Vanderbilt Law Review

Volume 71
Issue 3 *Issue 3 - April 2018*

Article 6

4-2018

Combating the Enemy Within: Regulating Employee Misappropriation of Business Information

Danielle J. Reid

Combating the Enemy Within: Regulating Employee Misappropriation of Business Information

Technological advancements vastly improve efficiency and productivity in the workplace. However, technology also brings with it the ability to transmit mass amounts of business information with ease. As technology continues to evolve and become increasingly prevalent in the modern workplace, the insider presents a considerable threat to employers. In fact, employers increasingly face disgruntled employees who are all too eager to download their employers' sensitive, confidential, and proprietary information before terminating the employment relationship. However, the digital age, a global economy, and a highly mobile workforce have rendered the law utterly unreliable in addressing employee misappropriation. In enacting the Defend Trade Secrets Act ("DTSA") in 2016, Congress sought to provide clear rules and predictability for everyone involved. Yet, the DTSA has already proven inadequate in creating any reliable expectations for employers or employees. This Note thus advocates for comprehensive statutory reform to address the unreliable legal framework. Specifically, this Note proposes that Congress amend the Computer Fraud and Abuse Act to limit its application in the employment context, and amend the DTSA to provide the Federal Trade Commission with the authority to regulate trade secret misappropriation.

INTRODUCTION

Imagine a scenario in which a trusted and loyal employee has access to a computer database containing confidential and proprietary information belonging to the employer. The employee's access to this information is vital to the efficient and successful operation of the employer's business. After some time, the employee becomes unhappy with his employer and resigns. Subsequently, the employer logs on to the employee's computer and discovers that the departing employee recently emailed a mass amount of the employer's confidential and proprietary information to his personal email account. The employer immediately panics, given that it must expend significant resources to determine exactly what information the employee has obtained, whether there was a data breach that must be reported to a proper authority, and what the employee might do with the information.

Unfortunately, this scenario is increasingly prevalent in the modern workplace and can be a potential nightmare for employers. It has become commonplace for employers to use electronic databases to store proprietary information, such as customer lists, financial data, and corporate strategies.[1] There is no question that technological advancements enabling the storage and transmission of mass amounts of information effectuate efficiency and productivity in the modern workplace; however, such advances also place a greater burden on employers seeking to protect proprietary and confidential information stored on computer databases.[2] In the ordinary course of business, it is

1. *See, e.g.*, Audra A. Dial & John M. Moye, *The Computer Fraud and Abuse Act and Disloyal Employees: How Far Should the Statute Go to Protect Employers from Trade Secret Theft?*, 64 HASTINGS L.J. 1447, 1448 (2013) (noting that employers now store business documents on electronic servers rather than in physical file cabinets).

2. *See, e.g.*, *Economic Espionage and Trade Secret Theft: Are Our Laws Adequate for Today's Threats?: Hearing Before the Subcomm. on Crime & Terrorism of the S. Comm. on the Judiciary*, 113th Cong. 8–9 (2014) (statement of Peter L. Hoffman, Vice President, Intellectual Property

often necessary for employers to allow certain employees to access proprietary information.[3]

Employers have long turned to trade secret law for a potential remedy against employees who misappropriate this proprietary information.[4] However, trade secret protection has become more difficult due to technological innovations, the pervasive use of smart devices, the ease with which data can be downloaded and disseminated, and the increased mobility of employees. In fact, it is often unclear what proprietary information even qualifies for protection as a trade secret.[5] Accordingly, as more business information is stored electronically, employers often turn to state computer fraud laws and the federal Computer Fraud and Abuse Act ("CFAA")—the application of which remains uncertain and inconsistent among jurisdictions.[6] Thus, the legal framework within which employers can protect their valuable business information is presently unclear, leaving employers and employees without guidance as to their legal rights and obligations regarding the use and protection of proprietary information.

To address this vast uncertainty, this Note advocates for comprehensive statutory reform of the current legal framework to provide both predictability and reliability in the regulation of the use and protection of business information. Part I introduces the competing policy considerations underlying the protection of business information and the current threats facing employers. Part II explores the laws

---

Management, The Boeing Company) ("[T]oday companies cannot simply lock their trade secrets in a safe. The vast majority of our business and engineering information is stored electronically. The digital age has brought great gains in productivity but also has increased risk."); S. REP. NO. 114-220, pt. 1, at 2 (2016) ("Protecting trade secrets has become increasingly difficult given ever-evolving technological advancements."); Thomas E. Booms, Note, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 545 (2011) ("Computers confer substantial benefits to employers by measurably increasing worker efficiency and allowing for greater connectivity between enterprises and individuals."); Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 204–05 (2012) ("One of a business's largest risks is the threat of the malicious insider.").

3. Of course, an employee's use of an employer's computer system and information generally is limited to some degree and may be governed by a computer or acceptable use policy. *See* Dial & Moye, *supra* note 1, at 1448 ("Many employers require their employees to follow 'computer use' policies . . . ."); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1645 (2003) ("[A]n owner may attempt to regulate computer privileges . . . by contract. The owner can condition use of the computer on a user's agreement to comply with certain rules.").

4. *See generally* Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429 (discussing trade secret law).

5. *See infra* Section II.B.

6. *See infra* Section II.C.

governing employment relationships, with a focus on the inadequate remedies currently available to employers. Part III proposes a reform that codifies reliable expectations for both employers and employees and simplifies enforcement. Specifically, it argues that Congress should amend the CFAA to limit its application in the employment context. It further contends that Congress should amend the recently enacted Defend Trade Secrets Act ("DTSA") to grant the Federal Trade Commission ("FTC") authority to implement and administer the civil provisions of the DTSA. Under this framework, the crux of trade secret protection would be pursued through a civil regime, with the Department of Justice ("DOJ") retaining authority to prosecute violations of the criminal prohibition of theft of trade secrets. In short, this Note exposes the unworkability of the current legal framework as it operates in the digital age and proposes statutory reform to effectuate a much-needed change in the regulation of employee misappropriation of business information.

I. IDENTIFYING THE ENEMY

Business information accounts for much of an employer's most valuable assets. This information includes business strategies, pricing and financial data, customer lists, data compilations, and reports. To accord the ideal amount of protection for business information, the law must strike a balance between the competing interests of employers, employees, and society. The digital age complicates this balance, rendering the current legal framework in dire need of change. Section A first discusses the competing policy interests underlying the protection of business information. Section B then explores the complications facing the modern workplace arising from technological advancements.

A. Competing Policy Interests

Employers have a legitimate interest in protecting their business information from unauthorized use or disclosure.[7] Protecting confidential business information is essential to a company's ability to develop products, provide services, and gain economic advantages. Employers spend significant amounts of time and money developing their business information because it contributes to their ability to

7. *See, e.g.*, RESTATEMENT OF EMP'T LAW § 8.07(b)(1) (AM. LAW INST. 2015) (stating that employers have a legitimate interest in protecting "trade secrets . . . and other protectable confidential information that does not meet the definition of trade secret").

maintain their competitive position and financial success. Business information can be extremely valuable not only to the employer but also to both rivals and employees (who can use it to compete)—leaving the information vulnerable to misappropriation. Misuse or disclosure of this information can significantly impair, or even destroy, the value of the information.

Employers have a strong interest in efficient business operations, and adequate protection of proprietary information is vital to maintaining such efficiency.[8] Employers must be able to communicate business information with employees who act and make decisions on behalf of their employers. Yet, employers would be hesitant to fully communicate with their employees if business information is not adequately protected from misappropriation.[9] Thus, too little protection of business information frustrates the communication necessary for efficient business operations.

On the other hand, employees have a strong interest in employment mobility, which can be compromised if the law affords business information too much protection. Providing too much protection of business information inhibits an employee's ability to move between jobs and to use the knowledge and skills gained during former employment. Imagine a lawyer who cannot tap into her wealth of knowledge (about the local court rules, substantive law, etc.) learned at one firm when she laterals to another. Employment mobility allows employees to pursue better opportunities, obtain increased wages, and escape toxic employers.[10] In fact, in the absence of special circumstances, the default rule in all U.S. jurisdictions is employment at will—which allows either the employer or employee to terminate the

8. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 481–82 (1974) (discussing the policy rationales behind trade secret law); Winston Research Corp. v. Minn. Mining & Mfg. Co., 350 F.2d 134, 138 (9th Cir. 1965) ("Unless protection is given against unauthorized disclosure of confidential business information by employees, employee-employer relationships will be demoralized; employers will be compelled to limit communication among employees with a consequent loss in efficiency; and business, espionage, deceit, and fraud among employers will be encouraged."); Jay Dratler, Jr., *Trade Secrets in the United States and Japan: A Comparison and Prognosis*, 14 YALE J. INT'L L. 68, 69 (1989) ("Trade secret law performs two vital functions: encouraging individual effort and investment in research and development and helping maintain 'standards of commercial ethics.' ").

9. *See Winston Research Corp.*, 350 F.2d at 138 (articulating that employers will be hesitant to communicate with employees if unauthorized disclosure of business information is not restricted).

10. *See* Matthew C. Palmer, Note, *Where Have You Gone, Law and Economics Judges? Economic Analysis Advice to Courts Considering the Enforceability of Covenants Not to Compete Signed After At-Will Employment Has Commenced*, 66 OHIO ST. L.J. 1105, 1124–25 (2005) (analyzing economics behind at-will employment doctrine).

employment relationship at any time and for any reason.[11] Unless the employer and employee agree otherwise, the at-will default rule enables employees to move freely between jobs.[12] This freedom to move between employers allows employees to continue growing their knowledge, skills, and experience.

Additionally, society as a whole has a strong interest in how much protection the law affords business information. The public desires innovative products and vigorous competition in the workplace. "The heart of our national economic policy long has been faith in the value of competition."[13] Competition produces lower prices and better goods and services.[14] Because of the importance of competition in our society, competitive behavior has long been regulated at the federal level.[15]

In sum, too much protection for employers diminishes healthy competition and reduces market efficiency.[16] Overprotecting business information can deter potential competitors from entering the market.[17] Constraining competition impedes the dissemination of ideas and processes and inhibits the market from channeling labor to its greatest productivity.[18] Yet, too little protection discourages innovation—which is essential to generating change, enhancing quality, and reducing prices. Employers can gain a competitive advantage through valuable developments and improvements; however, employers cannot afford to subsidize the costs of the necessary research and development without assurance that valuable developments will not be misappropriated[19]—

---

11. *See, e.g.*, Hanson v. Cent. Show Printing Co., 130 N.W.2d 654, 655–56 (Iowa 1964) (noting that absent a stipulation as to the duration of an employment relationship, employment contracts are no more than an indefinite general hiring terminable by either party); RESTATEMENT OF EMP'T LAW § 2.01 ("Default Rule of an At-Will Employment Relationship").

12. *See* 2 MARK A. ROTHSTEIN ET AL., EMPLOYMENT LAW § 8:4, at 521 (5th ed. 2014) ("[A]n at-will employee is as free to sever the employment relationship as the employer, and has no obligation to the former employer other than fiduciary obligations not to reveal trade secrets or otherwise to engage in tortious interference with business." (footnote omitted)).

13. Nat'l Soc'y of Prof'l Eng'rs v. United States, 435 U.S. 679, 695 (1978) (internal quotation marks omitted) (quoting Standard Oil Co. v. FTC, 340 U.S. 231, 248 (1951)).

14. *See, e.g.*, *Nat'l Soc'y of Prof'l Eng'rs*, 435 U.S. at 695 (discussing legislative intent behind the Sherman Act, which governs competition law).

15. *See, e.g.*, 15 U.S.C. § 1 (2012) ("Every contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade . . . is declared to be illegal."); *id.* § 45(a)(1)–(2) (declaring unfair methods of competition unlawful and empowering the FTC to prevent unfair methods of competition).

16. *See* Harlan M. Blake, *Employee Agreements Not to Compete*, 73 HARV. L. REV. 625, 627 (1960) (discussing the effect of postemployment restraints).

17. *Id.*

18. *Id.*

19. *See* Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 482 (1974) (noting that encouraging invention is one of the major policy objectives of trade secret law); Water Servs., Inc. v. Tesco Chems., Inc., 410 F.2d 163, 171 (5th Cir. 1969) ("If a trade secret is protected, the competitive

slowing the development of innovations that could raise quality of life for everyone.[20] Determining the amount of protection the law should provide business information is thus a delicate balance of competing societal interests.

B. Technology: Demoralizing the Employment Relationship

Technological advancements impact nearly every aspect of our lives, and the pervasive influence of technology is especially felt in the workplace.[21] Although technology can increase efficiency and productivity in the workplace, it also enables easier access to an employer's valuable business information. As such valuable assets become more easily copied and distributed, employment mobility exacerbates the risk to employers of employee misappropriation of business information.

