot be created by contract.").

does not constitute a trade secret.[156] If NDAs are not clear about what information is confidential, employers still lose their cases claiming breaches of confidentiality.[157] Scholars constantly criticize that NDAs could be interpreted too narrowly to get enforced and protect companies when courts only rely on common law.[158] Moreover, there are uncertainties that courts enforce or reject NDAs for policy reasons.[159] The policy reasons include, but are not limited to, promoting innovation and creation, reducing precaution costs, protecting privacy, and enforcing "standards of commercial ethics."[160] The failures of enforcing NDAs could constitute "security lapses," which result in failures to enforce trade secrets.[161]

In addition to NDAs, labor law and human capital law may function similarly to NDAs by strengthening the control of companies over the innovative contributions made by employees. Under the California Labor Code, employers can claim property rights on whatever employees produce in their employment due to the resources of the employers.[162] In *American Alloy Steel Corp. v. Ross*, the court ruled that trade secrets and confidential information, including the knowledge of employees obtained in these measures, are properties owned by employers.[163] Employees can use other information only after the termination of employment.[164] Companies do not hold property rights

156 *See id.* at 143 ("Where information is not a trade secret but constitutes confidential or proprietary information, it is argued that a party who contractually agrees to maintain the confidentiality of such information is bound to honor the contract.").

157 Epstein & Levi, *supra* note 70, at 905.

158 Risch, *supra* note 72, at 41.

159 *See* Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEG. STUD. 683, 689–90 (1980) ("Courts will accept these [confidentiality] agreements as evidence that the firm valued the information and attempted to preserve its secrecy, but they decide for themselves whether the information should actually be protected.").

160 *See* Bone, *supra* note 21, at 297. *See also* E. I. du Pont de Nemours & Co., 431 F.2d at 1016–17; Judge Richard Posner, Note, *Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy*, 106 HARV. L. REV. 461, 470–71 (1992).

161 Epstein & Levi, *supra* note 70, at 898.

162 CAL. LAB. CODE § 2860 (West 1988) ("Everything which an employee acquires by virtue of his employment, except the compensation which is due to him from his employer, belongs to the employer, whether acquired lawfully or unlawfully, or during or after the expiration of the term of his employment.").

163 Am. Alloy Steel Corp. v. Ross, 308 P.2d 494, 496–97 (Cal. Dist. Ct. App. 1957).

164 *Id.*

over the technical information[165] produced by employees but acquire property rights when the information constitutes trade secrets, which are kept in confidential and exclusive use.[166] Moreover, based on *Bd. of Trs. of the Leland Stanford Junior Univ. v. Roche Molecular Sys.*,[167] scholars like Lobel believe that employment relationships suggest a default and constant transfer of title of inventions from employees to employers.[168]

B. Trade Secret Law

The standard of trade secret protection widely accepted by most states originated from common law[169] and was formally added in the Restatement (First) of Torts in 1939.[170] This standard is substantially identical to the definition of trade secrets and the rules in the UTSA,[171] which the Uniform Law Commission sketched as statutory law in 1979.[172] In practice, empirical evidence showed that state courts often cite the

165 *See* Risch, *supra* note 72, at 14. *See also* E. I. Du Pont de Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917).

166 *See* Carpenter v. U.S., 484 U.S. 19, 25–27 (1987).

167 563 U.S. 776, 779 (2011) (holding that employers are assignees and owners of patents produced by using the sources of employers).

168 *See* Orly Lobel, *The New Cognitive Property: Human Capital Law and the Reach of Intellectual Property*, 93 TEX. L. REV. 789, 815 (2015) ("The 'automatic assignment' adopted by the Supreme Court has meant that an employment or assignment agreement signed at the beginning of employment automatically transfers title to the employer, with no further act of transfer required once those inventions are conceived and come into existence.").

169 *See* Brittany S. Bruns, *Criticism of the Defend Trade Secrets Act of 2016: Failure to Preempt*, 32 BERKELEY TECH. L. J. 469, 473 (2017). *See also* Peabody v. Norfolk, 98 Mass. 425 (Mass. 1868); Bone, *supra* note 21, at 251–59 (introducing how people and courts solve trade secret issues under property-based theory before the formation of the concept of trade secret and a separate trade secret law). Bone argues that trade secret protection discussed in Schiller's Article and the Roman Law is very different from today's trade secret law, so we do not trace the history of trade secret law to the Roman Law. *But see* A. Arthur Schiller, *Trade Secrets and the Roman Law: The Actio Servi Corrupti*, 30 COLUM. L. REV. 837 (1930), *in* A. ARTHUR SCHILLER, AN AMERICAN EXPERIENCE IN ROMAN LAW 1 (1971) (discussing the trade secret protection under the Roman Law).

170 *See* Victoria A. Cundiff, *Maximum Security: How to Prevent Departing Employees from Putting Your Trade Secrets to Work for Your Competitors*, 8 SANTA CLARA HIGH TECH. L. J. 301, 304 (1992).

171 *See id.* at 305 (introducing the definition of a trade secret in the UTSA, which is similar to the Restatement (Frist) of Torts). *See generally* Roman A. Klitzke, *The Uniform Trade Secrets Act*, 64 MARQ. L. REV. 277 (1980).

172 *See* Bruns, *supra* note 169, at 475.

UTSA but rarely cite Restatement (First) of Torts in trade secret disputes.[173]

All of the states, excluding North Carolina and New York, have voluntarily enacted the UTSA as of January 2020 to address trade secret protection,[174] rather than merely apply common law.[175] Even though the Uniform Law Commission does not list North Carolina as a state enacting the UTSA,[176] its trade secret law is close to the UTSA.[177] The trade secret law in New York also moves towards the UTSA.[178]

At the federal level, the DTSA enables civil claims for trade secret misappropriations to be a federal question of law since 2016.[179] It substantively aligns with the UTSA.[180] Therefore, trade secret law in this Article refers to how state courts and federal courts apply the UTSA, the DTSA, and relevant case law dealing with trade secret protection.[181]

In theory, scholars suggest that trade secret law is an efficient substitute for contractual and physical restrictions in trade secret protection.[182] First, trade secret law is consistent with tort theories to deter

173 David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in State Courts*, 46 GONZ. L. REV. 57, 61 (2011) ("Only 5% of the cases [between 1995–2009] cited the *Restatement (First) of Torts*.").

174 *See* UNIF. TRADE SECRET ACT (UNIF. LAW COMM'N 1985), https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 (last visited May 14, 2020).

175 *See* Almeling et al., *supra* note 173, at 76 (showing that most states that used common law were the states had not adopted the UTSA).

176 UNIF. TRADE SECRETS ACT (UNIF. LAW COMM'N 1985), https://www.uniformlaws.org/committees/community-home?CommunityKey=3a2538fb-e030-4e2d-a9e2-90373dc05792 (last visited May 14, 2020).

177 *See* SBUBHA GHOSH ET AL., INTELLECTUAL PROPERTY: PRIVATE RIGHTS, THE PUBLIC INTEREST, AND THE REGULATION OF CREATIVE ACTIVITY 10 (3rd ed., 2016).

178 Two bills were introduced in 2019 and proposed to adopt the UTSA. *See* H.R. 1657, 116th Cong. (2019); H.R. 2468, 116th Cong. (2019).

179 *See* Linton, *supra* note 14, at 8 ("The DTSA creates a federal civil cause of action for trade secret misappropriation."). Before the DTSA, only criminal claims for trade secret espionage qualified as a federal question under the Economic Espionage Act (EEA). Economic Espionage Act of 1996, Pub. L. No. 104–294, 110 Stat. 3488 (1996).

180 *See* Joseph P. Fishman & Deepa Varadarajan, *Similar Secrets*, 167 U. PA. L. REV. 1051, 1062 (2019). *See also* Sharon K. Sandeen & Christopher B. Seaman, *Toward a Federal Jurisprudence of Trade Secret Law*, 32 BERKELEY TECH. L. J. 829, 865–66 (2017); Lobel, *supra* note 149, at 380–81.

181 This Article does not address unfair competition legislation with respect to trade secret protection in the context of employment relationships.

182 *See* Lemley, *supra* note 28, at 313.

wrongful acts conducted by employees.[183] Second, trade secret law avoids overinvestment in secret protection by companies.[184] Third, it is also inefficient to frequently sue for CNCs or NDAs.[185] When courts hesitate to enforce contractual restrictions on employees, scholars suggest that companies should rely on trade secret law.[186] Moreover, applying common law to trade secret issues has a deficiency that courts do recognize the value of trade secrets, which is the secrecy itself.[187]

Under trade secret law, the primary test for bringing a civil claim of pursuing trade secret protection requires that a plaintiff establishes: (1) the existence of a trade secret; and (2) a misappropriation of the trade secret.[188] These two elements summarize the common rules in the Restatement (First) of Torts,[189] the UTSA,[190] and the DTSA.[191] In a broad sense, these three laws provide consistent definitions of trade secrets and misappropriations.[192] However, the two elements are applied with variations and uncertainties by state courts and federal courts when they apply the UTSA and the DTSA.[193]

In order to establish the first element, a trade secret should be novel, have independent economic value, and be maintained secretly with reasonable efforts.[194] With respect to the standard of independent

183 *Id.* at 319.

184 *Id.* at 334–35.

185 *See* Gilson, *supra* note 41, at 609.

186 *See* Levine & Sichelman, *supra* note 27, at 767 ("[T]rade secrets and patents can be used to mimic the preclusive effects of noncompetition agreements by creating significant penalties for bringing proprietary information to a new employer."); Barnett & Sichelman, *supra* note 90, at 9 ("A firm may use patents to protect against knowledge leakage through employee movement.").

187 *See* Risch, *supra* note 72, at 38, 41 (arguing that common law fails to create liabilities in all cases).

188 *See* Sandeen, *supra* note 155, at 126–27.

189 RESTATEMENT (FIRST) OF TORTS §§ 757–59 (Am. Law Inst. 1939).

190 UNIF. TRADE SECRET ACT (UNIF. LAW COMM'N 1985).

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

192 *See generally* Bruns, *supra* note 169 (discussing the uniformity and inconsistency of the DTSA and how states adopt the UTSA with variations).

193 *See generally id.*

194 18 U.S.C. § 1839(3) (2016).

