Journal of International Business and Law

Volume 18 | Issue 1 Article 7

12-1-2018

Into the Crucible: Considering the Springboard Doctrine in CFAA Litigation

Nam Youn Kim
Maurice A. Deane School of Law at Hofstra University

NOTE

INTO THE CRUCIBLE: CONSIDERING THE SPRINGBOARD DOCTRINE IN CFAA LITIGATION

*Nam Youn Kim**

I. INTRODUCTION

"I like to think of it less as embezzling and more as an involuntary goodwill contribution."[1]

The cataclysmic effects of a computer breach—and the misuse of confidential information—on a business or employer cannot be gainsaid. Indeed, when Certegy Check Services revealed in 2007 that a former employee stole customer records that revealed credit card numbers, bank accounts, and other personal information, it agreed to pay $850,000 for investigative costs and attorney's fees alone.[2] The most vexing concern, however, is the possibility of confidential information falling into the hands of a competitor. In a computer-driven era, this is an issue that is both timely and timeless for businesses. So where is the timely thinking for this timeless problem? The Computer Fraud and Abuse Act ("CFAA")[3] stands as a vehicle for relief, but it is still wanting in many aspects even if enacted by wise men.

To the dismay of employers, the culprit is often an employee: a survey of employees who lost or left a job in 2008 revealed that seventy-nine percent of respondents took data without their employer's permission.[4] Some employees take confidential information with them for the benefit of a competing business if not that of their own, and choose to exhaust their former employer's goodwill.[5] As a response, employers have utilized the CFAA not infrequently to bring civil actions against those employees. But a look at CFAA decisions in the employment context reveals a circuit split in which some courts only consider *access* and not *use* of information.[6] In some circuits, defective employees who misuse confidential information are not held liable under the CFAA because they technically had authorization to that information at the time of misappropriation.[7] For employers, this has left much to be desired.

---

* J.D. Candidate, Maurice A. Deane School of Law at Hofstra University, 2019. I would like to extend my gratitude to Professors Karen Fernbach and Juliana Campagna, as well as my Notes and Comments Editor, William Vallejo, for their invaluable comments and edits to this Note.

1 JIM BUTCHER, COLD DAYS 190 (2012).

2 Linda McGlasson, *Certegy Reaches Data Breach Settlement*, BANK INFO SECURITY (Apr. 20, 2010), https://www.bankinfosecurity.com/certegy-reaches-data-breach-settlement-a-2441.

3 18 U.S.C.S. § 1030 (LexisNexis 2017).

4 SYMANTEC, https://www.symantec.com/about/newsroom/press-releases/2009/symantec_0223_01 (last visited Dec. 12, 2018).

5 *See, e.g.*, Brian Krebs, *Data Theft Common by Departing Employees*, WASH. POST (Feb. 26, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/02/26/AR2009022601821.html; Howard Levitt, *How to Prevent an Employee Stealing Confidential Information*, FIN. POST (May 18, 2017), http://business.financialpost.com/executive/careers/how-to-prevent-an-employee-stealing-confidential-information.

6 *See, e.g.*, WEC Carolina Energy Sols. L.L.C. v. Miller, 687 F.3d 199 (4th Cir. 2012); LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

7 *Compare* United States v. John, 597 F.3d 263, 271 (5th Cir. 2010) (recognizing that courts have typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user), *with*

This Note addresses this very issue. It first provides an overview of the CFAA in relation to businesses and employers. It considers the impacts felt by businesses and employers then looks at a solution that other common law nations, specifically the United Kingdom and Canada, have espoused to deal with the above issue. This Note also turns to the National Labor Relations Act ("NLRA")[8] for guidance and discusses vicarious liability of new employers as well. There are Notes and Comments on the "agency," "contract," and "code-based" approaches to interpreting the CFAA,[9] but this Note is different. It suggests that American trial courts consider the "springboard" doctrine[10] for employers in CFAA litigation.

II. AN OVERVIEW OF THE COMPUTER FRAUD AND ABUSE ACT

Also known as the federal anti-hacking law, the CFAA was enacted in 1986 to "amend title 18, United States Code, to provide additional penalties for fraud and related activities in connection with access devices and computers, and other purposes."[11] It started out as a criminal statute that protected "federal interest computers"[12] and it was only through the 1994 amendment that civil actions were allowed under the CFAA.[13] Many people were unaware of its existence, but the CFAA drew nationwide attention and criticism when prosecutors utilized the CFAA to prosecute Aaron Swartz, a computer programmer who committed suicide after a years-long legal battle for mass downloading academic journals.[14] The American Civil Liberties Union brought more spotlight when it challenged the constitutionality of the CFAA, claiming that the statute's "exceeds authorized access" provision wrongfully prohibits academics, researchers, and journalists from visiting websites and investigating companies' online practices.[15] Recently, LinkedIn, a business-oriented social networking website, brought suit under the CFAA against a startup that was scraping publicly available data from LinkedIn's website.[16] With technological advances, the CFAA has become more relevant and has governed a growing number of situations.

LVRC Holdings L.L.C. v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (choosing to stay textual and rejecting any analysis of "use").

[8] 29 U.S.C. §§ 151-169 (2012).

[9] *See, e.g.*, Katherine M. Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819 (2009).

[10] The "springboard" doctrine recognizes that a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication.

[11] Computer Fraud and Abuse Act of 1986, S. 2281, 99th Cong. (1986).

[12] Computer Fraud and Abuse Act of 1986, H.R. 4718, 99th Cong. § 2 (1986).

[13] Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, tit. XXIX, 108 Stat. 2097, 2098 (1994) (codified at 18 U.S.C. § 1030(g)).