Employers increasingly encounter employees who abuse computer privileges to steal massive amounts of business information.[22]

---

advantage realized by the owner of the secret will enable him to recoup his development costs, hopefully before his competitors can 'reverse-engineer' the product and duplicate it."); Progressive Prods., Inc. v. Swartz, 258 P.3d 969, 976 (Kan. 2011):

> [T]he law of trade secrets recognizes that private parties invest extensive sums of money in certain information that loses its value when published to the world at large. . . . In doing so, the law allows the trade secret owner to reap the fruits of its labor and protects the owner's moral entitlement to these fruits. . . . Without trade secret protection, organized scientific and technological research could become fragmented, and society as a whole could suffer.;

Wexler v. Greenberg, 160 A.2d 430, 435 (Pa. 1960) ("Without some means of post-employment protection to assure valuable developments or improvements are exclusively those of the employer, the businessman could not afford to subsidize research or improve current methods."); *see also* OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: S. 1890 – DEFEND TRADE SECRETS ACT (2016), http://www.presidency.ucsb.edu/ws/index.php?pid=117358 [https://perma.cc/9KKA-8SJL] [hereinafter STATEMENT OF ADMINISTRATION POLICY] ("Effective protection of trade secrets promotes innovation that is the engine of the Nation's economy . . . ."); *cf.* Remarks by the President at Signing of S. 1890 – Defend Trade Secrets Act of 2016, 2016 DAILY COMP. PRES. DOC. 00309 (May 11, 2016):

> As many of you know, one of the biggest advantages that we've got in this global economy is that we innovate, we come up with new services, new goods, new products, new technologies. Unfortunately, all too often, some of our competitors, instead of competing with us fairly, are trying to steal these trade secrets from American companies. And that means a loss of American jobs, a loss of American markets, a loss of American leadership.

20. *See* H.R. REP. NO. 114-529, at 3 (2016).

21. *See* Dial & Moye, *supra* note 1, at 1448.

22. *See* Matthew Kapitanyan, *Beyond* WarGames*: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL'Y FOR INFO. SOC'Y 405, 407–09 (2012) (discussing the increased prevalence of internal data theft); Warren Thomas, Note, *Lenity on Me:* LVRC Holdings LLC v. Brekka *Points the Way Toward Defining Authorization and Solving the Split over the Computer Fraud and Abuse Act*, 27 GA. ST. U. L. REV. 379, 379 (2011) ("According to one recent survey, almost 60% of employees who leave their jobs take company data with them.

By way of illustration, consider the representative case of *WEC Carolina Energy Solutions LLC v. Miller*.[23] In *Miller*, the defendant worked as a project manager for a company that provided welding services to the power generation industry.[24] During his employment with the company, the defendant had access to the company's intranet and computer servers, enabling him to access numerous confidential and trade secret documents, including pricing terms, pending projects, and the company's technical capabilities.[25] Upon terminating his employment with the company, the defendant went to work for a competitor.[26] Prior to his resignation, however, the defendant downloaded a substantial number of the company's confidential documents and emailed them to his personal email account.[27] The defendant's previous company sued the employee and its competitor—alleging nine state law causes of action and a violation of the CFAA—after the defendant used this information in a presentation to win a project from a potential customer.[28] The court concluded, however, that the employer did not state a claim under the CFAA and dismissed the remaining claims for lack of jurisdiction.[29]

As *Miller* illustrates, the current threat to employers is significant because much of their business information is integral to their competitive advantage in today's economy.[30] Yet, such information is highly susceptible to theft given increased digitization of critical data and the ease with which employees can take this information by simply emailing it to a personal email account or downloading it to a flash drive.[31] Indeed, according to a 2016 study analyzing the state of cybersecurity and digital trust, sixty-nine percent of companies have experienced data theft by corporate insiders over the last twelve months.[32] Some estimate that damage to companies from data theft

---

Indeed, technological advances have made it easier than ever for employees to walk out the door with confidential information: 'The digital world is no friend to trade secrets.' " (footnote omitted) (quoting Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 361 (2009))).

23. 687 F.3d 199 (4th Cir. 2012).

24. *Id.* at 201–02.

25. *Id.* at 202.

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.* at 207 ("[W]e hold that WEC failed to state a claim for which the CFAA can grant relief . . . . Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees."); *see also infra* Section II.C.

30. *See* H.R. REP. NO. 114-529, at 3 (2016) (explaining the need for DTSA).

31. *Id.*

32. ACCENTURE & HFS RESEARCH, LTD., THE STATE OF CYBERSECURITY AND DIGITAL TRUST 2016: IDENTIFYING CYBERSECURITY GAPS TO RETHINK STATE OF THE ART 9 (2016),

could rise to ninety trillion dollars per year by 2030 if current trends continue.[33] Thus, the threat of employee misappropriation is extremely costly to employers.

II. NAVIGATING THE CURRENT LEGAL FRAMEWORK

An employer's right to protect its business information arises out of contractual agreements with employees, the duty of loyalty, statutory protection against misappropriation of trade secrets, and arguably federal and state computer fraud laws.[34] However, the laws governing competitive behavior of employees offer little certainty for employers and employees alike. To demonstrate this uncertainty, this Part addresses the current legal framework, ultimately showing that it provides inadequate protection to business information. First, Section A discusses two sources of state law governing employment relationships and introduces employers' legal remedies against employees who misappropriate business information. Section B then explores and analyzes the laws governing misappropriation of trade secrets. Finally, Section C introduces the CFAA and analyzes its applicability in the employment context.

A. Laws Governing the Employment Relationship

Contract and agency laws are two of the primary sources of law governing the employment relationship.[35] As such, employers may attempt to protect their information by relying on the enforcement of contractual postemployment restraints on competition and breach of fiduciary duty claims.[36] However, even in combination, these laws

---

https://www.accenture.com/t20160704T014005__w__/us-en/_acnmedia/PDF-23/Accenture-State-Cybersecurity-and-Digital-Trust-2016-Report-June.pdf#zoom=50 [https://perma.cc/7AGJ-S7JW]; *see also* Matthew Kalman, *Two-Thirds of Companies See Insider Data Theft, Accenture Says*, BLOOMBERG: TECH. (June 26, 2016, 7:13 AM), https://www.bloomberg.com/news/articles/2016-06-26/two-thirds-of-companies-see-insider-data-theft-accenture-says [https://perma.cc/ENN7-BKPN] (discussing the Accenture study); *Data Theft by Employees Affects 69% of Businesses: Accenture Survey*, INS. J. (June 27, 2016), http://www.insurancejournal.com/news/international/2016/06/27/418402.htm [https://perma.cc/3MCE-D2DD] (same).

33. Kalman, *supra* note 32.

34. *See infra* Section II.C.

35. *See, e.g.*, Fadeyi v. Planned Parenthood Ass'n of Lubbock, Inc., 160 F.3d 1048, 1051 (5th Cir. 1998) ("[A]n employment-at-will relationship is a contractual one, even though either party can terminate it without cause at any time."); RESTATEMENT (THIRD) OF AGENCY § 7.07(3)(a) (AM. LAW INST. 2006) ("An employee is an agent whose principal controls or has the right to control the manner and means of the agent's performance of work."); 1 ROTHSTEIN, *supra* note 12, § 1:29, at 153 ("[T]he employer-employee relationship is a contractual relationship.").

36. *See, e.g.*, Tradesman Int'l, Inc. v. Black, 724 F.3d 1004, 1006 (7th Cir. 2013) (listing counts alleged in employer lawsuit against former employees who opened a competing business).

(which have been used for decades to protect employers) are inadequate in today's technology driven world.

1. A Contractual Relationship

Despite the default rule of employment at will, most employment relationships are contractual.[37] Accordingly, an employer can attempt to protect its confidential business information by relying on contractual rights and remedies. For example, employers may include general confidentiality clauses in their employment contracts, which define the information the employer intends to protect and the employee's obligations to keep the information confidential.[38] Consequently, the employer has a potential claim under state law against any employee who breaches this contract by disclosing confidential information.

To extend protection of business information beyond the duration of the employment relationship, employers may enter into additional contractual agreements with their employees as a means of constraining postemployment competition.[39] Such agreements include nonsolicitation clauses, nondisclosure agreements, and covenants not to compete.[40] The least restrictive of these agreements is a nonsolicitation agreement, which is simply a commitment not to solicit the employer's clients or customers.[41] A nondisclosure agreement—which is slightly more restrictive—is a commitment not to disclose any

---

37. *See, e.g.*, *Fadeyi*, 160 F.3d at 1051 (noting that employment relationships are contractual).

38. *See, e.g.*, Unisource Worldwide, Inc. v. Valenti, 196 F. Supp. 2d 269, 273 (E.D.N.Y. 2002):

> [Paragraph] 2. *Disclosure of Confidential Information.* I shall not at any time during the term of my employment or thereafter, . . . use, publish, disclose or authorize anyone else to use, publish, or disclose any confidential information belonging to [the employer]. Confidential information includes, but is not limited to, models, drawings, memoranda and other materials, documents or records of a proprietary nature, information relating to research, finance, accounting, sales, personnel management and operations; and information particularly relating to customer lists, price lists, customer service requirements, costs of providing service and equipment, pricing, and equipment maintenance costs.

39. *See* Blake, *supra* note 16, at 625–26 (noting that employees may enter into covenants not to compete with their employers).

40. *See, e.g.*, Outsource Int'l, Inc. v. Barton, 192 F.3d 662, 665 (7th Cir. 1999) ("The Employment Agreement contained confidentiality and non-compete clauses as conditions of [the employee's] employment."). If an employee breaches one of these agreements, the employer may pursue a breach of contract claim seeking injunctive relief or damages. *See, e.g.*, *id.* at 666; Reliable Fire Equip. Co. v. Arredondo, 965 N.E.2d 393, 395 (Ill. 2011).

41. *See, e.g.*, Sevier Ins. Agency, Inc. v. Willis Corroon Corp. of Birmingham, 711 So. 2d 995, 997–1001 (Ala. 1998) (discussing nonsolicitation agreements), *overruled by* White Sands Grp., L.L.C. v. PRS II, LLC, 32 So. 3d 5 (Ala. 2009) (overruling *Sevier* and other cases to the extent they required proof of absence of justification as part of the prima facie case for wrongful interference with the business relationship).

confidential information learned during employment.[42] The most restrictive agreement—a noncompete—is a commitment not to engage in or start a similar profession or trade as that of the employer for a specified period of time following employment.[43]

The enforceability of these contractual agreements is uncertain at best.[44] Postemployment constraints on competition are considered to be in restraint of trade, and thus contrary to long-established public policy.[45] The policy against restraining trade is grounded in the resulting injury to the party restricted from competing and injury to the public through the deprivation of the restricted party's industry.[46] Moreover, many courts find that these agreements contravene public policy because they involve parties of unequal bargaining power and most employees are not given a real choice in accepting such agreements.[47] Since these contractual provisions are in tension with the default rule of employment at will and are contrary to public policy, they are subject to significant judicial scrutiny.[48] Courts will only enforce these contracts if they are reasonable in scope and protect the former employer's legitimate interests.[49] Courts have developed many tests to determine whether such agreements are reasonable.[50] They

---

42. *See, e.g.*, Innovation Ventures v. Liquid Mfg., 885 N.W.2d 861, 866 (Mich. 2016) (describing a nondisclosure agreement).

43. *See, e.g.*, Blake, *supra* note 16, at 625–26.

44. *See, e.g.*, Marsh USA Inc. v. Cook, 354 S.W.3d 764, 768–76 (Tex. 2011) (discussing the enforceability of covenants not to compete); *see also* Daniel P. O'Gorman, *Contract Theory and Some Realism About Employee Covenant Not to Compete Cases*, 65 SMU L. REV. 145, 147–48 (2012) (noting that even within a jurisdiction it is difficult to predict how a trial court will respond to a noncompetition agreement).

45. *See, e.g.*, Or. Steam Navigation Co. v. Winsor, 87 U.S. (20 Wall.) 64, 66 (1873) ("It is a well-settled rule of law that an agreement in general restraint of trade is illegal and void . . . .").

46. *Id.* at 68:

> There are two principal grounds on which the doctrine is founded, that a contract in restraint of trade is void as against public policy. One is, the injury to the public being deprived of the restricted party's industry; the other is, the injury to the party himself by being precluded from pursuing this occupation and thus being prevented from supporting himself and his family.

47. *See, e.g.*, Malic v. Coloplast Corp., 629 S.E.2d 95, 99 (Ga. Ct. App. 2006) (noting that most restrictive covenants in employment contracts are reviewed under strict scrutiny because they involve parties of unequal bargaining power, are drafted by the employer, and generally give the employee a take it or leave it choice); *see also* Rachel Arnow-Richman, *Cubewrap Contracts and Worker Mobility: The Dilution of Employee Bargaining Power via Standard Form Noncompetes*, 2006 MICH. ST. L. REV. 963 (discussing the lack of employee bargaining power when signing noncompetes).

48. *See generally* Palmer, *supra* note 10, at 1126–30 (discussing the enforcement of restrictive covenants in employment-at-will relationships).

49. *See, e.g.*, Blake, *supra* note 16, at 649; Palmer, *supra* note 10, at 1127.

50. *See, e.g.*, Eldridge v. Johnston, 245 P.2d 239, 250 (Or. 1952):

> Three things are essential to the validity of a contract in restraint of trade: (1) it must be partial or restricted in its operation in respect either to time or place; (2) it must be

generally will only enforce the noncompete if the restriction is limited in geographic scope and duration, is not harmful to the general public, and is not unreasonably burdensome on the employee.[51] And, because of wide variations in approaches to noncompetition agreements, a court's choice of law will often be decisive.[52]

Because of the questionable enforceability of these agreements, employers cannot rely on contractual provisions to protect against employee theft of company data. Even if a court does find the existence of an agreement necessary to protect employers' legitimate interests—such as the maintenance of proprietary or confidential business information—the agreement must still be reasonable in other aspects to be enforceable. If an agreement is too broad in scope or is against public interest, courts might find it unreasonable notwithstanding the legitimate protectable interest.[53] Furthermore, states such as California refuse to recognize such agreements at all, deeming these restraints on trade unenforceable altogether as against public policy.[54] The viability of these agreements as a means to protect employers from employee theft of company data is therefore uncertain at best, and as such, are an inadequate means for employers to protect themselves from disgruntled employees.