> [T]he term "trade secret" means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and

economic value, Johnson summarized five tests adopted by courts, uniformly suggesting that a trade secret has "transferable and objective positive value."[195] With respect to novelty or the scope of trade secret protection, the UTSA and DTSA definition of a trade secret excludes the information "generally known" or "readily ascertainable" to others.[196] Nevertheless, this definition is still broad.[197] It could protect information that is not in continuous commercial use as trade secrets.[198] When states enact the UTSA, the definition of a trade secret may be further broadened. For example, the California UTSA (CUTSA) definition of a trade secret is broader than the UTSA,[199] as the CUTSA excludes the "readily ascertainable" restriction.[200]

> whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if . . . the owner thereof has taken reasonable measures to keep such information secret; and . . . the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information.

Id. *See* UNIFORM TRADE SECRETS ACT § 1(4) (UNIF. LAW COMM'N 1985).

> "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that . . . derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and . . . is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Id. *See also* Buffets, Inc. v. Klinke, 73 F.3d 965, 967-68 (9th Cir. 1996).

195 Eric E. Johnson, *Trade Secret Subject Matter*, 33 HAMLINE L. REV. 545, 547 (2010).

196 *See* 18 U.S.C. § 1839(3)(B) (2016); UNIFORM TRADE SECRETS ACT § 1(4)(i) (UNIF. LAW COMM'N 1985).

197 *See* Charles Tait Graves & Elizabeth Tippett, *UTSA Preemption and the Public Domain: How Courts Have Overlooked Patent Preemption of State Law Claims Alleging Employee Wrongdoing*, 65 RUTGERS L. REV. 59, 97–101 (2012); Bruns, *supra* note 169, at 481–82 (arguing that the DTSA definition of a trade secret is close to the UTSA definition of a trade secret).

198 *See* Johnson, *supra* note 195, at 563.

199 Bruns, *supra* note 169, at 478–79.

200 CAL. CIV. CODE § 3426.1(d) (West 2012). *See also* Abba Rubber Co. v. Seaquist, 286 Cal. Rptr. 518, 528 (Cal. Ct. App. 1991) ("[W]hether a fact is 'readily ascertainable' is not part of the definition of a trade secret in California.").

In high-technology industries, however, the scope of an applicable trade secret may be relatively narrow.[201] Courts may dismiss a trade secret case for the plaintiff's failure to identify the alleged trade secret under either the UTSA or the DTSA, regardless of which claim is raised by the plaintiff.[202] Moreover, "pre-conception inventions" are excluded from being entitled to trade secret protection.[203] Trade secret law is hardly enforced against intangible spillovers.[204] Besides high-technology industries, there are also "odd cases" applying a narrow definition of trade secrets.[205] For example, the Court of Appeals for the Ninth Circuit denied trade secret protection for literary works based on lack of novelty and non-obviousness,[206] which are the requirements for patent protection.[207]

Moreover, in the employment context, courts may define trade secrets narrowly for public policies.[208] The Restatement (First) of Torts states that "[m]atters of public knowledge or of general knowledge in an industry cannot be appropriated by one as his secret."[209] Courts and scholars also uniformly agree that general skills, education, abilities, and experience of employees, probably trained by employers, are not trade secrets.[210] The uncertainty of the boundary of this exclusion is that courts do not clearly understand what constitutes the unprotectable "general knowledge, skill, and experience" ("KSE"), resulting in inconsistent decisions.[211]

201 Camilla A. Hrdy, *The General Knowledge, Skill, and Experience Paradox*, 60 B.C. L. REV. 2409, 2466–71 (2019) (citing cases decided in California, Florida, and New York in which courts applied a "particularity" requirement and rejected to apply broad trade secret protection against employees).

202 *See, e.g.*, Mission Measurement Corp. v. Blackbaud, Inc., 216 F. Supp. 3d 915, 920 (N.D. Ill. 2016) (citing Illinois UTSA to reject the plaintiff's DTSA claim); Lobel, *supra* note 168, at 810–11 (discussing same).

203 *See* SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1266 (3rd Cir. 1985).

204 *See* Gilson, *supra* note 41, at 578.

205 Jay Dratler, Jr., *Trade Secrets in the United States and Japan: A Comparison and Prognosis*, 14 YALE J. INT'L L. 68, 102 n. 140 (1989).

206 *See* Walker v. Univ. Books, Inc., 602 F.2d 859, 865 (9th Cir. 1979) (supporting the district court that denied trade secret protection due to the "both vague and obvious" information).

207 *See* 35 U.S.C. §§ 102–03.

208 *See generally* Hrdy, *supra* note 201.

209 RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).

210 *See generally* Robert Unikel, *Bridging the "Trade Secret" Gap: Protecting "Confidential Information" Not Rising to the Level of Trade Secrets*, 29 LOY. U. CHI. L. J. 841 (1998) (trying to draw a boundary between "unprotectable 'general skill and knowledge'" and "protectable 'trade secrets'").

211 *See generally* Hrdy, *supra* note 201.

Therefore, legal professions constantly recommend the use of NDAs to companies in information disclosure.[212] Signing NDAs explicitly establishes the knowledge about the existence of trade secrets.[213] NDAs are referenced by federal courts to determine whether companies adopt reasonable measures of trade secret protection.[214] However, confidential information does not necessarily qualify as enforceable trade secrets.[215] NDAs are neither a sufficient nor a necessary condition for showing the existence of trade secrets.[216] Moreover, NDAs aggravate rather than eliminate the uncertainties about whether a duty of confidentiality is breached.[217]

With respect to the second element, in short, misappropriations refer to the disclosure or the use of the trade secrets that are acquired by improper means without consent from their holders.[218] Courts need only

212 *See*, *e.g.*, Epstein & Levi, *supra* note 70, at 904–05; Cundiff, *supra* note 170, at 309.

213 *See* Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir. 1953).

214 David S. Almeling et al., *A Statistical Analysis of Trade Secret Litigation in Federal Courts*, 45 GONZ. L. REV. 291, 294 (2010).

215 Bernier v. Merrill Air Eng'rs, 770 A.2d 97, 107 (Me. 2001) (affirming a breach of contract but denying trade secret misappropriation because the information lacks economic value). Risch cited this case to distinguish common law from trade secret law. *See* Risch, *supra* note 72, at 38.

216 *See* Risch, *supra* note 72, at 38.; Sandeen, *supra* note 155, at 140 ("[W]hile a confidentiality agreement is some evidence of reasonable efforts, it is not determinative of the issue); Johnson, *supra* note 195, at 566 ("A trade secret is not a heap of confidential information.").

217 *See* Bone, *supra* note 21, at 276–77 (arguing that trade secret law leads thieves to invest in concealing, which increases the investigation costs of trade secret owners).

218 UNIFORM TRADE SECRETS ACT § 1(2) (UNIF. LAW COMM'N 1985).

> "Misappropriation" means: (i) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who (A) used improper means to acquire knowledge of the trade secret; or (B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was (I) derived from or through a person who has utilized improper means to acquire it; (II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or (III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or (C) before a material change of his position, knew or had reason to know that it was a trade secret ad that knowledge of it had been acquired by accident or mistake.

to check the second element when plaintiffs show that there is a valid trade secret. "Improper means" include, but are not limited to, criminal and tortious behaviors,[219] such as breaches of an obligation of confidentiality.[220] "Improper means" can be established against employees who derive the information through the employers if they own the obligation, even though the employees acquire technical information by employers' voluntarily training.[221] The obligation of confidentiality can be either explicit in a contract or implicit by duty.[222] However, this obligation can be waived under public policies, such as fair competition and the freedom of employee mobility.[223] Moreover, the second element is restrictively applicable when courts recognize a piece of information as a valid and enforceable trade secret.[224]

Some states allow companies to tackle a "threatened misappropriation" under the IDD,[225] which is embedded in the UTSA. The UTSA broadly indicates that "[a]ctual or threatened misappropriation may be enjoined."[226] The DTSA also adopts this rationale completely.[227]

Id.

219 Besides the listed criminal and tortious behaviors in the UTSA and the DTSA, a behavior that is "not itself a crime, a tort, or a breach of contract" may constitute an improper means. *See* Sandeen & Seaman, *supra* note 180, at 908. *See also* E. I. du Pont de Nemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970).

220 UNIFORM TRADE SECRETS ACT § 1(2)(ii)(B)(III) (UNIF. LAW COMM'N 1985).

221 UNIFORM TRADE SECRETS ACT § 1(1) (UNIF. LAW COMM'N 1985).

222 *See* Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir. 1953).

> [T]he Supreme Court of Pennsylvania painted, in broad strokes, the general picture of a claim of this nature, holding the essential elements to be: (1) existence of a trade secret, (2) communicated to the defendant (3) while he is in a position of trust and confidence and (4) use by the defendant to the injury of the plaintiff. This, then, is our broad basis for decision.

Id. See also Lemley, *supra* note 28, at 318 (listing obligations of protecting trade secrets which can be explicit by contracts or implicit by duty).

223 *See* Hrdy, *supra* note 201, at 2413 n.27.

224 *See generally id.* at 2433–34 (discussing the scope of trade secret protection).

225 Randall E. Kahnke et al., *Doctrine of Inevitable Disclosure*, FAEGRE & BENSON 1 (Sept. 2008), https://www.faegrebd.com/webfiles/Inevitable%20Disclosure.pdf.

226 UNIFORM TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N 1985).

227 18 U.S.C. § 1836(b)(3)(A)(i) (West 2016).

An "inevitable disclosure" refers to "the threat that an employer's trade secrets will be misappropriated during the course of the employee's subsequent employment."[228] Therefore, without actual harms, courts may still grant injunctions against threatened harms or to restrict employee mobility by applying the IDD.[229]

The IDD's application in trade secret protection, however, is controversial and often connected with the controversially-applied CNCs.[230] The IDD's application is affected by public policies with respect to employee mobility and the freedom of employment.[231] The most influential case in which the court adopted the IDD is *PepsiCo v. Redmond*.[232] After this case, "[t]wenty-one American jurisdictions have recognized the [IDD]."[233] Even though some states adopt the IDD, the IDD is restrictedly applied by courts, such as in Missouri[234] and New Jersey.[235] Moreover, the IDD is inconsistently applied in some states, such as Florida, Indiana, and Illinois.[236] Appendix lists the adoption of the IDD and its consistency with CNCs and the IDD by states in detail, suggesting controversies across and within states.