2. An Agency Relationship

Regardless of whether an employee is at will or subject to a contract, principles of agency law also govern employment relationships, as employees are agents of their employers during the

---

> on some good consideration; and (3) it must be reasonable, that is, it should afford only a fair protection to the interests of the party in whose favor it is made, and must not be so large in its operation as to interfere with the interests of the public.;

see also RESTATEMENT (SECOND) OF CONTRACTS § 188 (AM. LAW INST. 1981) ("(1) A promise to refrain from competition . . . is unreasonably in restraint of trade if (a) the restraint is greater than is needed to protect the promisee's legitimate interest, or (b) the promisee's need is outweighed by the hardship to the promisor and the likely injury to the public.").

51. *See, e.g.*, BDO Seidman v. Hirshberg, 712 N.E.2d 1220, 1223 (N.Y. 1999).

52. Tradesman Int'l, Inc. v. Black, 724 F.3d 1004, 1017 (7th Cir. 2013) (Hamilton, J., concurring). In some cases, this results in a race to the courthouse. *See, e.g.*, Advanced Bionics Corp. v. Medtronic, Inc., 59 P.3d 231 (Cal. 2002).

53. *See, e.g.*, MacGill v. Reid, 850 N.E.2d 926 (Ind. Ct. App. 2006) (concluding that although the employer had a legitimate protectable interest, the covenant was unreasonable in its scope and thus unenforceable).

54. CAL. BUS. & PROF. CODE § 16600 (West 2017) ("[E]very contract by which anyone is restrained from engaging in a lawful profession, trade, or business of any kind is to that extent void."); N.D. CENT. CODE § 9-08-06 (2018) ("Every contract by which anyone is restrained from exercising a lawful profession, trade, or business of any kind is to that extent void.").

term of employment.[55] Pursuant to agency law, agents have a fiduciary duty to act loyally for the principal's benefit in all matters connected with the relationship.[56] As such, employees generally "owe an undivided and unselfish loyalty to [their employer] during the term of their employment, such that there shall be no conflict between duty and self-interest."[57]

Many states recognize a cause of action for a breach of this duty of loyalty.[58] Employers may pursue breach of loyalty claims for predeparture activities, which typically involve an employee soliciting customers to open a competitive business, aiding a competitor and planning to join that competitor after termination of the employment relationship, or usurping a corporate opportunity.[59]

Agency law is also inadequate in protecting employers because of the significant limitations of fiduciary duty claims. An employer only has a claim for a breach of the duty of loyalty if the employee goes beyond mere planning and preparation and actually *engages in direct competition* with the employer *during* the term of the employment relationship.[60] The first limitation is that employees must engage in *direct competition* with the employer, which requires something more than agreeing, planning, or preparing to compete.[61] Thus, inchoate breaches of the duty of loyalty cannot serve as the basis of a colorable claim. These claims are further limited by the fact that the duty only lasts for the duration of the employment relationship. Thus, any use of misappropriated information following termination of the employment relationship would not constitute a breach of the employee's duty of

55. *See* RESTATEMENT (THIRD) OF AGENCY § 7.07(3)(a) (AM. LAW INST. 2006) ("[A]n employee is an agent whose principal controls or has the right to control the manner and means of the agent's performance of work . . . ."); *see also id.* § 1.01 ("Agency is the fiduciary relationship that arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act.").

56. *Id.* § 8.01.

57. Hedgeye Risk Mgmt., LLC v. Heldman, 196 F. Supp. 3d 40, 52 (D.D.C. 2016) (internal quotation marks omitted) (quoting Phillips v. Mabus, 894 F. Supp. 2d 71, 92 (D.D.C. 2012)).

58. *See, e.g.*, Scanwell Freight Express STL, Inc. v. Chan, 162 S.W.3d 477, 479 (Mo. 2005) (en banc) ("In the employer-employee relationship, this Court, drawing on the Restatement (2d) of Agency, has implicitly recognized a separate cause of action for b[r]each of the duty of loyalty . . . .").

59. *See* RESTATEMENT OF EMP'T LAW § 8.01(b) (AM. LAW INST. 2015).

60. *See, e.g.*, Jet Courier Serv., Inc. v. Mulei, 771 P.2d 486, 491–93 (Colo. 1989) (en banc); *Scanwell*, 162 S.W.3d at 477. For more information on the employee's duty of loyalty, see Catherine Fisk & Adam Barry, *Contingent Loyalty and Restricted Exit: Commentary on the* Restatement of Employment Law, 16 EMP. RTS. & EMP. POL'Y J. 413 (2012).

61. *Scanwell*, 162 S.W.3d at 479–80.

loyalty, so the employer would not have a valid fiduciary duty claim against the employee.[62]

B. Trade Secret Protection

Given the deficiencies demonstrated above under state contract and agency law, a more practical remedy for employers to protect proprietary information is through trade secret law, which does not require a contract specifically prohibiting the employee's use and disclosure of protected information.[63] Rather, trade secret law derives from notions of fair play and business ethics.[64]

Although trade secret law developed under the common law, most states today offer statutory protection of trade secrets.[65] Forty-eight states have enacted a version of the Uniform Trade Secrets Act ("UTSA"),[66] which codifies the common law principles of trade secret law. Under the UTSA, to qualify for trade secret protection, information must derive value from its secrecy and the employer must make reasonable efforts to maintain the information's secrecy.[67] An employer has a legal remedy when its trade secret is misappropriated, which the UTSA defines as:

> [D]isclosure or use of a trade secret of another without express or implied consent by a person who . . . at the time of disclosure or use, knew or had reason to know that his

---

62. *See Hedgeye*, 196 F. Supp. 3d at 53.

63. *See* Katherine V.W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 583–84 (2001) (noting that disclosure of trade secrets can be restrained in the absence of a specific covenant).

64. RINSDALE ELLIS, TRADE SECRETS, at iii (1953) ("In the absence of contract, the basis for [trade secret] protection is fair play and business ethics.").

65. Prior to states adopting the UTSA, most states recognized misappropriation of trade secrets as a common law tort claim. *See, e.g.*, Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 898 (Minn. 1983) (discussing the common law principles of trade secret law and stating that the UTSA clarifies many of the rules of the common law). A majority of the courts addressing the issue of whether the UTSA preempts state common law tort claims for misappropriation have held that it does. *See, e.g.*, Firetrace USA, LLC v. Jesclard, 800 F. Supp. 2d 1042, 1047–50 (D. Ariz. 2010).

66. *See* DAVID W. QUINTO ET AL., TRADE SECRETS: LAW AND PRACTICE § 1.01 (2017 ed.) (citing the trade secret statute of each state); *see also* Progressive Prods., Inc. v. Swartz, 258 P.3d 969, 976 (Kan. 2011) (stating that the UTSA seeks uniformity with other jurisdictions).

67. UNIF. 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: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

For a detailed description of the meaning of each element and how courts define what constitutes a trade secret under the UTSA, see QUINTO ET AL., *supra* note 66, § 1.03.

> knowledge of the trade secret was . . . acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use . . . .[68]

Though the classic example of a trade secret is the recipe for Coca-Cola,[69] employers today often seek trade secret protection for more general confidential business information, such as customer lists or business strategies.[70] Employers have even attempted to claim trade secret protection for employees' personal social media contacts.[71] With this expansion of information employers seek to protect, courts, employers, and employees face challenges in identifying what information constitutes a trade secret—a highly fact-intensive inquiry.[72]

Even if the information at issue involves a protectable subject matter, it can be particularly difficult to prove that the employer maintained adequate secrecy if numerous employees have access to the information on a computer database.[73] Developments in computer forensics have increased the ability of employers to track the downloading, copying, and emailing of files, which eases the burden on employers to demonstrate that an employee expropriated documents or files.[74] However, this can be an extremely costly endeavor for employers and such expenditures might not be worth the cost, especially when an employer is uncertain whether the allegedly misappropriated information qualifies for trade secret protection.

---

68. UNIF. TRADE SECRETS ACT § 1(2)(ii).

69. *See* TIMOTHY P. GLYNN ET AL., EMPLOYMENT LAW: PRIVATE ORDERING AND ITS LIMITATIONS 508 (3d ed. 2015) (explaining that the recipe for Coca-Cola is the paradigmatic trade secret, but it is more challenging today to identify what constitutes a trade secret); *see also* Spitz v. Proven Winners N. Am., LLC, 969 F. Supp. 2d 994, 1007 (N.D. Ill. 2013) ("Information that is generally known within an industry, even if not in the public at large, as well as information that can be readily duplicated without considerable time, effort, or expense, is not a trade secret.").

70. GLYNN ET AL., *supra* note 69, at 508; Catherine L. Fisk, *Working Knowledge: Trade Secrets, Restrictive Covenants in Employment, and the Rise of Corporate Intellectual Property*, 52 HASTINGS L.J. 441, 503–04 (2001) (describing the shift in what types of business assets employers claim as trade secrets).

71. *See, e.g.*, Cellular Accessories for Less, Inc. v. Trinitas LLC, No. CV 12-06736 DDP (SHx), 2014 WL 4627090, at *4 (C.D. Cal. Sept. 16, 2014) (finding that an issue of fact remains as to whether LinkedIn contacts are a protectable trade secret).

72. *See, e.g.*, Bradshaw v. Alpha Packaging, Inc., 379 S.W.3d 536, 541 (Ark. Ct. App. 2010) ("The question of what constitutes a trade secret is fact-intensive." (citing Vigoro Indus., Inc. v. Crisp, 82 F.3d 785 (8th Cir. 1996))).

73. *See, e.g.*, Natalie Flechsig, Note, *Trade Secret Enforcement After* TianRui*: Fighting Misappropriation Through the ITC*, 28 BERKELEY TECH. L.J. 449, 451 (2013) (noting that "[t]he danger of losing the secrecy status of a trade secret has increased with the advent of the Internet and a global workforce that has become highly mobile due to the increased collaboration between U.S. and foreign companies").

74. *See, e.g.*, Bimbo Bakeries USA, Inc. v. Botticella, 613 F.3d 102, 107–08 (3d Cir. 2010) (discussing revelations from testing by a computer forensics expert following departure of a high-level employee, including access patterns and use of external storage devices).

Thus, although once considered a reliable and adequate remedy for employers, the digitization of business assets and globalization of companies have rendered state trade secret law an uncertain and inconsistent legal regime. Although trade secret law has long been a matter of state law, Congress enacted the DTSA in 2016, creating a private federal cause of action for misappropriation of trade secrets.[75] The DTSA amended the Economic Espionage Act ("EEA"), which had previously made theft of trade secrets a federal crime but left civil remedies to state law.[76] In enacting the DTSA, Congress sought to address the concerns arising from a globalized economy and the movement of data across state lines.[77] Congress recognized that the variance in trade secret law among the states rendered it ineffective in a national and global economy, and suggested that federal courts are better situated to address trade secret misappropriation than state courts.[78] Thus, Congress enacted the DTSA in an attempt to provide "clear rules and predictability for everyone involved."[79]

The DTSA is in part modeled off of the UTSA.[80] The DTSA defines a trade secret as information that the owner has taken reasonable measures to keep secret and that derives independent economic value from not being generally known nor readily ascertainable through proper means.[81] Under the DTSA, the owner of a

---

75. *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (codified at 18 U.S.C. §§ 1832, 1833, 1836, 1839 (Supp. 2016)).

76. *See* 18 U.S.C. § 1832 (proscribing theft of trade secrets); H.R. REP. NO. 114-529, at 1, 4 (2016) (stating that the DTSA amends the EEA to provide a federal civil remedy for the misappropriation of trade secrets).

77. H.R. REP. NO. 114-529, at 4 ("The Defend Trade Secrets Act of 2016 (S. 1890) offers a needed update to Federal law to provide a Federal civil remedy for trade secret misappropriation.").

78. *Id.*

79. *Id.* at 6; *see also* STATEMENT OF ADMINISTRATION POLICY, *supra* note 19:

> The Administration strongly supports passage of [the DTSA], and appreciates the bipartisan effort that led to formulation of this bill . . . . [The DTSA] would establish a Federal civil private cause of action for trade secret theft that would provide businesses with a more uniform, reliable, and predictable way to protect their valuable trade secrets anywhere in the country.

80. H.R. REP. NO. 114-529, at 5 (noting that the DTSA's definition of misappropriation is modeled off of the UTSA).

81. 18 U.S.C. § 1839(3):

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper

trade secret has a private civil right of action for misappropriation if the trade secret is related to a product or service used in interstate or foreign commerce.[82] Mirroring the definition of the term under the UTSA, misappropriation under the DTSA includes acquisition by improper means and disclosure or use without consent.[83]

The DTSA, however, fails to promote uniformity and thus still lacks expectations upon which employers and employees can rely. Not only do employers now allege claims under both the DTSA and the applicable state's version of the UTSA, but decisions interpreting the DTSA also illustrate that federal courts look to state trade secret law from the state in which the court sits to analyze DTSA claims.[84] The DTSA has failed to produce case law independent of state trade secret laws such that trade secret law remains unpredictable among the states. Therefore, the uncertain and inconsistent legal framework will likely persist despite Congress's effort to establish uniformity and reliability.

C. The Computer Fraud and Abuse Act

Because so much of an employer's valuable business information is stored electronically, many employers have turned to computer fraud laws, including the CFAA and similar state statutes, to pursue claims against employees who misappropriate proprietary information using a computer.[85] Although originally enacted as a narrow antihacking

---

means by, another person who can obtain economic value from the disclosure or use of the information . . . .

82. *Id.* § 1836(b)(1).

83. *See id.* § 1839(5).

84. *See, e.g.*, Segerdahl Corp. v. Ferruzza, No. 17-CV-3015, 2018 WL 828062, at *2–3 (N.D. Ill. Feb. 10, 2018) (analyzing employer's claims under the DTSA and the Illinois Trade Secret Act ("ITSA") together); Openwave Messaging, Inc. v. Open-Xchange, Inc., No. 16-CV-00253, 2018 WL 692022, at *3–6 (N.D. Cal. Feb. 2, 2018) (analyzing employer's claims under the DTSA and California Uniform Trade Secret Act as one claim); Sterling Computs. Corp. v. Haskell, 4:17-CV-04073-KES, 2018 WL 671210, at *2–5 (D.S.D. Feb. 1, 2018) (analyzing employer's claims under the DTSA and UTSA together); Elsevier Inc. v. Doctor Evidence, LLC, 17-CV-5540, 2018 WL 557906, at *2–4 (S.D.N.Y. Jan. 23, 2018) (analyzing employer's claims under federal and New York trade secret law together); Kuryakyn Holdings, LLC v. Ciro, LLC, 242 F. Supp. 3d 789, 796–97 (W.D. Wis. 2017) (stating that "the court's analysis will use Wisconsin's UTSA, but the analysis would apply as well to the DTSA"); Mission Measurement Corp. v. Blackbaud, Inc., 216 F. Supp. 3d 915, 919–22 (N.D. Ill. 2016) (laying out federal and state trade secret law individually and then analyzing the two trade secret counts as one claim).

85. This Note discusses the federal Computer Fraud and Abuse Act, but most states have a statute with similar language under which employers may sue an employee. *See, e.g.*, MO. REV. STAT. § 569.095(1)(3) (2017) ("A person commits the offense of tampering with computer data if he or she knowingly and without authorization or without reasonable grounds to believe that he has such authorization . . . takes data . . . residing or existing internal or external to a computer, computer system, or computer network . . . .").

statute in 1984,[86] the rising presence of computers in the workplace, amendments expanding the scope of the act,[87] and the addition of a private civil right of action have led employers to increasingly rely on the CFAA to enforce computer use policies in the workplace.[88]

The CFAA in its current form defines several computer crimes.[89] Because Congress continually expands the scope of the CFAA,[90] the statute has played an increasingly important role in protecting employers from competition by former employees.[91] Prior to the enactment of the DTSA, employers often brought CFAA claims in conjunction with state trade secret claims as a way to bring the lawsuit in federal court.[92] Arguably, the DTSA alleviates the need for this strategy because it establishes federal question jurisdiction and allows employers to bring these suits in federal court.[93] However, because a CFAA claim does not require a noncompetition agreement or a finding that the information obtained constitutes a trade secret, employers

86. Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 1837 (codified as amended at 18 U.S.C. § 1030 (2012)) (defining three specific computer hacking crimes); *see also* Dial & Moye, *supra* note 1, at 1451 ("Originally, the CFAA was intended to be an anti-hacking statute."); David J. Schmidt, *The Computer Fraud and Abuse Act Should Not Apply to Misuse of Information Accessed with Permission*, 47 CREIGHTON L. REV. 423, 429 (2014) ("The legislative history demonstrates the CFAA was enacted as an anti-hacking statute.").

87. For a detailed analysis of the amendments to the Computer Fraud and Abuse Act, see Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–71 (2010).

88. *See* Taylor, *supra* note 2, at 208 ("The CFAA provides employers with a civil remedy in federal court, and it is increasingly used against former employees."); *see also* Booms, *supra* note 2, at 548–50 (discussing the increasingly broad scope of the CFAA and the benefits for employers resulting from civil actions against disloyal employees under the CFAA).

89. *See* 18 U.S.C. § 1030 (2012). The CFAA criminalizes using a computer to obtain national security information, accessing a computer without authorization or exceeding authorized access and thereby obtaining information, trespassing in a government computer, accessing a computer to defraud and obtain value, intentionally damaging a computer by knowing transmission, recklessly damaging a computer through intentional access, negligently causing damage and loss by intentional access, trafficking in passwords, and extorting by threatening to cause damage to a computer. *Id.*; *see also* COMPUT. CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 2 (2010), https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf [https://perma.cc/P4PZ-2SVE] [hereinafter PROSECUTING COMPUTER CRIMES] (summarizing CFAA penalties).

90. Kerr, *supra* note 87, at 1563–71 (discussing amendments to the CFAA).

91. *See* Kapitanyan, *supra* note 22, at 408–09 (discussing the prevalence of internal data theft); Booms, *supra* note 2, at 550 (discussing CFAA claims against disloyal employees); Taylor, *supra* note 2, at 208 ("The CFAA provides employers with a civil remedy in federal court, and it is increasingly used against former employees. Disgruntled employees who are about to resign often retain full access to computer systems and have the ability to copy data prior to their departure.").

92. *See, e.g.*, Booms, *supra* note 2, at 550 (noting that asserting a CFAA claim offers employers a doorway into federal court).

93. *See* 28 U.S.C. § 1331 (2012) ("The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.").

have continued (and likely will continue) bringing claims against employees under the CFAA even with the enactment of the DTSA.[94]

The broadest provision of the CFAA (and the most relevant in the employment context) provides that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished."[95] Although the CFAA was enacted as a criminal statute, it provides for a private civil cause of action if a CFAA violation results in one of five specified harms.[96] The most relevant in the employment context is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[97] Under the CFAA, loss includes the costs of investigation, forensic analysis, and other remedial measures incurred because of a violation of the CFAA.[98]

The CFAA contains a similarly broad definition of the term "computer,"[99] which "captures any device that makes use of a[n] electronic data processor."[100] A "protected computer" is any computer

---

94. *See, e.g.*, Segerdahl Corp. v. Ferruzza, No. 17-CV-3015, 2018 WL 828062, at *1 (N.D. Ill. Feb. 10, 2018) (listing claims alleged by employer, including claims under DTSA, ITSA, and CFAA); Teva Pharm. USA, Inc. v. Sandhu, No. 17-3031, 2018 WL 617991, at *2 (E.D. Pa. Jan. 30, 2018) (stating that employer brought claims under CFAA, DTSA, and Pennsylvania Uniform Trade Secrets Act); Frank N. Magid Assocs., Inc. v. Marrs, No. 16-CV-198-LRR, 2017 WL 3097257, at *1 (N.D. Iowa July 20, 2017) (discussing employer's claims against employee, including claims under both DTSA and CFAA); Chubb Ina Holdings Inc. v. Chang, No. 16-2354-BRM-DEA, 2017 WL 499682, at *11 (D.N.J. Feb. 7, 2017) (finding that employer stated claims under both CFAA and DTSA).

95. 18 U.S.C. § 1030(a)(2)(C) (2012).

96. *See id.* § 1030(g) (limiting the civil right of action to conduct involving one of the factors set forth in § 1030(c)(4)(A)(i)(I)–(V)); *id.* § 1030(c)(4)(A)(i)(I)–(V) (listing the following factors:

> (I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security).

97. *See id.* § 1030(c)(4)(A)(i)(I).

98. *See id.* § 1030(e)(11) (defining loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service"); Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting, LLC, 600 F. Supp. 2d 1045, 1052 (E.D. Mo. 2009) (holding that "the cost of the forensic analysis and other remedial measures associated with retrieving and analyzing Defendants' computers constitute 'loss' under [the] CFAA").

99. 18 U.S.C. § 1030(e)(1):

> "[C]omputer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device . . . .

100. United States v. Kramer, 631 F.3d 900, 902 (8th Cir. 2011).

"used in or affecting interstate or foreign commerce or communication."[101] It would be difficult to imagine a computer in the modern workplace that does not fit within this definition, as any computer connected to the internet affects interstate commerce and is therefore a protected computer.[102] Several courts have determined that an internet connection is sufficient to render a computer a protected computer under the CFAA.[103] For instance, in *United States v. Trotter*, the U.S. Court of Appeals for the Eighth Circuit explained that "[t]he Internet is an instrumentality and channel of interstate commerce," "[a]s both the means to engage in commerce and the method by which transactions occur."[104] As such, "[w]ith a connection to the Internet," a computer is "part of a system that is inexorably intertwined with interstate commerce," and therefore falls within the definition of a protected computer under the CFAA.[105]

For an employer to state a valid claim against a current or former employee under the broadest provision of the CFAA, then, an employer must allege that (1) the employee intentionally accessed a computer, (2) without authorization or exceeding authorized access, (3) thereby obtaining information, (4) from a protected computer, and (5) causing a loss suffered by one or more persons during any one-year period aggregating at least five thousand dollars.[106] Notably, the only element requiring an intentional act by the employee is the act of accessing the computer.

This private right of action enables employers to bring a claim against current or former employees who obtain information from a protected computer without authorization, or—as is more likely in the case of an employee—by exceeding authorized access and causing loss

---

101. 18 U.S.C. § 1030(e)(2)(B).

102. *See* PROSECUTING COMPUTER CRIMES, *supra* note 89, at 4 ("[I]t is enough that the computer is connected to the Internet; the statute does not require proof that the defendant also used the Internet to access the computer or used the computer to access the Internet."); Kerr, *supra* note 87, at 1570 ("[E]very computer around the world that can be regulated under the Commerce Clause is a 'protected computer' covered by 18 U.S.C. § 1030."); *see also* Shawn E. Tuma, *"What Does CFAA Mean and Why Should I Care?"—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 157 (2011) ("This . . . classification . . . essentially makes a protected computer out of every computer connected to the Internet and, quite possibly, every computer.").

103. *See, e.g.*, United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007).

104. 478 F.3d at 921 (internal quotation marks omitted) (quoting United States v. MacEwan, 445 F.3d 237, 245 (3d Cir. 2006)).

105. *Id.* (internal quotation marks omitted) (quoting *MacEwan*, 445 F.3d at 245).

106. 18 U.S.C. § 1030(a)(2)–(c)(2)(B)(iii); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009) (listing required elements for bringing an action under § 1030(g) based on a violation of § 1030(a)(2)).

to the employer.[107] With employers increasingly using a statute originally designed to prosecute external computer hackers against disloyal employees, courts are left to wrestle with the breadth of the CFAA and have struggled to interpret and apply it in the employment context.[108] Although the CFAA is a potentially powerful weapon for employers when employees misappropriate electronic information, its inconsistent application among circuits compromises its effectiveness.[109]

Interpretation of this statute, like any other, begins by looking to the text.[110] The CFAA does not define what it means for an individual to access a computer "without authorization," but does define the term "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that [the individual] is not entitled so to obtain or alter."[111] Thus, the term "exceeds authorized access" is generally understood to apply to the inside hacker ("who [is] authorized to access a computer"), as distinguished from the outside hacker ("who break[s] into a computer").[112] In the former case, the insider has allegedly exceeded his limited access by obtaining or altering information.[113]

Each of these phrases has generated interpretive issues. First, courts are split on whether an employee can access a computer "without authorization" by breaching his duty of loyalty, or if an employee accesses a computer "without authorization" only after the employer expressly revokes the employee's authorization.[114] Further, courts

---

107. *See, e.g.*, Taylor, *supra* note 2, at 208–09 (discussing the CFAA civil cause of action in the employment context).

108. Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615 (E.D. Pa. 2013) (citing P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, LLC, 428 F.3d 504, 510 (3d Cir. 2005)); *see also* Thomas, *supra* note 22, at 380 (" '[C]ourts have struggled over how to interpret the provisions of the CFAA' in the context of employer litigation over employees' misappropriation of data." (quoting ES & H, Inc. v. Allied Safety Consultants, Inc., No. 3:08-CV-323, 2009 WL 2996340, at *2 (E.D. Tenn. Sept. 16, 2009))).

109. *See, e.g.*, Dial & Moye, *supra* note 1, at 1449 ("[I]t has become unclear whether and to what extent the CFAA remains a viable method of enforcing the theft of electronic information by internal employees.").

110. *Cf.* Schindler Elevator Corp. v. United States *ex rel.* Kirk, 563 U.S. 401, 407 (2011) ("Because the statute does not define 'report,' we look first to the word's ordinary meaning." (citing Gross v. FBL Fin. Servs., Inc., 557 U.S. 167, 175 (2009); Asgrow Seed Co. v. Winterboer, 513 U.S. 179, 187 (1995))).

111. 18 U.S.C. § 1030(e)(6).

112. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (citing S. REP. NO. 104-357, at 11 (1996)); *see also* United States v. Nosal (*Nosal I*), 676 F.3d 854, 858, 863 (9th Cir. 2012).

113. PROSECUTING COMPUTER CRIMES, *supra* note 89, at 8.

114. *Compare* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that an employee's authorization to access a computer ended when the employee violated his duty of loyalty to his employer and accordingly the employee's actions were without authorization under the CFAA), *with* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009):

diverge on whether an employee "exceeds authorized access" in violation of the CFAA by accessing information he was authorized to obtain, but subsequently using the information for an improper or forbidden purpose.[115]

Among courts, there are generally two schools of thought: One is a broad interpretation that defines authorization by considering the intended use of the computer, a breach of the employee's duty of loyalty,[116] and computer use restrictions.[117] The other is a narrow interpretation that focuses on the employer's actions in restricting the employee's access (e.g., revoking access or limiting access by requiring codes or passwords).[118] Both of these interpretations are inappropriate as applied in the employment context.