IV. Risks of Disclosing Technical Information in Employment Relationships

Companies have marginal costs of information disclosure resulting from employee mobility or betrayal. The literature about

228 Ryan M. Wiesner, *A State-By-State Analysis of Inevitable Disclosure: A Need for Uniformity and a Workable Standard*, 16 MARQ. INTELL. PROP. L. REV. 211, 228 (2012).

229 *See, e.g.*, PepsiCo, Inc. v. Redmond, 46 F.3d 29 (7th Cir. 1995).

230 M. Claire Flowers, *Facing the Inevitable: The Inevitable Disclosure Doctrine and the Defend Trade Secrets Act of 2016*, 75 WASH. & LEE L. REV. 2207, 2217 (Fall 2018).

231 Eleanore R. Godfrey, *Inevitable Disclosure of Trade Secrets: Employee Mobility v. Employer's Rights*, 3 J. HIGH TECH. L. 161, 167 (2004).

232 *See Redmond*, 46 F.3d at *29.

233 Allot Commc'ns., Ltd. v. Cullen, No. 10-E-0016, 2010 N.H. Super. LEXIS 11, at *7 (N.H. Super. Ct. Feb. 7, 2010).

234 *See* H & R Block E. Tax Servs., Inc. v. Enchura, 122 F. Supp. 2d 1067, 1074 (W.D. Mo. 2000).

235 There is an inconsistency in between the application of IDDs by the 3rd Circuit and New Jersey state courts. *Compare* Cont'l Group, Inc. v. Amoco Chems. Corp., 614 F.2d 351, 356 (3d Cir. 1980) (rejecting threatened misappropriation), *with* Nat'l Starch & Chem. Corp. v. Parker Chem. Corp., 530 A.2d 31, 33 (N.J. Super. Ct. App. Div. 1987) (protecting threatened misappropriation).

236 Wiesner, *supra* note 228, at 219–21.

employee turnover discusses the value of employees and their knowledge as assets.[237] There is some technical information accessible to both employees and the public, such as "general [KSE],"[238] the disclosure of which does not increase the loss to the company holding the information. However, when an employee leaves or betrays, the company loses this employee as human capital and some technical information only held by the employee. Meanwhile, employee mobility or betrayal may also result in probable losses for disclosing some unpublished technical information held by the company but accessible to the employee.

In conducting innovation and transmitting technical information between the company and employees, the company bears disclosure risks, and employees bear legal risks if information disclosure triggers legal restrictions. The two types of risks and the probability of disclosing the unpublished technical information can be reduced by physical or legal restrictions placed by the company on employees. This Part explains the risks and the company's probable losses due to employee mobility or betrayal and information disclosure, which can be reduced or prevented by legal protection.

A. Allocation of Disclosure Risks

Figure 2 maps different legal or physical measures of securing technical information in two axes. A company's disclosure risks are depicted by the Y-axis. The X-axis depicts a departing, betrayal, or reckless employee's legal risks of disclosing the technical information received, produced, or potentially produced in the company. The employee has low legal risks if there are no enforceable legal restrictions against information disclosure. By contrast, the company has high disclosure risks if it expects to exclusively use unpublished technical information. However, there may be no enforceable legal restrictions against the disclosure of the information.

[237] Urbancová Hana & Linhartová Lucie, *Staff Turnover as a Possible Threat to Knowledge Loss*, 3 J. COMPETITIVENESS 84, 84 (2011).

[238] *See generally* Hrdy, *supra* note 201.

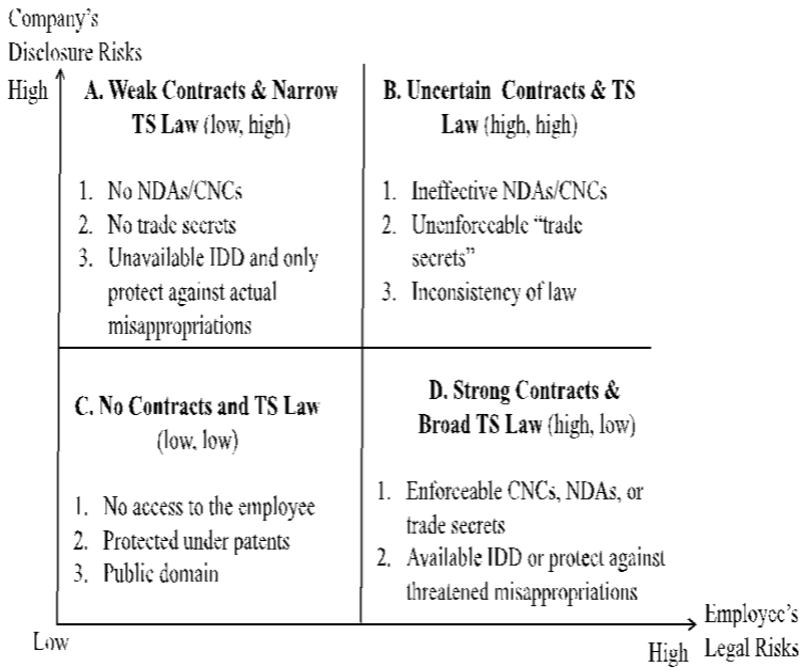

Figure 2. Risks Allocation by Legal Security Measures.[239]

In three circumstances, the company bears low disclosure risks. First, the company may deny the employee access to unpublished technical information by physical measures. Thus, the employee cannot disclose the information that he has not learned. Second, the company may voluntarily reveal the information to the public as patents (i.e., P_1) or in the public domain (i.e., *D*). Correspondingly, the employee does not bear legal liabilities for the information disclosure. Third, the company may have strong legal protection for the information, such as enforceable NDAs, CNCs, or trade secrets under the UTSA, the DTSA, or the IDD. In such a situation, the employee bears high legal risks for information disclosure caused by him for his legal duties.

Broad trade secret law, such as the CUTSA and the IDD, reduces disclosure risks borne by the company compared to average trade secret law.[240] The CUTSA enables trade secret protection for confidential

[239] Wang, *supra* note 49.

[240] *See* Risch, *supra* note 72, at 54 (suggesting that trade secret protection in California is stronger than other states and reduces litigation costs and litigation uncertainties).

information readily ascertainable to the public.[241] Moreover, compared to the UTSA that may enjoin threatened misappropriations,[242] the IDD and the DTSA enjoin departing employees from threatened misappropriations, broader than the UTSA's fundamental protection scope.[243] By contrast, some courts that narrowly adopt the UTSA enjoin actual misappropriations, as shown in Appendix. In such a circumstance, the difficulties in enforcing a trade secret increase disclosure risks borne by the company.

In contrast to the circumstances of imposing low disclosure risks to the company, it bears high disclosure risks without any legal protection or under ineffective legal protection. The company can establish fiduciary duties against information disclosure by using CNCs, NDAs, or other security measures. However, the fiduciary duties may not be properly or effectively established.

The company bears high disclosure risks if it reveals information to the employee but releases him from any fiduciary duties. First, it is apparent that the employee does not bear any legal risks if the employee does not own fiduciary duties to the company. Thus, when the employee self-teaches the information without direct authorization of information accessibility given by the company, the company fails to impose explicit fiduciary duties on the employee. Second, CNCs and NDAs that are signed by the employee but are ineffective and not enforceable do not impose fiduciary duties successfully. Some states commonly do not enforce CNCs for legislative restrictions (e.g., California).[244] In such a circumstance, the employee bears low legal risks for the information disclosure solely governed by the unenforceable CNCs because the employee knows that the signed CNC is very likely to be void. Some states set strict thresholds for enforcing CNCs, such as time length and geographical scope.[245] Similarly, courts may refuse to enforce NDAs for policy reasons,[246] which results in high uncertainties about enforcing the

241 *See* CAL. CIV. CODE § 3426.1(d) (West 2012); Abba Rubber Co. v. Seaquist, 286 Cal. Rptr. 518, 528 (Cal. Ct. App. 1991).

242 18 U.S.C. § 1836(b)(3)(A) (2016); UNIFORM TRADE SECRETS ACT § 2(a) (UNIF. LAW COMM'N 1985).

243 Kahnke et al., *supra* note 225, at 2.

244 *See*, *e.g.*, CAL. BUS. & PROF. CODE. § 16600 (Deering 1941); CAL. LAB. CODE § 2802 (Deering 1937).

245 *E.g.*, Boulanger v. Dunkin' Donuts, Inc., 815 N.E.2d 572, 576–77 (Mass. 2004) ("A covenant not to compete is enforceable only if it is necessary to protect a legitimate business interest, reasonably limited in time and space, and consonant with the public interest.").

246 *See* Kitch, *supra* note 159, at 689–90. *See also* discussion *supra* Section II.A.

signed NDAs and high disclosure risks. For instance, non-trade secret confidential information addressed by NDAs may not be enforceable in courts.[247] If the NDAs are void, the employee, again, bears low legal risks for the invalidity of the NDAs. Moreover, the company may not sign adequate NDAs to effectively cover each unit of technical information that the company is not ready to reveal to the public.[248] Therefore, the confidential information other than trade secrets imposes high risks borne by the company and the employee. On the one hand, the confidential information imposes fiduciary duties on the employee, suggesting high legal risks if he reveals the information. On the other hand, the scope of trade secrets is narrower than confidential information. The company may believe that it holds "trade secrets," which merely constitute confidential information rather than enforceable trade secrets under trade secret law (e.g., P_3, P_4, and P_5). As a result, the company may lose the exclusive rights over the information if courts refuse to protect the information under trade secret law.

B. Ineffectiveness of Legal Protection for Unpublished Technical Information

The restrictions and uncertainties of the legal security measures for prohibiting information disclosure suggest four reasons explaining that the legal security measures cannot effectively protect unpublished technical information. First, some types of secrets may not be enforceable against employees under CNCs, NDAs, and trade secret law. The contracts and trade secret law have various uncertain boundaries depending on the technical information's function and significance in business. Second, courts may refuse to enforce secrets for policy reasons. Third, some employees may process Phase I transactions of unpublished information without the company's knowledge, which may be outside of the legal protection under contract law and trade secret law. Fourth, the company may not know the existence of some knowledge only held by its employees and cannot enforce its legal rights under contract law or trade secret law. These four theoretical arguments about the ineffective legal protection have been proved by Schmidt's empirical evidence: knowledge spillovers are inevitable regardless of trade secret protection.[249]

247 *See* Sandeen, *supra* note 155, at 143 ("Where information is not a trade secret but constitutes confidential or proprietary information, it is argued that a party who contractually agrees to maintain the confidentiality of such information is bound to honor the contract.").