Courts interpreting the CFAA broadly find violations of the statute when an employee misuses information obtained from the employer's computer, even if the employee was given access to the information obtained.[119] As such, an employee may access a computer "without authorization" or "exceed[ ] authorized access" in violation of the CFAA when he uses information obtained contrary to the employer's interest[120] or in violation of the employer's computer use policy.[121]

Although a broad interpretation of the CFAA more adequately protects valuable business assets from employee misappropriation,

---

> [A] person uses a computer "without authorization" under [the CFAA] when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

115. *Compare* WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206–07 (4th Cir. 2012) (adopting a narrow reading of the phrase "exceeds authorized access" and holding that it "appl[ies] only when an individual . . . obtains or alters information on a computer beyond that which he is authorized to access"), *and Nosal I*, 676 F.3d at 863 (holding that " 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions"), *with* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (holding that an employee exceeded authorized access "when he obtained personal information for a nonbusiness reason"), *and* United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (concluding "that access may be exceeded if the purposes for which access has been given are exceeded").

116. *Citrin*, 440 F.3d at 420–21; Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (concluding that employees lose their authorization to access their employer's computer when they send proprietary information to a competitor).

117. *See Rodriguez*, 628 F.3d at 1263–64; *John*, 597 F.3d at 271; EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001) (concluding that an employee may exceed authorized access by breaching a confidentiality agreement).

118. *See* United States v. Valle, 807 F.3d 508, 524–25 (2d Cir. 2015); *Miller*, 687 F.3d at 206; *Nosal I*, 676 F.3d at 860.

119. *See, e.g.*, *Rodriguez*, 628 F.3d at 1263–64; *John*, 597 F.3d at 271.

120. *Citrin*, 440 F.3d at 421; *Shurgard*, 119 F. Supp. 2d at 1125.

121. *See Rodriguez*, 628 F.3d at 1263–64; *John*, 597 F.3d at 272; *Explorica*, 274 F.3d at 582.

interpreting the CFAA to include violations of computer use restrictions is overly broad.[122] In *United States v. Nosal* (*Nosal I*), the U.S. Court of Appeals for the Ninth Circuit addressed the notice problem that would arise by allowing criminal liability under the CFAA to turn on "private policies that are lengthy, opaque, subject to change and seldom read."[123] The court noted that this interpretation would allow "private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law," transforming whole categories of innocuous behavior into federal crimes simply because a computer is involved.[124] As such, the Ninth Circuit declined to follow the approach of other circuits applying the CFAA to corporate computer use restrictions.[125]

As applied in the employment context, the broad view inappropriately brings the intent of the employee and use of the information into the analysis rather than focusing on the employee's authority to access the information.[126] This enables employers to circumvent causes of action specifically intended to address misappropriation by employees. Furthermore, a violation of the CFAA subjects an employee to both civil and criminal liability. Thus, a mere violation of an employment contract becomes a federal tort and a federal criminal offense.[127] This is especially problematic given that the only element requiring an intentional act by the employee is the act of

122. *See, e.g.*, *Nosal I*, 676 F.3d at 860; Kerr, *supra* note 87, at 1599 ("Because Internet users routinely ignore the legalese that they encounter in contracts governing the use of websites, Internet Service Providers (ISPs), and other computers, broad judicial interpretations of unauthorized access statutes could potentially make millions of Americans criminally liable for the way they send e-mails and surf the Web.").

123. *Nosal I*, 676 F.3d at 860.

124. *See id.* (discussing examples of innocuous conduct that may constitute a violation of the CFAA). Furthermore, the effects of such a broad interpretation are not limited to the employment context. As the Ninth Circuit noted, the effect of this broad construction on the workplace "pales by comparison with its effect on everyone else who uses a computer, smartphone, iPad, Kindle, Nook, X-box, Blu-Ray player or any other Internet-enabled device." *Id.* at 860–61. All of the devices that people routinely use online rely on remote access to computers, which "is governed by a series of private agreements and policies that" that few people are aware of or understand but that can serve as the basis for CFAA liability. *Id.* Further, "website owners retain the right to change the terms [of service] at any time and without notice." *Id.* at 862. Thus, this construction of the CFAA would allow rather innocuous behavior—completely outside of the employment context—to become criminal "without an act of Congress, and without any notice." *Id.* at 861–62.

125. *Id.* at 863.

126. *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013) ("These rulings wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use.").

127. *See* Enhanced Recovery Co., LLC v. Frady, No. 3:13-cv-1262-J-34JBT, 2015 WL 1470852, at *8 (M.D. Fla. Mar. 31, 2015); Advanced Micro Devices, Inc. v. Feldstein, 951 F. Supp. 2d 212, 218 (D. Mass. 2013).

accessing the computer.[128] Thus, a broad interpretation is inappropriate as applied in the employment relationship.

Courts following the narrow interpretation hold that an employee—usually an authorized computer user—does not act "without authorization" until the employer has rescinded that authorization.[129] And an employee only "exceeds authorized access" when he "obtains or alters information on a computer beyond" what that employee "is authorized to access," which essentially requires the employee to circumvent restrictions to gain entry into a system beyond his ordinary access.[130] Accordingly, courts with this view find that misappropriation or misuse of information is not a sufficient basis for CFAA liability.[131]

Under the narrow interpretation it is more difficult for employers to protect electronically stored business assets, including confidential and proprietary information. Arguably, this interpretation is inadequate in protecting employers because it allows employees who steal massive amounts of company data to escape CFAA liability simply because their employer entrusted them with access to valuable

128. *See supra* note 106 and accompanying text.

129. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009).

130. *See, e.g.*, WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012).

131. *See* United States v. Valle, 807 F.3d 508, 524–27 (2d Cir. 2015); *Miller*, 687 F.3d at 206; *Nosal I*, 676 F.3d 854, 858, 860 (9th Cir. 2012). The DOJ endorsed this interpretation in the criminal context in a memorandum to U.S. Attorneys outlining its intake and charging policy for computer crimes. *See* Memorandum from the Attorney Gen. to the U.S. Attorneys & Assistant Attorney Gens. for the Criminal & Nat'l Sec. Div. (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download [https://perma.cc/2M63-J3C7]. The DOJ articulated several factors for federal prosecutors to consider when deciding whether to pursue CFAA cases, including sensitivity of the information, national and economic interests, furtherance of larger criminal endeavors, impact on third parties, and deterrence value. *Id.* at 1–2.

information in the ordinary course of business.[132] However, employers have a number of other remedies upon which they can rely.[133]

Both interpretations are problematic not only for conduct in the workplace but also for conduct engaged in by ordinary citizens, like password sharing.[134] The CFAA, a statute not intended for use in the employment context, fails to balance the competing policy interests underlying state employment laws and trade secret law. Further, it remains an unpredictable legal remedy for employers because it is unclear how a court will interpret the CFAA in the employment

---

132. Even the narrow construction of the CFAA risks criminalizing a broad category of common actions outside of the employment context. In *United States v. Nosal* (*Nosal II*), the Ninth Circuit found that a former employee violated the CFAA by accessing the employer's computer system using the log-in credentials of a current employee. *See* 844 F.3d 1024, 1028 (9th Cir. 2016). The dissent raised the concern that the majority's interpretation captures "ubiquitous, useful, and generally harmless" conduct, and "threatens to criminalize all sorts of innocuous [password sharing] engaged in daily by ordinary citizens"—like sharing Netflix, Hulu, or HBO Go account information. *Id.* at 1049, 1053 (Reinhardt, J., dissenting). Under either a broad or narrow interpretation of the CFAA, password sharing in the streaming service context may violate the statute because streaming services such as Netflix specifically prohibit password sharing. *See Netflix Terms of Use*, NETFLIX § 7(a), https://help.netflix.com/legal/termsofuse?locale=en &docType=termsofuse (last updated Aug. 1, 2017) [https://perma.cc/6SMS-ZH39]:

> The member who created the Netflix account and whose Payment Method is charged is referred to here as the Account Owner. The Account Owner has access and control over the Netflix account. The Account Owner's control is exercised through use of the Account Owner's password and therefore to maintain exclusive control, the Account Owner should not reveal the password to anyone.;

see also B. Alan Orange, *Netflix, HBOGo & Facebook Password Sharing Is Now a Federal Crime*, MOVIEWEB (July 9, 2016), http://movieweb.com/netflix-hbo-facebook-password-sharing-fedral-crime/ [https://perma.cc/BU4G-HY6Q]; Bre Payton, *Court: Yes, Sharing Your Nexflix Password Is Illegal*, FEDERALIST (July 11, 2016), http://thefederalist.com/2016/07/11/court-yes-sharing-your-netflix-password-is-illegal/ [https://perma.cc/LSP2-U7QD]; *Ruling Could Make Sharing Passwords for Subscription Services a Federal Crime*, FOX NEWS (July 11, 2016), http://www.foxnews.com/politics/2016/07/11/ruling-could-make-sharing-passwords-for-subscription-services-federal-crime.html [https://perma.cc/6ZAP-DMKX]. Although it may seem absurd, streaming companies, producers, or artists may attempt to deter this conduct at the expense of the millions of Americans who engage in password sharing. With the pervasive presence of password sharing, harmed parties may want to ensure they are properly and fairly paid for their work, products, or services. Further, given the copyright litigation from illegal music downloading that exploded over a decade ago, and the more recent copyright litigation involving illegal movie downloads, artists and producers may similarly find that with the prevalence of password sharing today, they are not being paid fairly for the public's access to their work and may want to take action to deter this conduct. Although Netflix has not attempted to enforce its prohibition on password sharing, it is possible that others may take action. For example, if entertainment streaming companies pay artists or producers related to the number of account holders, such password sharing may have a more harmful effect than people think, which may even discourage producers or artists from allowing these companies to stream their works. For an instance of the illegal downloads litigation, see, for example, Julianne Pepitone, *50,000 BitTorrent Users Sued for Alleged Illegal Downloads*, CNNMONEY (June 10, 2011, 3:59 PM), http://money.cnn.com/2011/06/10/technology/bittorrent_lawsuits/ [https://perma.cc/GF2T-DF4Y].

133. *See supra* Sections II.A, II.B.

134. *See supra* notes 124, 132.

context.[135] A broad view enables employers to circumvent the requirements of other causes of action merely because the employer's information is stored on a computer, presenting considerable notice concerns for employees. Conversely, a narrow view does not adequately protect most of an employer's business information from employee misappropriation. In sum, the CFAA is an inappropriate legal remedy in the employment context.

III. FORTIFYING THE FRONT: RELIABLE EXPECTATIONS FOR EMPLOYERS AND EMPLOYEES REGARDING THE PROTECTION AND USE OF BUSINESS INFORMATION

Knowledge and information are valuable assets in the digital age.[136] Employers strive to protect much of their valuable business information, but given the conflicting policy interests at issue, it is often unclear whether a court will enforce contractual constraints on competition, if the employer can establish trade secret status, or how a court will interpret the CFAA in the employment context. As employers digitize more of their valuable assets and information, there must be a reliable legal framework governing the rights and obligations of employees and employers. The law, at times, becomes ill suited to the digital age, and must accommodate for advances in technology.[137]

This Part advocates for comprehensive statutory reform to adequately address misappropriation of business information in the digital age. The proposed reform aims to create reliable expectations on the front end, balance the competing interests at stake, and sufficiently protect employers in the digital age, while also eliminating concerns about the overbreadth of the CFAA. This Part first advocates that Congress amend the CFAA to eliminate the civil cause of action in the employment context and further define "exceeds authorized access" by clarifying that it refers to the unauthorized procurement of information rather than an improper use or misappropriation of information obtained with permission. This Part further proposes that Congress amend the DTSA to charge the FTC with implementation and

135. *See, e.g.*, Teva Pharm. USA, Inc. v. Sandhu, No. 17-3031, 2018 WL 617991, at *3 (E.D. Pa. Jan. 30, 2018) ("How to apply the definition of 'exceeds authorized access' under section 1030(a)(4) of the CFAA when it is an employee who properly accessed and improperly used the information has split the circuit courts.").

136. *See, e.g.*, Chris Montville, Note, *Reforming the Law of Proprietary Information*, 56 DUKE L.J. 1159, 1159 (2007) ("As the nation continues its shift toward an information economy, knowledge becomes an ever more significant asset for American employers.").

137. *Cf.* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (stating that it may be necessary to reconsider Fourth Amendment jurisprudence where the current approach has become "ill suited to the digital age").

administration of the DTSA, leaving the criminal offense of theft of trade secrets under the EEA as it was before enactment of the DTSA. Although each of these statutory amendments can stand on its own, the comprehensive reform proposed would best promote predictability in this area of law and protect both employers and employees.

A. Protecting Employees and Ordinary Computer Users Under the CFAA

While the CFAA remains a valuable tool to prosecute external computer hacking, application of the statute in the employment context has proven problematic at best.[138] Therefore, this Section proposes that Congress amend the CFAA in two respects. First, Congress should exclude claims against former or current employees from the provision authorizing private civil causes of action.[139] Second, Congress should adopt the narrow view of the CFAA by clarifying the CFAA's current definition of "exceeds authorized access" and limit it even further.

First, Congress should amend the CFAA to limit the availability of the private cause of action in the employment context. Specifically, Congress should amend section 1030(g), which authorizes private civil actions, to exclude from its authorization actions brought by employers against former or current employees. Thus, Congress should add to the end of section 1030(g) the limitation that "no action may be brought under this subsection by an employer against a current or former employee."