248 *See* Epstein & Levi, *supra* note 70, at 898.

249 *See generally* Schmidt, *supra* note 26.

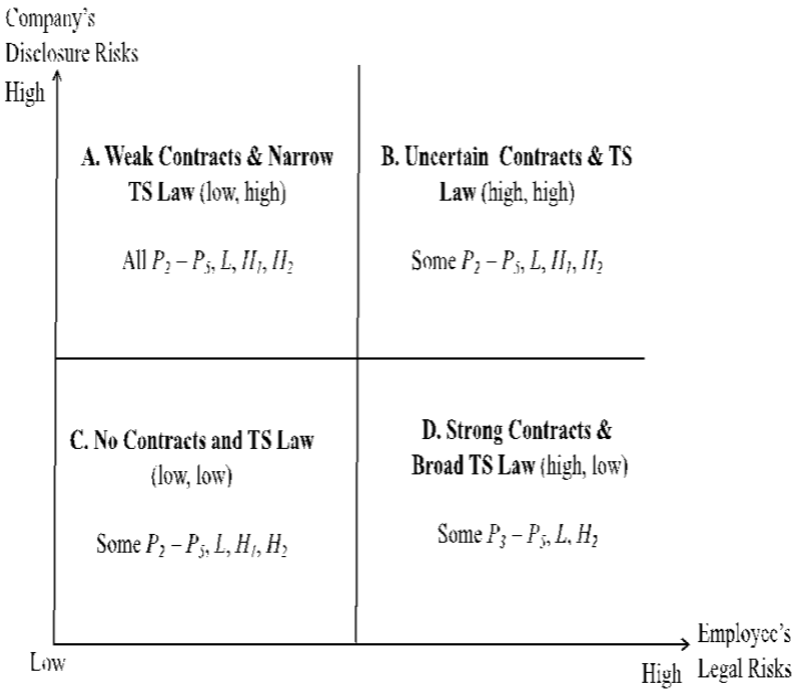

Figure 3. Risks Allocation by Information Types.[250]

First, CNCs, NDAs, and trade secret law can conceal the unpublished technical information deployed by a company in its first-generation products or production (i.e., P_2). CNCs are confined to the protection against the company's competitors (i.e., $P_2 - P_5$, L, H_1, H_2). By contrast, other types of unpublished technical information (i.e., the technical information for developing the second-generation products P_3, deterring competitors P_4, or being deposited P_5) may not be enforceable under trade secret law due to their hardship to establish the existence of enforceable trade secrets. Trade secret law does not impose liabilities on employees for all types of secrets. Moreover, CNCs cannot perfectly conceal them, either, because these types of information can be more attractive to non-competitors than competitors. In addition, NDAs governing these types of information in confidential may not be enforceable if there is a threshold of showing trade secrets for courts to

[250] Wang, *supra* note 49.

enforce the NDAs. NDAs are neither a sufficient nor a necessary condition for establishing enforceable trade secrets.[251]

Second, courts give policy reasons to decline to enforce NDAs, CNCs, and secrets.[252] Knowledge spillovers are a public good, which can be caused by information disclosure or employee mobility.[253] Thus, courts may refuse to enforce fiduciary duties imposed in NDAs or under trade secret law for knowledge spillovers and to promote social innovation. Moreover, courts may decline to apply the IDD or enforce CNCs for the same reason or the freedom of employment.[254] By contrast, courts may also enforce NDAs, CNCs, and secrets for other policy reasons, including but not limited to promoting innovation and creation, reducing precaution costs, protecting privacy, and enforcing "standards of commercial ethics".[255] Taking NDAs as an example, Lobel suggests that NDAs are a double-edged sword in innovation.[256] On the one hand, NDAs crush startup competitors and deter competitors from hiring employees of a company or acquiring its confidential information.[257] On the other hand, NDAs deter the company from hiring talented employees from their competitors.[258] Overall, the uncertain policy reasons adopted by courts may result in either ineffective or effective legal protection for all types of unpublished technical information.

Third, contract law and trade secret law may not be effective to protect unpublished technical information for information asymmetries, which are discussed in Part II. Franco and Mitchell suggested that a company is incapable in knowing how much employees exactly learn the unpublished technical information held by the company.[259] Other scholars also broadly recognize the existence of information asymmetries.[260] Even though adequate NDAs may cover all the confidential information against the employees who access the information with authorization, NDAs cannot effectively impose fiduciary duties on the employees who self-

251 *See* Risch, *supra* note 72, at 6–8; Sandeen, *supra* note 155, at 125; Johnson, *supra* note 195, at 551.

252 *See, e.g.*, Shearson Lehman Bros. Holdings, Inc. v. Schmertzler, 166 A.D.2d 216 (N.Y. App. Div. 1986). *See also* Kitch, *supra* note 159, at 697.

253 Pace, *supra* note 117, at 441–42.

254 Godfrey, *supra* note 231, at 167.

255 Bone, *supra* note 21, at 250; Kitch, *supra* note 159, at 685.

256 Lobel, *supra* note 149, at 370.

257 *Id*. at 377.

258 *Id*.

259 Franco & Mitchell, *supra* note 60, at 603.

260 *E.g.*, Png, *supra* note 25; Schwartz, *supra* note 31; Dass et al., *supra* note 65, at 4 (suggesting that small firms suffer the information asymmetries the most).

teach the information without authorization. As a result, the company does not have an enforceable NDA against the self-taught employees and may lose the trade-secret information against any outsiders. Regardless of whether or not there are enforceable CNCs and the unpublished technical information is used by a direct competitor, knowledge spillovers created by the employees at least result in deadweight losses for the company.

Fourth, NDAs, CNCs, or trade secret law is incapable of imposing fiduciary duties on employees for the asymmetric information only held by employees (i.e., L, H_1, and H_2). The company hardly knows the information held only by employees (i.e., L, H_1, H_2)[261] and to estimate the information value.[262] The employee inventor has the absolute control of the technical information before the information is disclosed to the company.[263] Thus, the company is incapable of retrieving the information unknown to it. Yeh argues that it usually takes a long time for companies to realize that their trade secrets are misappropriated by (departing) employees, which creates difficulties for companies to enforce trade secret protection.[264] However, companies suffer insuperable hardships for the asymmetric information only held by employees. On the one hand, most startups file patents to avoid trade secret litigations, suggested by the empirical evidence of Shalem and Trajtenberg.[265] On the other hand, NDAs and trade secret law cannot be precautions against such a situation for the failure of imposing fiduciary duties when companies do not control the information. Even though courts recognize the property rights of companies over the technical information developed by their R&D investment, the companies should not pursue the rights under contract law and trade secret law.[266] Moreover, CNCs restricting employee mobility prevent the information from being disclosed to competitors, but cannot restrict departing employees from disclosing the information to others or force the employees to transfer the information back to the company.

The company may be entitled to the property rights of the asymmetric information under labor law, human capital law,[267] or patent

261 *See* Schwartz, *supra* note 31.

262 *See* Png, *supra* note 25.

263 *See generally* Anton & Yao, *supra* note 17.

264 *See* YEH, *supra* note 18, at 13–14.

265 *See* Trajtenberg & Shalem, *supra* note 103, at 129.

266 *See generally* Bd. of Trs. of the Leland Stanford Junior Univ. v. Roche Molecular Sys., 563 U.S. 776, 792 (2011); Preston v. Marathon Oil Co., 684 F.3d 1276, 1288–89 (Fed. Cir. 2012); Anton & Yao, *supra* note 17; Lobel, *supra* note 149.

267 CAL. LAB. CODE § 2860 (2019) ("Everything which an employee acquires by virtue of his employment, except the compensation which is due to him from his employer, belongs to the employer, whether acquired lawfully or

law, especially after the modern utilitarian law prevails Locke's labor theory that laborers own the property rights of what they produce, rather than contract law or trade secret law.[268] Thus, disclosing such asymmetric information may increase legal risks associated with labor law or human capital law rather than legal risks associated with contract law or trade secret law. This increase is limited because employees can always argue that the information is in the public domain (i.e., *D*). The startups funded by departing employees (spin-outs) always file patents to prevent trade secret legal issues raised by their previous employer.[269] This consequence of filing patents with the asymmetric information held by them increases disclosure risks borne by the previous employer.

C. Reduced Innovation Without Contracts and Trade Secret Law

The high risks of disclosing technical information by employees borne by a company increase the company's security costs in innovation and deter its innovation. There are three ways to reduce the disclosure risks without increasing the legal risks borne by employees. First, the company can disregard CNCs, NDAs, and trade secret law to reduce the disclosure risks. The cheapest way to reduce the disclosure risks is to voluntarily reveal the information to the public for free. Then, the KSE of employees are broadened for the open access to the information. Moreover, the information then is contributed to the public domain (i.e., *D*) and spur social innovation as knowledge spillovers, regardless of employee mobility. However, there is no control for the company if the information is contributed to the public domain.[270] The company may suffer the loss of developing the information and do not sustain innovation.

A company hardly disclose its information to the public for free, but it may generate more revenue for exclusively holding the information (i.e., storing the information as P_1 to P_5).[271] A reasonable information holder maximizes its income received from the information.[272] Legal professions reminded that many industries profit from IP rights, rather than

unlawfully, or during or after the expiration of the term of his employment."). *See also* Am. Alloy Steel Corp. v. Ross, 308 P.2d 494, 497 (Cal. Dist. Ct. App. 1957).

268 *See generally* LOCKE, *supra* note 83.

269 *See* Anton & Yao, *supra* note 84, at 192, 203 (reasoning as a result of weak negotiation power owned by employees).

270 *See* Hall et al., *supra* note 16, at 376.

271 *See generally* Bhattacharya & Guriev, *supra* note 35. *But see* Schmidt, *supra* note 26, at 7 (suggesting a marketing stunt for open innovation).

272 *See* COOTER & ULEN, *supra* note 55, at 12–13.

merely products.[273] Thus, to reduce disclosure risks, companies will persist in securing the technical information in secrecy (i.e., P_2 to P_5) against both the public and employees or under patents (i.e., P_1) for maintaining the exclusive rights. Both of the options are expensive, which is supported by the literature introducing the efficiency of trade secret law.[274]

Securing the information from employees, however, harms innovation, which is opposed to the goal of trade secret law.[275] When reducing the disclosure risks, the company refuses to train employees in KSE and strictly forbids employees from accessing the unpublished technical information. The worst case is that the unused information (i.e., P_3 to P_5) does not generate imminent value and drops in deadweight losses to both the company and the society. Therefore, scholars desire developing trade secret law for increasing the training.[276] However, the literature stops at where employees can receive few additional KSE in such a situation. The harm of strictly blocking information from employees also includes limited innovation activities conducted by employees, low innovation incentives of employees, and low employee stability and loyalty. Employees can learn or acquire the unpublished information (i.e., P_2 to P_5) by self-teaching, suggesting a failure of reducing the disclosure risks.

D. Reduced Innovation Under Contracts and Trade Secret Law

A company can reduce its disclosure risks by relying on legal security measures other than patent law, such as CNCs, NDAs, and trade secret law. The legal security measures impose fiduciary duties on employees, which increases legal risks borne by them. Shifting the company's disclosure risks to employees as legal risks is only effective under a precondition that the contracts (i.e., CNCs and NDAs) or trade secrets should be enforceable under the law. Otherwise, the legal risks increase without a decrease in the disclosure risks. For example, even though the company believes that it has trade secrets, the "trade secrets"

273 *See* Almeling, *supra* note 15, at 1104.

274 Filing patent applications is costly, and the information may not be patentable. Moreover, the information's R&D costs and patenting costs may not be fully compensated by the 20-year patent protection. *See e.g.*, Friedman et al., *supra* note 22, at 65; Levine & Sichelman, *supra* note 27, at 755–70 (listing eight reasons for using trade secrets to substitute for patents); Lemley, *supra* note 28, at 339–41. *But see* Bone, *supra* note 21, at 269, 271–77.

275 *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 489 (1974) (encouraging companies to share information with employees).

276 *E.g.*, Lemley, *supra* note 28. *But see* Bone, *supra* note 21, at 271.

may probably not enforceable when lacking: (1) a narrow scope; (2) economic value; (3) novelty; or (4) actual misappropriations.[277]

The increased legal risks borne by employees for reducing the disclosure costs harm both the company's innovation and social innovation. Superficially, the high legal risks for fiduciary duties deter employees from mobility, betrayal, or revealing confidential information in other forms. Employees are prohibited from using the arguable technical information (i.e., P_2 to P_5) after the employment or disclosing the information to outsiders. Accordingly, the literature suggests that assured exclusive rights induce large businesses to invest in R&D under the sacrifice of entrepreneurship and innovation conducted by startups.[278]

As a result of the strong exclusive rights for the company imposing strong fiduciary duties, however, employees may not have incentives to learn or acquire the information from the company. Moreover, under the high legal risks for information disclosure, employees also have few incentives to transfer the information to the employers if they are the controllers of the information (i.e., L, H_1, and H_2), reducing Phase II transactions. The increased legal risks borne by employees reduce the disclosure risks borne by the company by squeezing the size of unpublished information (i.e., accumulated P_2 to P_5) learned, used, or contributed by employees.

By contrast, employees have motivations to transfer their creative technical information to outsiders[279] and hide it from the company, even though the company expects their loyalty.[280] Employees have expectations on their internal and external career path.[281] However, their intelligence and the technical information produced by their intelligence have unbalanced values to the employees and the company. First, information producers—employees value the technical information more than the information receivers—the company.[282] Second, the company may undervalue the information.[283] On the one hand, the value of the technical information depends on how the company manipulates and deploys the information in its business.[284] On the other hand, because of the costs associated with training employees, the company pays relatively

277 *See* discussion *supra* Section II.B.

278 *See* Lobel, *supra* note 149, at 377 (arguing that DTSA that strengthens trade secret protection has large harm effects on small firms).

279 *See generally* Trajtenberg & Shalem, *supra* note 103.

280 *See, e.g.*, Lemley, *supra* note 28, at 335.

281 *See* Contigiani et al., *supra* note 30, at 2938.

282 Risch, *supra* note 72.

283 Png, *supra* note 25.

284 Lemley, *supra* note 28.

lower wages to employees compared to their contribution to the company.[285] Third, outsiders may pay more to employees for the technical information than the company or be more efficient to deploy or further develop the information, which may drive employee mobility.[286] Therefore, it is groundless to suggest that restricting information mobility by trade secret law can promote the "esprit de corps" of companies.[287] Png suggested that employees always make tradeoffs between learning and receiving payments.[288] Based on the theory of Fosfuri and Rønde, employee mobility is high if employees hold the technical information that is valuable to second-stage products.[289] Scholars also observed that in the states without strong trade secret protection, companies increase salaries or hire relatives for retaining employees.[290]

V. Balance the Enforcement of Contracts and Trade Secret Law

According to the nexus between information management and innovation in the use and enforcement of contracts and trade secret law,[291] courts should find the balance between reducing the disclosure risks resulted from employee mobility or betrayal and promoting innovation invested by companies and conducted by employees or outsiders. When courts and legislators support the legal security measures adopted by companies, courts should foresee both a probable decrease in innovation and the decreased knowledge spillovers for the strong exclusive rights given to companies under contract law or trade secret law. This Article argues that courts should narrowly enforce NDAs as consistent as the scope of trade secret law but broaden the scope of trade secret protection without a harm on employee loyalty. It is more efficient for innovation to strengthen trade secret protection by adopting the IDD than enforcing CNCs.

A. Non-Disclosure Agreements

285 Barnett & Sichelman, *supra* note 90.

286 *See* YEH, *supra* note 18; Bhattacharya & Guriev, *supra* note 35; Trajtenberg & Shalem, *supra* note 103.

287 Levine & Sichelman, *supra* note 27, at 768 ("[T]here is no doubt that trade secrecy can serve such a purpose and thus help promote the esprit de corps of a well-run startup.").

288 Png, *supra* note 25.

289 Fosfuri & Ronde, *supra* note 31, at 46–47.

290 *See* Lippoldt & Schultz, *supra* note 64, at 9.

291 *See* discussion *infra* Part IV. *See also* discussion *infra* Sections V.C, V.D.

NDAs may not effectively reduce the disclosure risks borne by a company because not all confidential information (i.e., P_2 to P_5) is protectable under NDAs.[292] Under ineffective NDAs, the disclosure risks borne by the company and the legal risks of its employees are both high. As Epstein & Levi reminded, while NDAs can deter information disclosure by employees, NDAs can never be perfectly competent to indicate and cover every unit of confidential information.[293] The high dual risks suggest high security costs for the company and harm the company's innovation, incentives of employees to improve their KSE, and social innovation.

Courts can reject enforcement of NDAs or narrowly enforce NDAs for encouraging knowledge spillovers and social innovation. Instead, courts can enforce NDAs for protecting enforceable trade secrets.[294] Denials of NDAs are a utilitarian process for accumulating knowledge spillovers. First, denials of NDAs filter out social deadweight losses due to the information's inefficient use by its owners from all the confidential information (i.e., P_2 to P_5). Second, denials of NDAs allow efficient use of the filtered information under competition.

B. Trade Secret Law

The ineffectiveness of NDAs in trade secret protection can be fixed by trade secret law.[295] Courts do not enjoin a company from enforcing NDAs for trade secrets.[296] Moreover, inadequate NDAs that do not thoroughly cover each unit of unpublished or confidential information, but establish implicit fiduciary duties, may trigger the liability for trade secret misappropriations. The trade secret information disclosed by bad faith employees who self-learn the information is enforceable under trade secret law.[297]

The strengthened protection under the UTSA and the DTSA suggests an increase of security costs, which does not necessarily suggest legal inefficiency. Statistics showed that NDAs are necessary but not

292 Sandeen, *supra* note 155, at 143 (suggesting that it is arguable about whether or not confidential agreements are binding).

293 Epstein & Levi, *supra* note 70, at 900.

294 *See*, *e.g.*, Sandeen, *supra* note 155, at 143.

295 *See id*. at 132 (suggesting the use of trade secrets to define the boundary of confidential relationships).

296 *Id*. at 126–27.

297 *See* Lemley, *supra* note 28, at 318 (suggesting that the obligation of trade secret protection is set either explicit by contracts or implicit by duty).

sufficient to establish the element of reasonable efforts in federal courts,[298] while it is neither a necessary nor a sufficient condition for establishing trade secrets according to the UTSA.[299] The company also needs other physical security measures to show reasonable efforts for protecting confidential technical information (i.e., P_2 to P_5) as trade secrets, while the security does not need to be perfect.[300] These physical security measures do not strictly prohibit employees from accessing the information, but allow them to use the information due to the legal protection. The information's economic value should offset security costs for the company but required by law, so trade secret protection is still efficient for the company. Otherwise, the company pursues patents for protecting the information, or disposes it in the public domain.[301]

Trade secret law supplementing NDAs, however, shrinks the scope of information protection. Confidential technical information addressed in NDAs (i.e., P_2 to P_5) may not be entitled to trade secret protection for lack of novelty or independent economic value. For example, confidential information readily ascertainable to the public is not novel and not entitled to trade secret protection in some states other than California.[302] Broad trade secret protection, such as the CUTSA and the IDD, narrows the gap between the scope of trade secret law-protectable information and the scope of confidential technical information (i.e., P_2 to P_5). Broad trade secret protection fixes some ineffective or unenforceable NDAs, and strong trade secret law can reduce the company's disclosure losses and disclosure risks. As a result, broad trade secret law and strong trade secret protection function as rewards for the company to train employees and may further improve the company's R&D investment.[303]

It is reasonable that most scholars support the relief of novelty requirements for trade secret protection.[304] Without communicating the

298 Almeling et al., *supra* note 214, at 294.

299 *See* Risch, *supra* note 72; Sandeen, *supra* note 155, at 140; Johnson, *supra* note 195, at 566.

300 *See* Lemley, *supra* note 28, at 325.

301 *See generally* Schmidt, *supra* note 26.

302 *See* CAL. CIV. CODE § 3426.1 (West 2012); ABBA Rubber Co. v. Seaquist, 286 Cal. Rptr. 518, 528–29 (Cal. Ct. App. 1991).

303 *Compare* Lemley, *supra* note 28, at 313 (arguing that trade secret protection encourages information disclosure to employees), *with* Bone, *supra* note 21, at 271 (expressing doubt about how trade secret law can promote information disclosure).