Employers already have numerous alternative causes of action against current and former employees who obtain information from their employers' computers. Eliminating the civil cause of action in the employment context will encourage employers to proceed under causes of action that account for the competing policy interests behind the protection of business information. This limitation will prevent employers from being able to circumvent the requirements of contract, tort, or trade secret law to sue employees merely because they obtained *any* information from *any* computer. If the information obtained by an employee does not qualify for protection as a trade secret, the employer's attempt to prohibit the former employee from using the information seems akin to an attempt to eliminate ordinary competition even though use of the information by the employee would not give the employee the type of unfair advantage that these laws aim to

138. *See supra* Section II.C.
139. *See* 18 U.S.C. § 1030(g) (2012).

prevent.[140] Moreover, eliminating this remedy will encourage employers to be more diligent in drafting employment contracts and policies, thus providing employees with more adequate notice of their obligations with respect to their employers' business information.

Further, Congress should adopt the narrow view of the CFAA by clarifying the CFAA's current definition of "exceeds authorized access."[141] Generally, computer owners define a user's authorized access and can regulate the user's privileges by code (e.g., requiring a password to gain access to certain information) or by contract (e.g., a Terms of Use agreement).[142] Under the broad view of the CFAA, which delineates liability based on contract-based restrictions, computer owners are able to define the scope of criminality—which may result in a strikingly broad criminal prohibition without substantial connections to the rationales behind criminal punishment.[143] Employees and other computer users may be unaware of the implications of violating computer use restrictions regarding information that they are authorized to access.

Congress should thus clarify the CFAA's current definition of "exceeds authorized access" to avoid a broad criminal prohibition of conduct based on violations of computer use restrictions alone. Currently, the statute defines this term as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[144] Congress should clarify this definition by adding "for any purpose" at the end of the definition and specifying that "the accesser does not exceed authorized access by using access to a protected computer for an improper purpose." Amending the CFAA in this way will promote consistent applications of the CFAA among courts and limit the potential of criminal liability for employees. Congress should further limit the scope of the CFAA by clarifying that "authorization" encompasses "the permission of *either* the system owner *or* a legitimate account holder."[145]

Of course, amending the CFAA in these respects does not adequately protect employers in a world of constantly evolving

---

140. *See* Tradesman Int'l, Inc. v. Black, 724 F.3d 1004, 1014 (7th Cir. 2013).

141. *See* 18 U.S.C. § 1030(e)(6).

142. *See* Kerr, *supra* note 3, at 1644 ("[A] computer user can engage in computer misuse by circumventing code-based restrictions, or by breaching contract-based restrictions.").

143. *See id.* at 1651 (arguing for a narrow interpretation of computer misuse statutes to require circumvention of code-based restrictions and stating that "[b]y granting the computer owner essentially unlimited authority to define authorization, the contract standard delegates the scope of criminality to every computer owner").

144. 18 U.S.C. § 1030(e)(6).

145. *Nosal II*, 844 F.3d 1024, 1051 (9th Cir. 2016) (Reinhardt, J., dissenting).

information technology where inside "hackers" are one of the biggest threats to employers' information.[146] However, when entrusting employees with some of their most valuable assets, employers need some assurance that employees will not abuse inside access to misappropriate proprietary information.[147] Without such an assurance, employers may be hesitant to allow any employee to access proprietary information, preventing employers from efficiently operating their businesses.[148] To create reliable expectations, both employers and employees must be aware of acceptable uses under the law and the potential liability for unacceptable uses.

B. Combating the Insider Threat Through the DTSA and the Regulatory State

The DTSA is an appropriate vehicle to address theft of business information by employees who may not have "exceed[ed] authorized access" to obtain such information under the CFAA, but are nonetheless culpable because they lacked authorization to take such information. Unlike the CFAA, the DTSA focuses on what the employee is allowed to do with information obtained rather than how the employee initially obtained it. The DTSA does not focus on the *unauthorized access* of protected information but rather on the *use or disclosure* of information without consent and the acquisition of information through *improper means*—which includes "theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means."[149] Thus, employers should be able to rely on the DTSA for legal recourse. However, even if employers rely

146. *See* Kapitanyan, *supra* note 22, at 408–09 ("The malicious insider is one of the most significant threats companies face because the malicious insider has relatively easy access to a company's most valuable assets and knows exactly where to find them. . . . [T]he great[est] threat lurks within businesses themselves.").

147. *See, e.g.*, Winston Research Corp. v. Minn. Mining & Mfg. Co., 350 F.2d 134, 138 (9th Cir. 1965) (articulating that employers will be hesitant to communicate with employees if unauthorized disclosure of business information is not restricted).

148. *Id.* ("Unless protection is given against unauthorized disclosure of confidential business information by employees, employee-employer relationships will be demoralized; employers will be compelled to limit communication among employees with a consequent loss in efficiency; and business, espionage, deceit, and fraud among employers will be encouraged.").

149. 18 U.S.C. §§ 1839(5)(A)–(B), 1839(6)(A) (Supp. 2016). This is a more appropriate means to address misappropriation of proprietary information and violations of computer use policies, as a breach of an express contract in obtaining a trade secret is conduct that will be deemed improper for purposes of finding trade secret misappropriation, and in the absence of a contract, courts will often find an implied duty of confidentiality or implied-in-fact contract. *See* James W. Hill, *Trade Secrets, Unjust Enrichment, and the Classification of Obligations*, VA. J.L. & TECH., Spring 1999, at 1, ¶¶ 30–32, http://vjolt.org/wp-content/uploads/2017/Articles/vol4/issue/home_art2.html [https://perma.cc/HT3K-KGMT].

on the DTSA instead of the CFAA when their information is misappropriated, there remains a lack of clarity and many caveats with this approach.[150] This Section thus proposes changing the DTSA to provide power to the FTC to administer the civil regime of trade secret protection. Specifically, it proposes enabling the FTC to prescribe rules and general statements of policy, issue administrative orders, and commence civil actions.[151]

Although the DTSA aimed to promote reliability and uniformity in trade secret law, identifying what information qualifies for trade secret protection remains uncertain. As federal courts rely on established *state* trade secret laws to interpret and apply the DTSA, federal trade secret law varies among federal courts sitting in different states.[152] This lack of uniformity is problematic given that employers increasingly operate across state lines. Thus, for employers to adequately protect their information, they must stay attuned to the trade secret laws in each state in which they operate. This would likely be extremely costly and time consuming for employers. Furthermore, employees who misuse their employer's information risk facing significant liability even although neither the employer nor the employee is certain whether the information qualifies for trade secret protection until after litigation ensues.

Currently the DTSA provides for private civil actions and enables the Attorney General to obtain injunctive relief in civil actions, with the EEA providing for criminal penalties—which is similar to the framework set forth in state trade secret statutes.[153] This multiparadigm legal framework, long enforced in state courts, generally offered adequate protection for employers prior to the complexity brought about by the digitization of business information.[154] However, as discussed above, this area of law is becoming too complex to fit comfortably within the current legal framework. Given that neither the DOJ nor federal courts possess a specialized expertise in trade secret law, they rely on established state trade secret law, which does not adequately address new types of digital business assets.[155] Therefore,

150. For instance—as described above—with employers increasingly storing proprietary information on computer databases, there are many forms of valuable business assets that may not constitute a trade secret because the asset does not derive independent economic value from its secrecy or the employer does not take sufficient efforts to maintain the asset's secrecy because the asset is contained on a computer database that multiple employees are enabled to access.

151. *Cf.* 15 U.S.C. § 56 (2012) (outlining litigation procedure for the FTC); *id.* § 57a(a)(1) (authorizing the FTC to prescribe rules and general statements of policy).

152. *See supra* note 84 and accompanying text.

153. *See* 18 U.S.C. § 1836(a)–(b).

154. *See supra* Section II.B.

155. *See supra* Section II.B.

this Section proposes that the DTSA be administered by a federal agency to best promote uniformity and reliability in trade secret law.

Federal administrative law aims to empower experts in a given field to give meaning and content to vague policies set forth by Congress.[156] Accordingly, federal agencies fill in the details of broad statutes by using their expertise to create prospective, consistent policies. In this context an agency is better suited than courts to take into account the competing interests at stake in protecting business information. Allowing an agency to administer the DTSA would promote reliability and consistency in the complex area of trade secret misappropriation.

Specifically, Congress should grant the FTC the authority to administer the DTSA because the competing policies at stake under the DTSA are core to the mission of the FTC, which is to "protect consumers by preventing anticompetitive, deceptive, and unfair business practices . . . without unduly burdening legitimate business activity."[157] The FTC is "dedicated to advancing consumer interests while encouraging innovation and competition in our dynamic economy."[158] Accordingly, the FTC is well suited to promote policies under the DTSA that adequately balance the interests inherent in protecting business information while effectively promoting competition.

Arguably, the FTC already possesses authority to regulate trade secret misappropriation under the Federal Trade Commission Act ("FTC Act").[159] Although primarily focused on consumer welfare, the FTC Act makes unlawful "unfair methods of competition in or affecting commerce,"[160] and empowers the FTC to "prevent persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce . . . ."[161] Under established common law, trade secret law and misappropriation fall under the umbrella of unfair competition law and arguably could be regulated under the FTC Act.[162] However, because the DTSA already provides a

156. *See generally* Felix Frankfurter, *The Task of Administrative Law*, 75 U. PA. L. REV. 614, 614 (1927).

157. *About the FTC*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc (last visited Jan. 26, 2018) [https://perma.cc/C88F-JQUK].

158. *What We Do*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do (last visited Jan. 26, 2018) [https://perma.cc/5V8K-GP9V].

159. *See infra* note 162 and accompanying text.

160. 15 U.S.C. § 45(a)(1) (2012).

161. *Id.* § 45(a)(2).

162. *See, e.g.*, Myriad Dev., Inc. v. Alltech, Inc., 817 F. Supp. 2d 946, 981 (W.D. Tex. 2011):

> The law of unfair competition is the umbrella for all statutory and nonstatutory causes of action arising out of business conduct which is contrary to honest practice in industrial or commercial matters. Within the broad scope of unfair competition are the

statutory scheme with respect to trade secret misappropriation, the DTSA remains a more practical and specific framework through which to regulate trade secret misappropriation. Thus, amending the DTSA to grant the FTC authority to administer the statute and regulate trade secret misappropriation offers a better solution to protect both employers and employees.

To effectuate this change, Congress could amend the DTSA by adding provisions that provide the FTC with the power to enforce the DTSA, with the same jurisdiction, powers, and duties as the FTC Act as if its provisions were incorporated into the DTSA.[163] This would enable the FTC to makes rules and regulations pursuant to the DTSA, as well as issue orders and file suits in the district courts of the United States.[164]

To adequately protect business information with consistency and reliability, the DTSA should encompass more specific and definite language. The FTC can promote uniformity by taking the broad language of the DTSA and providing guidance to employers and employees on its meaning and enforcement. The DTSA defines a trade secret in broad terms,[165] which are susceptible to many interpretations and meanings, resulting in an unclear and unreliable legal framework.

> independent causes of action such as trade-secret law . . . and misappropriation, to name only a few.

(alteration in original) (quoting U.S. Sporting Prods., Inc. v. Johnny Stewart Game Calls, Inc., 865 S.W.2d 214, 217 (Tex. App. 1993)); *see also* FTC v. R.F. Keppel & Bro., Inc., 291 U.S. 304, 310–12 (1934):

> As proposed by the Senate Committee on Interstate Commerce and as introduced in the Senate, the bill which ultimately became the Federal Trade Commission Act declared "unfair competition" to be unlawful. But it was because the meaning which the common law had given to those words was deemed too narrow that the broader and more flexible phrase "unfair methods of competition" was substituted. Congress, in defining the powers of the Commission, thus advisedly adopted a phrase which, as this Court has said, does not "admit of precise definition, but the meaning and application of which must be arrived at by what this court elsewhere has called 'the gradual process of judicial inclusion and exclusion.' "

(quoting FTC v. Raladam Co., 283 U.S. 643, 648 (1931)).

163. *See, e.g.*, 15 U.S.C. § 70e.

164. *Id.*

165. 18 U.S.C. § 1839(3) (Supp. 2016):

> [A]ll forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if—(A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information . . . .

Clarifying this complex definition with specificity fits comfortably within the competence of the FTC.[166]

In administering the DTSA, the FTC should issue rules or guidance as necessary to identify specific types of business information that are protected under the statute—which may vary among industries. For instance, the FTC can determine whether customer lists in a certain industry qualify as a trade secret under the DTSA by considering the nature of the industry, an employee's relationship with the customers in that industry, and the secrecy and value of a customer list in the industry.[167] Although this is a complex task and the FTC may not currently possess the resources or the capability to identify all cognizable protectable information, this approach is better than leaving to the courts the entire task of deciding whether information qualifies for protection *after* the information is already misappropriated. Once proprietary business information is disclosed or misappropriated it

166. *See, e.g.*, *R.F. Keppel & Bro., Inc.*, 291 U.S. at 314 ("[The FTC] was created with the avowed purpose of lodging the administrative functions committed to it in 'a body specially competent to deal with them by reason of information, experience and careful study of the business and economic conditions of the industry affected' . . . ." (quoting S. REP. NO. 63-597, at 9, 11 (1914))).