304 *See e.g.*, Pamela Passman et al., *Economic Impact of Trade Secret Theft: A Framework for Companies to Safeguard Trade Secrets and Mitigate Potential Threats*, CTR. RESPONSIBLE ENTERPRISE & TRADE (2014). *See also* Vincent Chiappetta, *Myth, Chameleon or Intellectual Property Olympian? A Normative Framework Supporting Trade Secret Law*, 8 GEO. MASON L. REV. 69,

confidential information to outsiders, the company has difficulties in evaluating both the novelty and the economic value of its unpublished technical information. R&D activities conducted within the company form the information.[305] If the company is less confident on the long-term value of the information—especially the information potentially being used in production (i.e., P_2 and P_3)—the company is more likely to disclose the information in a patent application (i.e., P_1 or D).[306] Then, the security costs for the company are reduced, and the public benefits from the knowledge spillovers. This argument about the novelty requirement in trade secret law supplements the literature about IP strategies for protecting innovative information under patents or trade secrets.[307]

Companies that try to enforce trade secrets unevenly understand that innovation is a process of exchanging information in Phase I and Phase II, and between insiders and outsiders.[308] Myopic companies are conditioned to exchange information in employee training (i.e., Phase I transaction) by trade secret protection,[309] but ignore Phase II transactions and the benefits of knowledge spillovers that are contributed by outsiders.

Economists criticized the mixed use of NDAs and trade secrets for the public interest.[310] NDAs are *ex ante* without knowing the information value, which may not fairly compensate inventor employees.[311] However, trade secret law protecting innovative and valuable information does not give the employees a second chance to renegotiate with companies.[312] Weak negotiation powers on the side of employees discourage Phase II information transactions and expand information asymmetries.[313] The literature also reminds the risks that strong trade secret law (e.g., the IDD) may harm competition.[314] For example, companies may abuse it to sue

73 (1999).

305 *See* Sandeen, *supra* note 155, at 142 (suggesting that economic value of the information may not be defined in a short term but instead varies by the user of the information).

306 *See* Schmidt, *supra* note 26, at 3, 7 (arguing for the publishment of technical information for free).

307 *See*, *e.g.*, Michael R. McGurk & Jia W. Lu, *The Intersection of Patents and Trade Secrets*, 7 HASTINGS SCI. & TECH. L. J. 189, 205 (2015) (comparing between trade secrets or patents strategically).

308 *See* Ritala et al., *supra* note 78, at 22.

309 *See id.*

310 *See* Anton & Yao, *supra* note 84, at 203.

311 *See id.*

312 *See id.*

313 *See id.* at 192.

314 *See* Sandeen, *supra* note 155, at 154 (citing the IP theory discussed by Justice Scalia). *See also* Wal-Mart Stores, Inc. v. Samara Bros., Inc., 529 U.S. 205, 214 (2000) (discussing the possibility of over-protection for intellectual

departing employees to restrain competitions with startups rather than repair harms caused by trade secret misappropriations.[315]

Relatively inessential, some scholars encourage courts to shrink the scope of trade secret protection further for protecting employees. For example, Hrdy suggested that courts should enforce or reject trade secrets by an employee-oriented measure that the KSE of talented employees are not treated as trade secrets.[316] She inherited Turner's suggestion that personal KSE are not trade secrets, regardless of their value and secrecy status.[317] Giving property rights of the information or knowledge that employees know of, but is invested by companies to employees, only increases the transaction costs in Phase I and induces Phase II knowledge transactions.[318] Renegotiations between companies and employees may not be activated if employees hold property rights. Recall the failure of Locke's labor theory in this utilitarian IP world.[319] The key in determining trade secret scope by courts is not to assign property rights of technical information to employees or companies but rather to allocate the efficient deployer of the information between the companies and outsiders (e.g., competitors or spin-out start-ups). With a presumption of the freedom of employment, enforcing trade secrets is a balance between the deadweight losses and marginal gains for companies and the marginal costs of duplicate innovation for outsiders that departing employees join.[320] Outsiders may deploy the information more efficiently than the companies originating the information (e.g., P_4 or P_5). Lemley relied on the Arrow's information paradox and suggested this possibility.[321] He also suggested that eliminating the secrets that exist only for legal protection can reduce social costs.[322] Moreover, he reminded courts that trade secret owners might not be first movers but only have the possibility of becoming first

property rights).

315 *See*, *e.g.*, Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470 (1974). *See also* Bone, *supra* note 21, at 279.

316 *See* Hrdy, *supra* note 201, at 2463–64.

317 *See id.* at 2449. *See also* AMEDEE E. TURNER, THE LAW OF TRADE SECRETS 115–72 (1962).

318 *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972).

319 *See generally* LOCKE, *supra* note 82. *But see* Lemley, *supra* note 28 (categorizing trade secrets as IP rights); Gordon, *supra* note 83, at 1608 (criticizing Locke's theory and the interests of individuals in innovation).

320 *See* Risch, *supra* note 72, at 38 (arguing that there are marginal costs for outsiders when departing employees cannot use the information under trade secret protection).

321 *See* Lemley, *supra* note 28, at 339 n.119.

322 *See id.* at 336.

movers.[323] Fisher and Oberholzer-Gee also suggested policymakers to incumbent innovation followers for encouraging them to invent around existing technologies.[324]

Therefore, it is an exaggeration for scholars to equalize the function of the IDD and CNCs.[325] The core of applying the IDD is to protect trade secrets rather than employee stability, regardless of whether the freedom of employment may be conflicted with trade secret protection. If trade secret misappropriations after employee mobility create irreparable harm, courts may learn from the injunction rules for patents in e*Bay Inc. v. MercExchange, L.L.C*[326] and carefully adopt the IDD.[327] While injunctive relief means little to patent owners as a form of remedies,[328] without a public entity issuing formal property rights to trade secret owners,[329] injunctions for trade secret owners do not function more than confirming their property rights over the information, which may facilitate licensing the information by outsiders.[330]

Being lavish in adopting the IDD and granting injunctions suggests excessive first-mover advantages, which harms competition and small businesses and may result in market inefficiency.[331] Some empirical evidence suggests that while implementing the IDD does not increase employee mobility and knowledge spillovers, the rules against the IDD result in a higher level of expert mobility and knowledge spillovers.[332]

[323] *See id.* at 340 n.122.

[324] William W. Fisher III & Felix Oberholzer-Gee, *Strategic Management of Intellectual Property: An Integrated Approach*, 55 CAL. MGMT. REV. 157, 177 (2013).

[325] The appendix suggests that many states do not consistently adopt the IDD and enforce CNCs. *See* Godfrey, *supra* note 231, at 167 (combining the analyses of the IDD and CNCs). *Cf.* Patio Enclosures, Inc. v. Herbst, 39 F. App'x. 964, 969 (6th Cir. 2002).

[326] 547 U.S. 388 (2006).

[327] The *ex parte* seizure remedy under the DTSA has a similar effect, suggested by Lobel. *See* Lobel, *supra* note 149, at 374.

[328] Gene Quinn & Eileen McDermott, *The Year in Patents: The Top 10 Patent Stories of 2019*, IPWATCHDOG.COM (Dec. 29, 2019), https://www.ipwatchdog.com/2019/12/29/year-patents-top-10-patent-stories-2019/id=117177/ (commenting that giving more injunctive relief functions as restating the patent issuance and is not what patentees expect).

[329] *See generally* Hall et al., *supra* note 16 (distinguishing formal IP and informal IP).

[330] *See generally* Calabresi & Melamed, *supra* note 318.

[331] *See* Sandeen, *supra* note 155, at 154 (criticizing over-protection for trade secrets). *See also* Lobel, *supra* note 149, at 377–78.

[332] I.P.L. Png & Sampsa Samila, *Trade Secrets Law and Engineer/Scientist Mobility: Evidence from "Inevitable Disclosure"* (Feb. 2013), http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=7892A0D935B1417F

Some empirical evidence suggests that the IDD harms innovation quality.[333] Therefore, California is a moderate model of trade secret protection. On the one hand, it broadens the scope of trade secret protection *ex ante* by protecting "readily ascertainable" information.[334] On the other hand, it has a high *ex post* bar of enforcing the broad trade secret by broadly not adopting the IDD but asking for actual harm.[335]

Least importantly in terms of innovation efficiency, Hyde in the late 1990's suggested that courts should compensate company reputations under trade secret law rather than their trade secret damages,[336] which was criticized by Gilson for lack of efficiency.[337] Preliminary injunctions may function as reputational compensations in the U.S., suggested by how copyright infringers are sued for protecting privacy,[338] and also expected by trade secret owners.[339] However, companies are encouraged to receive such reputational compensations from the patent regime, which is a filing, examination, and registration system.[340]

C. Covenants Not to Compete

Enforcing CNCs can be understood as a reward to a company for training and investing in employees for improving their inventiveness and KSE. Enforcing a CNC suggests low security costs for preventing information disclosure to a company's competitors, especially the information being used in production (i.e., P_2).[341] Moreover, employee stability also ensures the success of developing second-generation

3A3C4E0ECA9D0FA6?doi=10.1.1.308.5620&rep=rep1&type=pdf.

333 *See* Contigiani et al., *supra* note 30, at 2924.

334 *See* CAL. CIV. CODE § 3426.1(d) (West 2016); ABBA Rubber Co. v. Seaquist, 286 Cal. Rptr. 518, 519 (Ct. App.1991).

335 *E.g.*, Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277 (Cal. Ct. App. 2002).

336 *See* Alan Hyde, Real Human Capital: The Economics and Law of Shared Knowledge 137–40 (May 1998) (unpublished manuscript) (on file with N.Y.U. L. REV.); Gilson, *supra* note 41, at 601 (citing Hyde's suggestion).

337 *See* Gilson, *supra* note 41, at 624.

338 *See generally* Andrew Gilden, *Copyright's Market Gibberish*, 94 WASH. L. REV. 1019 (2019).

339 *See* McGurk & Lu, *supra* note 307, at 205.

340 *See* Quinn & McDermott, *supra* note 328 (suggesting that preliminary injunctions have limited benefits for patent owners since giving a preliminary injunction is not more than repeating the USPTO's issuance).