167. Although some courts have developed a body of case law determining when a customer list can be protected as a trade secret, the law still varies among states (and thus among federal courts applying the DTSA), and whether the customer list is protected is determined after it is misappropriated. The FTC could use variations of the established case law to create proposed rules or guidance regarding whether a customer list is protected. For an example of a court's interpretation of trade secret law concerning whether customer lists are protected, see *Pyro Spectaculars North, Inc. v. Souza*, 861 F. Supp. 2d 1079, 1088 (E.D. Cal. 2012), which looked to an extensive summary of California law:

> With respect to the general availability of customer information, courts are reluctant to protect customer lists to the extent they embody information which is readily ascertainable through public sources, such as business directories . . . On the other hand, where the employer has expended time and effort identifying customers with particular needs or characteristics, courts will prohibit former employees from using this information to capture a share of the market. Such lists are to be distinguished from mere identities and locations of customers where anyone could easily identify the entities as potential customers . . . As a general principle, the more difficult information is to obtain, and the more time and resources expended by an employer in gathering it, the more likely a court will find such information constitutes a trade secret . . . The requirement that a customer list must have economic value to qualify as a trade secret has been interpreted to mean that the secrecy of this information provides a business with a substantial business advantage . . . In this respect, a customer list can be found to have economic value because its disclosure would allow a competitor to direct its sales efforts to those customers who have already shown a willingness to use a unique type of service or product as opposed to a list of people who only might be interested . . . Its use enables the former employee to solicit both more selectively and more effectively.

(alterations in original) (quoting Morlife, Inc. v. Perry, 66 Cal. Rptr. 2d 731, 735–36 (Ct. App. 1997)). This summary also illustrates the complexity involved in discerning whether business information can even qualify for trade secret protection. It is extremely unrealistic to expect employers, employees, or courts to have any reasonable expectations when relying on the extremely fact-intensive case law analyzing trade secret claims.

loses its value. Thus, a forward-looking approach to identifying protected information best ensures the continuing value of an employer's proprietary information.

The FTC should further identify what constitutes "reasonable measures to keep such information secret" so that employers can take appropriate measures to protect their information from misappropriation.[168] Specifying whether certain computer access restrictions are "reasonable" would allow an employer to take the appropriate measures before the trade secret is misappropriated. The FTC should also specify what it means for information to "derive independent economic value."[169]

Enabling the FTC to fill in these details would create expectations upon which both employers and employees can rely. By making the information available to employers and employees ex ante, employees would be on notice of the acceptable uses of certain information belonging to their employer, and thus able to avoid liability. Likewise, employers would have guidance on how best to protect their information to ensure they can seek legal recourse if their information is subsequently misappropriated. To ensure the information is adequately communicated to employees, the FTC could, for example, require that employers provide employees with notice encompassing information about the employer's assets that are protected by the DTSA and the consequences of violating the DTSA as a condition of the employer seeking protection for its information under the DTSA.[170]

Congress should further provide the FTC with the authority to issue administrative orders and litigate civil actions. When an alleged violation of the DTSA occurs, the owner of the trade secret can file a complaint with the FTC, and the FTC can issue upon the alleged perpetrator an order enjoining the use or disclosure of the trade secret.[171] If the alleged perpetrator violates the order or the use of the trade secret has already caused damage to the owner of the trade secret,

168. *See* 18 U.S.C. § 1839(3)(A).

169. *See id.* § 1839(3)(B).

170. *Cf.* 18 U.S.C. § 1833(b)(3) (requiring employers to provide notice of immunity from liability for certain exceptions to the prohibition against misappropriation to employees in an agreement or contract governing use of trade secrets and confidential information in order for the employer to be awarded exemplary damages or attorney fees in an action against an employee to whom notice was not provided). The FTC could require similar notice for general liability under the DTSA in order to *pursue* an action against employees under the DTSA.

171. *Cf.* 15 U.S.C. § 45(b) (2012) (authorizing the FTC to issue complaints for violations of the FTC Act).

the FTC can commence a civil action in the appropriate district court, and allow the owner of the trade secret to intervene in the action.[172]

Charging the FTC with creating and specifying the details of the DTSA will encourage more consistency and clarity than the current regime provides. Not only would this provide employers with the benefit of specificity ex ante about what information is protected, it also has the added benefit of a centralized system through which these actions must proceed. When employers are considering whether to sue employees in these circumstances, employers must calculate the risks and benefits of pursuing litigation. The uncertainty about whether the information taken by the employee is protected may well deter the employer from bringing a claim against the employee at all. With a centralized system, the employer likely has an additional indication about whether the information qualifies for protection and can make a comparatively informed decision before pursuing the litigation.[173] Further, business information for which employers seek protection will likely continue to change in the future, and agencies have more flexibility to amend rules and guidance than courts or Congress.[174]

Under this regulatory regime, the DOJ would remain charged with prosecuting criminal offenses under the EEA. The provision proscribing theft of trade secrets encompasses a higher mens rea standard than the section addressing civil actions for misappropriation. Specifically, the EEA requires showings of intent to convert a trade secret, intent or knowledge that the offense will injure an owner of that trade secret, and knowledge of the act that constitutes the theft of the trade secret as compared to the DTSA, which merely requires a showing that the alleged perpetrator had reason to know that the trade secret was acquired through improper means.[175] In prosecuting violations

172. *Cf. id.* § 56(a) (outlining the procedures for the FTC to exercise its authority to litigate under the FTC Act).

173. *Cf.* Tradesman Int'l, Inc. v. Black, 724 F.3d 1004, 1017 (7th Cir. 2013) (Hamilton, J., concurring) (discussing how variation in states' treatment of noncompetes is a powerful factor in calculating the risks and benefits of litigation).

174. *See* 5 U.S.C. § 553 (2012) (outlining procedures for agencies, which includes the process of amending rules or guidance).

175. *Compare* 18 U.S.C. § 1832(a):

> Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly—(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; . . . shall . . . be fined . . . or imprisoned . . . .,

under the EEA, the DOJ likely considers the intent of the actor and the wantonness of the violation as it does in CFAA violations. However, unlike the CFAA where there is no additional requirement of a showing of intent for criminal liability above what is required for civil liability, Congress has already accounted for notice concerns by protecting individuals and organizations from excessive criminal penalties involving inadvertent violations.[176] Because of the differences in the civil and criminal regimes, the DOJ should remain charged with pursuing criminal violations under the EEA.

Providing an agency with the power to administer a federal statute presents a potential risk of agency capture. Since employers generally are more powerful and have a greater ability to influence federal agencies than individual employees given their size and resources, employers could have an influence over decisionmaking, presenting a risk that the DTSA could become too protective of employers in protecting their business information—at the expense of employees and the public at large.[177] However, this proposed regime protects against agency capture in several ways. First, the FTC is an independent agency, which generally creates an extra buffer against interest group pressures that might harm the public interest or a vulnerable group.[178] Second, the courts still retain jurisdiction over actions brought by the FTC under the DTSA, thus providing for an independent decisionmaker.

The burden of federal regulations on employers should not be underestimated. The complexities involved in the increasingly prevalent administrative state can be a nightmare for employers to navigate. However, regulating the protection of business information through a federal agency does not entail the same concerns. Employers would not be required to comply with the DTSA unless they intend to rely on the statute to hold employees accountable for misappropriation of business information. Rather, charging the FTC with administration of the DTSA would merely provide employers with guidance to best

---

with id. § 1836(b)(1) (authorizing the owner of a trade secret that is misappropriated to bring a civil action), *and id.* § 1839(5) ("[T]he term 'misappropriation' means—(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means . . . .").

176.The penalties for a violation of theft of a trade secret are severe. *See id.* § 1832(a) (authorizing for punishment of an individual who commits the offense of theft of trade secrets fines or imprisonment of "not more than 10 years, or both"); *id.* § 1832(b) (authorizing for punishment of an organization that commits the offense of theft of trade secrets fines of "not more than the greater of $5,000,000 or 3 times the value of the stolen trade secret").

177. *See* Rachel E. Barkow, *Insulating Agencies: Avoiding Capture Through Institutional Design*, 89 TEX. L. REV. 15, 21–24 (2010) (discussing independent agencies and the need to insulate agencies from capture).

178. *Id.* at 24.

protect their information if they intend to seek legal recourse under the DTSA. Employers expend significant resources developing their business information, and accordingly, they should encourage more specificity and reliability under the DTSA to ensure their business information is protected. Moreover, this reform would enable employees to better understand their rights and obligations with respect to their employers' business information. It would provide guidance and notice to employees who might otherwise be unaware of the implications of misusing such information.

CONCLUSION

The ease with which employees can copy, download, and transfer proprietary information from employers' computer databases presents a considerable threat to employers. In the ordinary course of business, employers must authorize certain employees to access proprietary information and rely on employees to use such information for proper business purposes. Employers should be able to provide employees with access to this information without fear that an employee will misappropriate the information without legal recourse.

The current scheme of protection for employers' proprietary information is unworkable. Despite the recently enacted federal trade secret legislation, the application of trade secret law remains a mystery to employers, employees, and courts. Congress should amend the CFAA to limit the civil cause of action in the employment context and clarify that a computer user does not "exceed[ ] authorized access" by using his permission to access a computer for improper purposes. Moreover, Congress should also amend the DTSA to grant the FTC authority to administer the DTSA to promote reliability and consistency.

*Danielle J. Reid**

* J.D. Candidate, 2018, Vanderbilt Law School; B.B.A., B.A., 2015, Southern Methodist University. I would like to thank Professor Jennifer Bennett Shinall for providing insightful feedback to refine my topic and arguments, and Professor Kevin Stack for providing helpful insights for crafting my solution. I would also like to thank the editors and staff of the *Vanderbilt Law Review* for their tireless work and dedication. Finally, I am extremely grateful to my family for their constant love, support, and encouragement.

***

VANDERBILT LAW REVIEW

2017-2018 EDITORIAL BOARD

VANDERBILT LAW SCHOOL

OFFICERS OF THE UNIVERSITY

Nicholas S. Zeppos, *Chancellor of the University; Professor of Law*
Susan Wente, *Provost and Vice Chancellor for Academic Affairs*
Audrey Anderson, *Vice Chancellor, General Counsel and Secretary of the University*
Jeffrey Balser, *Vice Chancellor for Health Affairs and Dean of the School of Medicine*
Steve Ertel, *Vice Chancellor for Communications*
Nathan Green, *Interim Vice Chancellor for Public Affairs*
Anders Hall, *Vice Chancellor for Investments and Chief Investment Officer*
Eric Kopstain, *Vice Chancellor for Administration*
John M. Lutz, *Vice Chancellor for Information Technology*
Tina L. Smith, *Interim Vice Chancellor for Equity, Diversity and Inclusion and Chief Diversity Officer*
Susie Stalcup, *Vice Chancellor for Development and Alumni Relations*
Brett Sweet, *Vice Chancellor for Finance and Chief Financial Officer*
David Williams II, *Vice Chancellor for University Affairs and Athletics; Athletics Director; Professor of Law*

LAW SCHOOL ADMINISTRATORS

Chris Guthrie, *Dean of the Law School; John Wade-Kent Syverud Professor of Law*
Lisa Bressman, *Associate Dean for Academic Affairs; David Daniels Allen Distinguished Chair in Law; Professor of Law*
Susan Kay, *Associate Dean for Clinical Affairs; Clinical Professor of Law*
Spring Miller, *Assistant Dean for Public Interest; Lecturer in Law*
Larry Reeves, *Associate Professor of Law; Associate Dean & Director, Law Library*
Christopher Serkin, *Associate Dean for Academic Affairs; Professor of Law*

FACULTY

Brooke Ackerly, *Associate Professor of Political Science; Associate Professor of Philosophy; Associate Professor of Law; Affiliated Faculty, Women's and Gender Studies; Principal Investigator, Global Feminisms Collaborative*
Philip Ackerman-Lieberman, *Associate Professor of Jewish Studies and Law; Associate Professor of Religious Studies; Affiliated Associate Professor of Islamic Studies and History; Professor of Law*
Rebecca Allensworth, *Professor of Law*
Robert Barsky, Professor of French, English and Jewish Studies; Professor of Law
Margaret M. Blair, *Milton R. Underwood Chair in Free Enterprise; Professor of Law*
Lauren Benton, *Dean, Vanderbilt University College of Arts and Science; Nelson O Tyron, Jr Chair in History; Professor Law*
Frank Bloch, *Professor of Law Emeritus*
James F. Blumstein, *University Professor of Constitutional Law and Health Law & Policy; Professor of Management; Owen Graduate School of Management; Director, Vanderbilt Health Policy Center*