341 *See* Franco & Mitchell, *supra* note 60, at 583 (calling CNCs as a surplus for employers because of preventing employees spin-out to maximize their benefits).

products.[342] By contrast, Fosfuri and Ronde suggested that the valuable information that can be applied in second-generation products (i.e., P_3) spurs employee mobility, knowledge spillovers, and competition.[343] In addition, the protected information includes both the information known to the company and the asymmetric information that is only held by employees but can be used to compete with the company (e.g., H_1). Overall, the loss from disclosing unpublished information under CNCs can be as low as the loss under trade secret law, which requires higher security costs compared to CNCs. The CNC substitute for costly trade secret law is supported by empirical evidence that where CNCs are strongly enforced, trade secret law is not frequently claimed against employees/employers.[344]

CNCs are, however, inefficient when companies are uncertain about their entitlement of the rewards, or courts are not clear about who should be entitled to the rewards. On the side of companies, even though the legislation does not strictly prohibit CNCs, some states usually do not enforce CNCs, such as California.[345] Moreover, the enforceable CNC protection of information is limited to a short period, particular geographical areas, the type of information, and the receivers of the disclosed information. In other words, only CNCs fail to secure both the information and the revenue generated by the information and cannot reduce disclosure risks borne by the companies. A probable grievous outcome of using CNCs is that innovation within companies is worsened when employees lack the incentives and abilities to create valuable technical information.[346] CNCs increase the costs of employees to find jobs, and reduce the incentives of employees to learn and acquire technical information from companies.[347] The legal risks of breaches of CNCs restrict employee mobility.[348] However, the legal risks do not create incentives for employees to transfer their knowledge to employers. Thus, CNCs cannot eliminate asymmetry information only held by employees (i.e., L, H_1, and H_2).

342 Fosfuri & Ronde, *supra* note 31, at 46.

343 *Id.* at 47–48.

344 *See* Png, *supra* note 25, at 4.

345 *See, e.g.*, CAL. BUS. & PROF. REG. § 16600 (West 1941); CAL. LAB. CODE § 2802 (West 2016); Ixchel Pharma, LLC v. Biogen Inc., No. 2:17-00715, 2018 U.S. Dist. LEXIS 13548, at *12–13 (E.D. Cal. Jan. 25, 2018).

346 *Compare* Png, *supra* note 25, at 8–9 (suggesting that CNCs reduce innovation and entrepreneurship), *with* Barnett & Sichelman, *supra* note 90, at 5 (arguing no causal relationships between CNCs and innovation and the employee turnover).

347 *See* Contigiani et al., *supra* note 30, at 2929–31.

348 *See* Gilson, *supra* note 41, at 606 (suggesting that CNCs reduce employee mobility but do not improve innovation).

On the side of courts and legislators, the culture of strengthening CNC enforcement does not benefit the public interest. Creating a culture of anti-spillovers by CNCs prevents companies from acquiring the benefits of spillovers from others. This culture can also be interpreted as a culture of over-rewarding companies, especially large businesses, which decreases competition in the market. Companies extend their market power by CNCs rather than high-tech products, which have a relatively short life span.[349] The rewards are not free, but the rewards reduce profits received from continued innovation.[350] Companies, including the rewarded large businesses, cannot hire leading employees from leading companies to produce more technical information in that culture.[351] Empirical evidence shows that the states with strong CNC enforcement on average have lower employee mobility but more low-wage employees and higher recruitment costs compared to other states.[352] Moreover, the comparison between Silicon Valley and Route 128 suggests that CNCs are inefficient in promoting innovation in the industry of cumulative technologies.[353] Prohibiting employers from using CNCs is one significant characteristic of Silicon Valley,[354] even though no literature supports the causal effect of this prohibition on the success of Silicon Valley. Risch noted that companies can only rely on CNCs when the law is not clear about the scope of trade secrets, while the uncertainties of enforcing CNCs increase the costs in Phase I transactions.[355]

Moreover, CNCs may result in reverse-selection and only unenthusiastic employees are retained.[356] An innovative departing employee following his CNC may bring the knowledge to other cities or industries. As a result, the knowledge may spill to other cities or industries, which may not efficiently benefit the development of domestic innovation but benefit the society in general. Therefore, as Fosfuri and Rønde suggested, when enforcing CNCs, courts should not treat it as an

349 *See id.* at 613 (explaining that CNCs in Massachusetts have provided "critical additional protection . . . because trade secret protection of tacit knowledge is ineffective").

350 *See* Fosfuri & Ronde, *supra* note 31, at 47; Franco & Mitchell, *supra* note 60, at 586.

351 *See* Franco & Mitchell, *supra* note 60, at 586.

352 Evan Starr et al., *Mobility Constraint Externalities*, 30 ORG. SCI. 961, 962 (2019).

353 *See* Gilson, *supra* note 41, at 629.

354 *See id.* (suggesting courts and policymakers not blindly replicate or follow the legal model of Silicon Valley but adopt CNCs depending on their domestic demands and industry characteristics).

355 Risch, *supra* note 72, at 41.

356 *See* Contigiani et al., *supra* note 30, at 2923.

independent contract issue but rather should take the local labor market and market competition into consideration.[357] Otherwise, enforcing CNCs suggests over-rewards and harms R&D incentives and public interests.[358] Therefore, it is not surprising that the U.S. Federal Trade Commission moved against CNCs and proposed rules to limit the use of them.[359]

D. Employee Loyalty

Under the legal risks shifted by companies, it is still possible that employees may develop their knowledge unknown to the company (i.e., H_1, and H_2) with outsiders or in spin-out startups. Then, while the valuable information may not be a deadweight loss to the society (i.e., L), it is still a deadweight loss to the company. It is not clear whether or not outsiders can deploy the information more efficiently than the company. In other words, the use of the information by a company other than the previous employer may or may not be efficient.

It could be more efficient for the previous company to decide the value of the asymmetric information held only by employees. Otherwise, its early-stage investment in the information would never be collected from outsiders or spin-out startups. The company may appreciate the innovativeness of the contributors and invest in the information inside the company or fund it in a subsidiary (spinoffs). However, the company cannot force employees to utterly reveal their ideas, which form valuable technical information. Loyal employees may be more active in revealing their valuable or innovative ideas to the company, suggesting a lower degree of asymmetric information only held by employees (i.e., L, H_1, and H_2).

Even though it is an old story to improve employee loyalty through management measures,[360] it is controversial how courts treat employee loyalty in trade secret cases. Strong concerns about employee loyalty or confidential relationships lead courts to enforce fiduciary duty without a shell of trade secrets.[361] Alternatively, the strong property-right

357 *See* Fosfuri & Ronde, *supra* note 31, at 60.

358 *See id*.

359 Braden Campbell, *Noncompete Developments to Watch for in 2020*, LAW360 (Jan. 14, 2020 10:55 PM), https://www.law360.com/articles/1234422/noncompete-developments-to-watch-for-in-2020-.

360 *See* Epstein & Levi, *supra* note 70, at 900–02 (suggesting that the use of leadership or morale can improve employee loyalty).

361 *See, e.g.*, Mass. Eye & Ear Infirmary v. QLT Phototherapeutics, Inc., 559 F.3d 1 (1st Cir. 2009); NovelAire Techs., LLC v. Harrison, 2009-1372 (La. App. 4 Cir. 10/13/10), 50 So. 3d 913. *See also* Graves & Tippett, *supra* note

theory may substitute confidential relationships and lead courts to affirm the property rights of companies over any information developed under their investment and sources.[362] However, the idea of assigning strong property rights to trade secret owners has been criticized by scholars.[363] In practice, the property-right theory is primarily adopted to solve patent issues[364] or criminal trade secret claims,[365] but rarely adopted in civil trade secret cases.[366] In other words, courts adopt broad property rights for trade secret owners and criminal sanctions against employees under the Economic Espionage Act ("EEA") to deter both trade secret thefts and the decrease in employee loyalty.[367] The question remains for future studies on how the EEA can deter bad faith information disclosure or improve employee loyalty. The bottom line for civil trade secret law is not to discourage employee loyalty for creating moral-hazard crises.[368]

VI. Conclusion

CNCs, NDAs, and trade secret law are ineffective to protect unpublished technical information due to legal uncertainties and information asymmetries between companies and employees. The

197, at 88–89.

362 *See, e.g.*, Bd. of Trs. of Leland Stanford Junior U. v. Roche Molecular Sys., Inc., 563 U.S. 776 (2011). *See also* Lobel, *supra* note 168, at 814.

363 *See*, *e.g.*, Sandeen & Levine, *supra* note 25, at 366 (suggesting the law adopts liability rule rather than property rule); Risch, *supra* note 72, at 27.

364 *E.g.*, *Bd. of Trs. of Leland Stanford Junior U.*, 563 U.S. at 786 ("[U]nless there is an agreement to the contrary, an employer does not have rights in an invention 'which is the original conception of the employee alone.'" (quoting United States v. Dubilier Condenser Corp., 289 U.S. 178, 189 (1933)); Preston v. Marathon Oil Co., 684 F.3d 1276 (Fed. Cir. 2012).

365 *See*, *e.g.*, People v. Aleynikov, 104 N.E.3d 687 (N.Y. 2018) (setting boundaries between public domain and the company properties).

366 *See*, *e.g.*, Waymo LLC v. Uber Techs., Inc., No. C 17-00939, 2017 U.S. Dist. LEXIS 73843 (N.D. Cal. May 15, 2017); Cadence Design Sys., Inc. v. Avant! Corp., 57 P.3d 647, 650 (Cal. 2002) ("California does not treat trade secrets as if they were property."); Hrdy, *supra* note 201, at 2411–13 (introducing the trial process of the *Waymo LLC v. Uber Techs., Inc.*); Risch, *supra* note 72, at 24–25.

367 *See generally* CHARLES DOYLE, CONG. RES. SERV., R42681, STEALING TRADE SECRETS AND ECONOMIC ESPIONAGE: AN OVERVIEW OF THE ECONOMIC ESPIONAGE ACT (Aug. 19, 2016), https://fas.org/sgp/crs/secrecy/R42681.pdf (explaining the EEA mechanism); Lobel, *supra* note 168, at 802–03 (suggesting that the scope of the EEA definition of trade secrets is broader than the UTSA).

368 *But see generally* Fishman & Varadarajan, *supra* note 180 (proposing applying copyright similarity standards for the determination of trade secret misappropriations, which ignores the importance of employee loyalty and may induce more moral-hazard issues).

information asymmetries, which result in moral-hazard issues, decrease innovation efficiency. When enforcing CNCs, NDAs, and trade secret law, courts need to balance between promoting innovation incentives and over-rewarding first-mover advantages. NDAs need to be narrowly enforced but supplemented by trade secret law or CNCs. However, CNCs are less efficient than trade secret law in terms of promoting innovation. Contracts and trade secret law cannot eliminate but may aggravate the information asymmetries, which need to be alleviated by improving employee loyalty under internal management and the law that does not harm employee loyalty.