C. Dent Bostick, *Professor of Law Emeritus*; *Dean Emeritus*
Michael Bressman, *Professor of the Practice of Law*
Jon Bruce, *Professor of Law Emeritus*
Christopher (Kitt) Carpenter, *Professor of Economics*; *Professor of Law; Professor of Health Policy*; *Professor of Leadership, Policy and Organization*
Edward K. Cheng, *Professor of Law*; *FedEx Research Professor for 2017-18*
William Christie, *Frances Hampton Currey Professor of Management in Finance*; *Professor of Law*
Ellen Wright Clayton, *Craig-Weaver Chair in Pediatrics*; *Professor of Law; Professor of Health Policy*
Mark Cohen, *Justin Potter Professor of American Competitive Enterprise*; *Professor of Law; University Fellow, Resources for the Future*
Robert Covington, *Professor of Law Emeritus*
Andrew Daughety, *Gertrude Conaway Vanderbilt Professor of Economics*; *Professor of Law*
Colin Dayan, *Robert Penn Warren Professor in the Humanities*; *Professor of Law*
Paul H. Edelman, *Professor of Mathematics*; *Professor of Law*
Joseph Fishman, *Assistant Professor of Law*
James Ely, Jr., *Milton R. Underwood Professor of Law Emeritus*; *Professor of History Emeritus; Lecturer in Law*
Brian T. Fitzpatrick, *Professor of Law*
Tracey E. George, *Charles B. Cox III and Lucy D. Cox Family Chair in Law & Liberty*; *Professor of Political Science; Director, Cecil D. Branstetter Litigation & Dispute Resolution Program; Professor of Law*
Daniel J. Gervais, *Milton R. Underwood Chair in Law; Professor of French*; *Director, Vanderbilt Intellectual Property Program Director, LL.M. Program; Professor of Law*
Leor Halevi, *Associate Professor of History*; *Associate Professor of Law*
Joni Hersch, *Cornelius Vanderbilt Chair; Professor of Law and Economics*; *Co-Director, Ph.D. Program in Law and Economics*
Alex J. Hurder, *Clinical Professor of Law*
Sarah Igo, *Associate Professor of History*; *Associate Professor of Law*
Owen D. Jones, *New York Alumni Chancellor's Chair in Law*; *Professor of Biological Sciences; Director, MacArthur Foundation Research Network on Law and Neuroscience; Professor of Law*
Allaire Karzon, *Professor of Law Emerita*
Nancy J. King, *Lee S. and Charles A. Speir Professor of Law*
Russell Korobkin, *Visiting Professor of Law*; *Richard G. Maxwell Professor of Law, UCLA Law School*
Craig Lewis, *Madison S. Wigginton Professor of Finance; Professor of Law*
David Lewis, *Chair of the Department of Political Science; William R. Kenan, Jr. Professor of Political Science*; *Professor of Law*
Harold Maier 1937-2014, *David Daniels Professor of Law Emeritus*
Terry A. Maroney, *Professor of Law; Professor of Medicine, Health, and Society*; *Chancellor Faculty Fellow; 2016-17 Andrew W. Mellon Foundation Fellowship at the Center for Advanced Study in the Behavioral Sciences, Stanford University; Co-Director, George Barrett Social Justice Program*
John Marshall, *Associate Professor of Law Emeritus*
Larry May, *W. Alton Chair of Philosophy*; *Professor of Law*
Sara Mayeux, *Assistant Professor of Law*
Holly McCammon, *Professor of Sociology; Professor of Human and Organization Development*; *Professor of Law*
Karla McKanders, *Clinical Professor of Law*
Thomas McCoy, *Professor of Law Emeritus*

Thomas McGinn, *Professor of History; Professor of Law*
Timothy Meyer, *Professor of Law*
Robert Mikos, *Professor of Law*
Beverly I. Moran, *Professor of Law; Professor of Sociology*
Michael A. Newton, *Professor of the Practice of Law; Director, Vanderbilt-in-Venice Program*
Robert S. Reder, *Professor of the Practice of Law; Partner, Milbank Tweed Hadley & McCloy (Retired)*
Jennifer Reinganum, *E. Bronson Ingram Professor of Economics; Professor of Law*
Philip Morgan Ricks, *Professor of Law*
Amanda M. Rose, *Professor of Law*
Barbara Rose, *Instructor in Law*
James Rossi, *Associate Dean for Research; Professor of Law; Director, Program in Law and Government*
Edward L. Rubin, *University Professor of Law and Political Science*
John B. Ruhl, *David Daniels Allen Distinguished Chair in Law; Professor of Law; Director, Program in Law and Innovation; Co-Director, Energy, Environment, and Land Use Program*
Herwig Schlunk, *Professor of Law*
Jeffrey A. Schoenblum, *Centennial Professor of Law*
Sean B. Seymore, *Professor of Law; Professor of Chemistry*
Daniel J. Sharfstein, *Tarkington Chair of Teaching Excellence; Professor of Law; Professor of History; Chancellor Faculty Fellow; Co-Director, George Barrett Social Justice Program*
Matthew Shaw, *Assistant Professor of Education; Assistant Professor of Law*
Suzanna Sherry, *Herman O. Loewenstein Chair in Law*
Jennifer Shinall, *Assistant Professor of Law*
Ganesh N. Sitaraman, *Professor of Law*
Paige Marta Skiba, *Professor of Law*
Christopher Slobogin, *Milton R. Underwood Chair in Law; Professor of Law; Director, Criminal Justice Program; Affiliate Professor of Psychiatry*
Kevin Stack, *Lee S. and Charles A. Speir Chair in Law; Professor of Law; Director of Graduate Studies, Ph.D. Program in Law and Economics*
Carol Swain, *Professor of Political Science; Professor of Law*
Jennifer Swezey, *Assistant Professor of Law; Director, Legal Writing Program*
Randall Thomas, *John S. Beasley II Chair in Law and Business; Director, Law & Business Program; Professor of Management, Owen Graduate School of Management*
R. Lawrence Van Horn, *Associate Professor of Management (Economics); Associate Professor of Law; Executive Director of Health Affairs*
Michael P. Vandenbergh, *David Daniels Allen Distinguished Chair in Law; Director, Climate Change Research Network; Co-Director, Energy, Environment, and Land Use Program Professor of Law*
W. Kip Viscusi, *University Distinguished Professor of Law, Economics, and Management; Co-Director, Ph.D. Program in Law and Economics*
Alan Wiseman, *Professor of Political Science; Professor of Law*
Ingrid Wuerth, *Helen Strong Curry Chair in International Law; Professor of Law; Director, International Legal Studies Program*
Yesha Yadav, *Professor of Law; Enterprise Scholar for 2017-19; Faculty, Co-Director, LL.M. Program*

Lawrence Ahern III, *Adjunct Professor of Law; Partner, Brown & Ahern*
Arshad Ahmed, *Adjunct Professor of Law; Co-Founder, Elixir Capital Management*
Richard Aldrich Jr., *Adjunct Professor of Law; Partner, Skadden Arps Slate Meagher & Flom (Retired)*
Andrea Alexander, *Research Services Librarian; Lecturer in Law*
Samar Ali, *Adjunct Professor of Law; Attorney, Bass Berry & Sims*
Roger Alsup, *Instructor in Law*
Paul Ambrosius, *Adjunct Professor of Law; Member, Trauger & Tuke*
Rachel Andersen-Watts, *Instructor in Law*
Raquel Bellamy, *Adjunct Professor of Law; Attorney, Bone McAllister Norton*
Gordon Bonnyman, *Adjunct Professor of Law; Staff Attorney, Tennessee Justice Center*
Kathryn (Kat) Booth, *Instructor in Law*
Linda Breggin, *Adjunct Professor of Law; Senior Attorney, Environmental Law Institute*
Larry Bridgesmith, *Adjunct Professor of Law; Coordinator Program on Law & Innovation; Inaugural Executive Director, Institute for Conflict Management, Lipscomb University*
Judge Sheila Jones Calloway, *Adjunct Professor of Law; Juvenile Court Magistrate, Metropolitan Nashville*
Jenny Cheng, *Lecturer in Law*
William Cohen, *Adjunct Professor of Law*
Christopher Coleman, *Adjunct Professor of Law*
Roger Conner, *Adjunct Professor of Law; Special Consultant on Public Service Career Development*
Matthew Curley, *Adjunct Professor of Law; Member, Bass Berry & Sims*
S. Carran Daughtrey, *Adjunct Professor of Law; Assistant U.S. Attorney, Middle District of Tennessee*
Hans De Wulf, *Visiting Professor of Law; Professor, Financial Law Institute, University of Ghent, Belgium*
Diane Di Ianni, *Adjunct Professor of Law*
Patricia Eastwood, *Adjunct Professor of Law; Senior Corporate Counsel, Caterpillar Financial Services Corporation*
Jason Epstein, *Adjunct Professor of Law; Partner, Nelson Mullins*
William Farmer, *Adjunct Professor of Law; Member, Jones Hawkins & Farmer*
Carolyn Floyd, *Research Services Librarian; Lecturer in Law*
Glenn Funk, *Adjunct Professor of Law; District Attorney General, 20th Judicial District of Tennessee*
Jason Gichner, *Adjunct Professor of Law; Attorney, Morgan & Morgan*
Vice Chancellor Sam Glassock, *Adjunct Professor of Law; Vice Chancellor, Delaware Court of Chancery*
Aubrey (Trey) Harwell, *Adjunct Professor of Law*
Kirsten Hildebrand, *Instructor in Law*
Darwin Hindman III, *Adjunct Professor of Law; Shareholder, Baker Donelson*
The Honorable Randy Holland, *Adjunct Professor of Law; Justice, Delaware Supreme Court*
David L. Hudson, *Adjunct Professor of Law*
Abrar Hussain, *Adjunct Professor of Law; Co-founder and Managing Director, Elixir Capital Management*
Lynne Ingram, *Adjunct Professor of Law; Assistant U.S. Attorney, Middle District of Tennessee*
Marc Jenkins, *Adjunct Professor of Law; Director and Corporate Counsel, Asurion*
Martesha Johnson, *Adjunct Professor of Law; Assistant Public Defender, Metropolitan Nashville Public Defender's Office, 20th Judicial District*

Michele Johnson, *Adjunct Professor of Law*; *Executive Director, Tennessee Justice Center*
Lydia Jones, *Adjunct Professor of Law*
The Honorable Kent Jordan, *Adjunct Professor of Law*; *Circuit Judge, U.S. Court of Appeals for the Third Circuit*
Andrew Kaufman, *Adjunct Professor of Law*
Suzanne Kessler, *Adjunct Professor of Law*; *Of Counsel, Bone McAllester Norton*
Russell Korobkin, *Visiting Professor of Law; Richard C. Maxwell Professor of Law, UCLA Law School*
Kelly Leventis, *Instructor in Law*
Jerry Martin, *Adjunct Professor of Law*; *Partner, Barrett Johnston Martin & Garrison*
Will Martin, *Adjunct Professor of Law*; *General Counsel, FirstBank*; *Retired Board Chair, Stewardship Council*
Cheryl Mason, *Adjunct Professor of Law*; *Vice President, Litigation HCA*
Richard McGee, *Adjunct Professor of Law*
James McNamara, *Adjunct Professor of Law*; *Assistant Public Defender, Metropolitan Nashville Public Defender's Office*
Robert McNela, *Adjunct Professor of Law; Shareholder, Liskow & Lewis*
Bryan Metcalf, *Adjunct Professor of Law*; *Member, Bass Berry & Sims*
Caitlin Moon, *Adjunct Professor of Law; Founder and Legal Counsel, Ledger Law; Co-founder and Chief Operating Officer, Legal Alignment*
Kelly Murray, *Instructor in Law*
Francisco Müssnich, *Adjunct Professor of Law*; *Senior Partner, Barbosa Müssnich & Aragao Advogados*
Sara Beth Myers, *Adjunct Professor of Law*; *Assistant Attorney General, State of Tennessee*
William Norton III, *Adjunct Professor of Law*; *Partner, Bradley Arant Boult Cummings*
R. Gregory Parker, *Adjunct Professor of Law*; *Member, Bass Berry & Sims*
C. Mark Pickrell, *Adjunct Professor of Law*; *Owner, Pickrell Law Group*
Michael Polovich, *Adjunct Professor of Law; Assistant Attorney General*
Mary Prince, *Associate Director for Library Services*; *Lecturer in Law*
Rahul Ranadive, *Adjunct Professor of Law; Of Counsel, Carlton Fields*
Eli Richardson, *Adjunct Professor of Law*; *Member, Bass Berry & Sims*
Steven Riley, *Adjunct Professor of Law*; *Partner, Riley Warnock & Jacobson*
Brian Roark, *Adjunct Professor of Law*; *Partner, Bass Berry & Sims*
Barbara Rose, *Instructor in Law*
John Ryder, *Adjunct Professor of Law*; *Member, Harris Shelton Hanover Walsh*
Deborah Schander, *Associate Director for Public Services*; *Lecturer in Law*
Mark Schein, *Adjunct Professor of Law*; *Chief Compliance Officer, York Capital Management*
Paul Schnell, *Adjunct Professor of Law*; *Partner, Skadden Arps Slate Meagher & Flom*
Teresa Sebastian, *Adjunct Professor of Law*
Arjun Sethi, *Adjunct Professor of Law*
Dumaka Shabazz, *Adjunct Professor of Law*; *Assistant Federal Public Defender, Middle District of Tennessee*
Justin Shuler, *Adjunct Professor of Law*; *Associate, Paul Weiss*
Joseph Slights, Adjunct Professor of Law; *Vice Chancellor, Delaware Court of Chancery*
Willy Stern, *Adjunct Professor of Law*
Judge Amul Thapar, *Adjunct Professor of Law*; *Judge, U.S. Court of Appeals for the Sixth Circuit*
Wendy Tucker, *Adjunct Professor of Law*; *Attorney, McGee, Lyons and Ballinger*; *Member, Tennessee Board of Education*

F. Mitchell Walker, *Adjunct Professor of Law; Partner, Bass Berry & Sims*
Timothy Warnock, *Adjunct Professor of Law; Partner, Riley Warnock & Jacobson*
Robert Watson, *Adjunct Professor of Law; Senior Vice President & Chief Legal Officer, Metropolitan Nashville Airport Authority*
Margaret Williams, *Adjunct Professor of Law; Senior Research Associate, Federal Judicial Center*
Thomas Wiseman III, *Adjunct Professor of Law; Partner, Wiseman Ashworth Law Group*
Tyler Yarbro, *Adjunct Professor of Law; Partner, Dodson Parker Behm & Capparella*

***