Appendix

State	**USTA**	**CNC**	**IDD/Actual or Threatened Misappropriation**
Arizona	Yes	Yes. *See* Gann v. Morris, 596 P.2d 43 (Ariz. Ct. App. 1979).	Not clear/decided.
Arkansas	Yes	No. *See* Bendinger v. Marshalltown Trowel Co., 994 S.W.2d 468 (Ark. 1999).	IDD. *See* Bendinger v. Marshalltown Trowel Co., 994 S.W.2d 468 (Ark. 1999).
California	Yes	No. *See* CAL. BUS. & PROF. CODE §§ 16600–17365 (West 2020).	Actual harm & no IDD. *See* Whyte v. Schlage Lock Co., 125 Cal. Rptr. 2d 277 (Cal. Ct. App. 2002).
Colorado	Yes	No. *See* Saturn Sys., Inc. v. Militare, 252 P.3d 516 (Colo. App. 2011).	Not clear/decided.
Connecticut	Yes	Yes. *See* Aetna Ret. Servs. v. Hug, No. CV 970479974S, 1997 Conn. Super. LEXIS 1781 (Conn. Super. Ct. June 18, 1997).	IDD. *See* Aetna Ret. Servs. v. Hug, No. CV 970479974S, 1997 Conn. Super. LEXIS 1781 (Conn. Super. Ct. June 18, 1997).
Delaware	Yes	Yes. *See* W.L. Gore & Assocs. v. Wu, C.A. No. 263-N, 2006 Del. Ch. LEXIS 65 (Del. Ch. Mar. 30, 2006).	IDD. *See* E. I. Du Pont De Nemours & Co. v. Am. Potash & Chem. Corp., 200 A.2d 428 (Del. Ch. 1964).
Florida	Yes	No, but plausibly applicable. *See* Fountain v. Hudson Cush-N-Foam Corp., 122 So. 2d 232 (Fla. Dist. Ct. App. 1960).	Threatened harm. *See* Del Monte Fresh Produce Co. v. Dole Food Co., Inc., 148 F. Supp. 2d 1326 (S.D. Fla. 2001).
Georgia	Yes	Yes, but limited applicability to key employees. *See* GA. CODE. ANN. § 13-8-50 (2020); Blair v. Pantera Enters., Inc.,	IDD. *See* Essex Grp., Inc. v. Southwire Co., 501 S.E.2d 501 (Ga. 1998).

		824 S.E.2d 711 (Ga. Ct. App. 2019).	
Illinois	Yes	No. *See* 820 ILL. COMP. STAT. 90/10 (2017).	IDD. *See* 765 ILL. COMP. STAT. 1065/3(a) (2009); PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995).
Indiana	Yes	No. *See* Bridgestone/Firestone, Inc. v. Lockhart, 5 F. Supp. 2d 667 (S.D. Ind. 1998).	IDD, *See* Ackerman v. Kimball Int'l, Inc., 652 N.E. 2d 507 (Ind. 1995).
Iowa	Yes	Yes. *See* Lamp v. Am. Prosthetics, Inc., 379 N.W.2d 909 (Iowa 1986).	IDD. *See* Barilla Am., Inc. v. Wright, No. 4-02-CV-90267, 2002 U.S. Dist. LEXIS 12773 (S. D. Iowa July 5, 2002).
Kansas	Yes	Yes. *See* Idbeis v. Wichita Surgical Specialists, P.A., 112 P.3d 81 (Kan. 2005).	IDD. *See* Bradbury Co., Inc. v. Teissier-duCros, 413 F. Supp. 2d 1203 (D. Kan. 2006).
Kentucky	Yes	Yes. *See* Charles T. Creech, Inc. v. Brown, 433 S.W.3d 345 (Ky. 2014).	Actual harm & no IDD. *See* Invesco Inst. (N.A.), Inc. v. Johnson, 500 F. Supp. 2d 701 (W.D. Ky. 2007).
Louisiana	Yes	No. *See* LA. STATE. ANN. § 23:921 (2015).	IDD. *See* LA. STATE. ANN. § 51:1432 (1981).
Maryland	Yes	Yes, but not favored. *See* Millward v. Gerstung Int'l Sport Educ., Inc., 302 A.2d 14 (Md. 1973); Ecology Servs. v. Clym Envtl. Servs., LLC, 952 A.2d 999 (Md. Ct. Spec. App. 2008).	Actual harm & no IDD. *See* LeJeune v. Coin Acceptors, Inc., 849 A.2d 451 (Md. 2004).
Massachusetts	Yes	Yes. *See* MASS. GEN. LAWS ANN. ch. 149, § 24L (West 2018);	IDD. *See* ArchiText, Inc. v. Kikuchi, No. 90572, 2005 Mass. Super. LEXIS 487

		Boulanger v. Dunkin' Donuts Inc., 815 N.E.2d 572 (Mass. 2004).	(Sup. Ct. Mass. May 19, 2005).
Michigan	Yes	Yes, but not favored. *See* MICH. COMP. LAWS ANN. § 445.774a (West 2020); Huron Tech. Corp. v. Sparling, No. 316133, 2014 Mich. App. LEXIS 1675 (Mich. Ct. App. Sept. 11, 2014).	IDD. *See* MICH. COMP. LAWS ANN. § 445.1903 (West 1998).
Minnesota	Yes	Yes. *See* La Calhene, Inc. v. Spolyar, 938 F. Supp. 523 (W.D. Wis. 1996).	IDD. *See* La Calhene, Inc. v. Spolyar, 938 F. Supp. 523 (W.D. Wis. 1996).
Missouri	Yes	Yes. *See* Healthcare Servs. Ozarks, Inc. v. Copeland, 198 S.W.3d 604 (Mo. 2006).	IDD in legislation. *See* Mo. Rev. Stat. § 417.455.1. But no IDDs recognized in courts. *See* Panera, LLC v. Nettles, No. 4:16-cv-1191, 2016 U.S. Dist. LEXIS 101473 (E.D. Mo. Aug. 3, 2016).
Nevada	Yes	No. *See* NEV. REV. STAT. § 613.330 (2017).	No IDD. *See* Ginkgo v. V., No. CV16-01869, 2016 Nev. Dist. LEXIS 3183 (Nev. Dist. Ct. Dec. 5, 2016).
New Hampshire	Yes	No. *See* N.H. REV. STAT. ANN. § 275:70 (2014).	Threatened harm & no IDD. *See* N.H. REV. STAT. ANN. § 350-B:2 (1990); Allot Commc'ns., Ltd. v. Cullen, No. 10-E-0016, 2010 N.H. Super. LEXIS 11 (N.H. Superior Ct. Feb. 2, 2010).
New Jersey	Yes	Yes. *See* Nat'l Starch & Chem. Corp. v. Parker Chem. Corp., 530 A.2d 31 (N.J. Super. Ct. App. Div. 1987).	IDD. *See* Nat'l Starch & Chem. Corp. v. Parker Chem. Corp., 530 A.2d 31 (N.J. Super. Ct. App. Div. 1987).
New Mexico	Yes	Yes. *See* Bowen v. Carlsbad Ins. & Real Estate Inc.,	Not clear/decided. *See* Insure N.M., LLC v. McGonigle, 995 P.2d 1053 (N.M. Ct. App. 2000).

		724 P.2d 223 (N.M. 1986).	
New York	No	Yes, but not favored. *See* BDO Seidman v. Hirshberg, 712 N.E.2d 1220 (N.Y. 1999); Sutherland Glob. Servs., Inc. v Stuewe, 902 N.Y.S.2d272 (N.Y. App. Div. 2010).	IDD. *See* Spinal Dimensions, Inc. v. Chepenuk, No. 4805–07, 2007 WL 2296503 (N.Y. Sup. Ct. 2007).
North Carolina	Close	Yes. *See* N.C. GEN. STAT. ANN. § 75-4 (2005).	IDD. *See* Travenol Labs., Inc. v. Turner, 228 S.E.2d 478 (N.C. Ct. App. 1976).
Ohio	Yes	Yes. *See* P & G v. Stoneham, 747 N.E.2d 268 (Ohio Ct. App. 2000).	IDD. *See* P & G v. Stoneham, 747 N.E.2d 268 (Ohio Ct. App. 2000).
Oregon	Yes	Yes, but can be voidable. *See* OR. REV. STAT. § 653.295 (2020).	Yes. *See* OR. REV. STAT. § 653.295 (2020).
Pennsylvania	Yes	Yes. *See* Pittsburgh Logistics Sys., Inc. v. BeeMac Trucking, LLC, 202 A.3d 801 (Pa. Super. Ct. 2019).	IDD. *See* 12 PA. STAT. AND. CONS. STAT. ANN. §§ 5302–03 (West 2004).
Texas	Yes	Yes. *See* TEX. BUS. & COM. CODE § 15.50 (West 2009).	Actual harm & no IDD. *See* Cardinal Health Staffing Network. Inc. v. Bowen, 106 S.W.3d 230 (Tex. App. 2003).
Utah	Yes	Yes. *See* TruGreen Cos., L.L.C. v. Mower Bros., Inc., 199 P.3d 929 (Utah 2008).	Threatened harm. *See* CDC Restoration & Constr., LC v. Tradesmen Contractors., LLC, 274 P.3d 317 (Utah Ct. App. 2016).
Vermont	Yes	Yes, but not favorable. *See* Dicks v. Jensen, 768 A.2d 1279 (Vt. 2001).	Not clear/decided. *See* Davison v. Caleidoscope Commc'n. Co., No. S0436-04, 2004 Vt. Super. LEXIS 88 (Vt. Nov. 8, 2004).
Virginia	Yes	Yes.	Threatened harm & no IDD.

		See Assurance Data, Inc. v. Malyevac, 747 S.E.2d 804 (Va. 2013).	*See* Motion Control Sys., Inc. v. East., 546 S.E.2d 424 (Va. 2001).
Washington	Yes	Yes. *See* Sheppard v. Blackstock Lumber Co., 540 P.2d 1373 (Wash. 1975).	IDD. *See* Moore v. Commercial Aircraft Interiors, LLC, 278 P.3d 197 (Wash. Ct. App. 2012).