[14] Grant Burningham, *The Most Hated Law on the Internet and Its Many Problems*, NEWSWEEK (Apr. 16, 2016), http://www.newsweek.com/most-hated-law-internet-and-its-many-problems-cfaa-448567.

[15] *Sandvig v. Sessions – Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online*, ACLU (Sept. 12, 2017), https://www.aclu.org/cases/sandvig-v-sessions-challenge-cfaa-prohibition-uncovering-racial-discrimination-online.

[16] Prayag Narula, *LinkedIn Vs. hiQ Ruling Casts A Long Shadow Over The Tech Industry*, FORBES (Sept. 20 2017), https://www.forbes.com/sites/forbestechcouncil/2017/09/20/linkedin-vs-hiq-ruling-casts-a-long-shadow-over-the-tech-industry/#60d15cb45e6c.

Suing under the CFAA can be more advantageous than suing under the Uniform Trade Secrets Act or the Defend Trade Secrets Act because a claimant does not need to prove that the information obtained is a trade secret.[17] In trade secret litigation, claimants must first and foremost surmount the "trade secret" hurdle if they are going to satisfy the "likelihood of success on the merits" element for a preliminary injunction.[18] But intangibles like business goodwill may not be considered a trade secret, even though they are still considered assets on a balance sheet—this means that employers can suffer injury even if no trade secret is involved. In contrast a claimant may recover such intangible assets under the CFAA.

Many claimants, nonetheless, sue under all three statutes and more. State laws similar to the CFAA exist, but the CFAA can be used to invoke federal jurisdiction, which may be advantageous for employers in many instances.[19] Many state judges are elected and often times, there may be grounds for recusal in tech-heavy states.[20]

The CFAA states, in pertinent part: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access,[21] and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section."[22] Under subsection (c), "The punishment for an offense under subsection (a) or (b) of this section is . . . a fine under this title or imprisonment for not more than ten years, or both . . . ."[23] The statute of limitations for the CFAA is two years.[24] It runs from "the date of the act complained of or the date of the discovery of the damage."[25]

The term "protected computer" includes a computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."[26] Thus, in *United States v. Ivanov*, the court upheld the

---

[17] There is simply no mention of "trade secret" in 18 U.S.C. § 1030.

[18] *See, e.g.*, Sole v. Wyner, 551 U.S. 74, 84 (2007) (discussing probability of success factor); Ashcroft v. ACLU, 542 U.S. 656 (2004); John Leubsdorf, *Preliminary Injunctions: In Defense of the Merits*, 76 FORDHAM L. REV. 33, 35 (2007) ("[T]he strength of the plaintiff's case under the substantive law—usually referred to as the plaintiff's likelihood of prevailing—is an important, perhaps the most important, factor in determining whether the plaintiff can obtain preliminary relief.").

[19] 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.").

[20] Chris Zubak-Skees, *California earns 'C' for judicial financial disclosure*, THE CTR. FOR PUB. INTEGRITY (May 19, 2014), https://www.publicintegrity.org/2013/12/04/13721/california-earns-c-judicial-financial-disclosure ("California Justice Kathryn Werdegar owned between $100,001 and $1 million worth of stock in Wells Fargo – yet the judge participated in a court decision denying an appeal to a couple who accused Wells Fargo of predatory lending and unlawful foreclosure . . . In January 2012, Justices Ming Chin and Joyce Kennard joined the majority opinion in *O'Neil v. Crane Co.* Crane, an industrial-product manufacturer was sued for a wrongful death . . . Caterpillar, a heavy equipment maker filed a "friend-of-the-court" brief on behalf of the defendants. Chin and Kennard both owned Caterpillar stock in 2012.").

[21] Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at *14 (E.D. Pa. July 13, 2007) ("[T]he point of the access requirement, as explained by the Senate Committee, is to ensure that the use of the computer is integral to the perpetration of a fraud, in contrast to the more expansive definitions of mail and wire fraud.").

[22] 18 U.S.C.S. § 1030(a) (LexisNexis 2017).

[23] *Id.* § 1030(c).

[24] *Id.* § 1030(g).

[25] *Id.*

[26] *Id.* § 1030(e)(2)(B).

indictment of the defendant who, from his home in Russia, hacked into a computer system in Connecticut.[27] This applies in the employment context as well, because when employees access their employer's computer and misappropriate information, the computer is most likely used to affect "interstate or foreign commerce or communication."[28]

Further, "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator . . . [which] may be brought only if the conduct involves 1 of the factors set forth in subclauses" of the statute.[29] The pertinent subclause is (c)(4)(A)(i)(I), which provides a cause of action for "loss to 1 or more persons during any 1-year period . . . aggregating at least $ 5,000 in value[.]"[30]

Loss under the CFAA is defined 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."[31] Damages are defined as "any impairment to the integrity or availability of data, a program, a system, or information."[32] In *Spec Simple, Inc. v. Designer Pages Online, L.L.C.*, Judge Kornreich accurately stated that, based on the plain definition, "Damages for unfair competition injuries . . . are not recoverable under the CFAA."[33] Thus, properly asserting loss or damages is vital to a successful CFAA claim.

When the 1994 amendment allowed civil actions to be brought under the CFAA, employers seized it as a vehicle for gaining relief.[34] However, in the employment context—specifically the scenario where an employee misappropriates confidential information—there has been a circuit split. This split is over the scope of the "exceeds authorized access" provision.[35] The following question sums up the heart of the matter: is a former employee off the hook for misusing confidential information as long as they were previously authorized to access it by their former employer?

In *United States v. John*, where the defendant account manager accessed Citigroup's internal computer system and provided her half-brother with customer account information

---

[27] 175 F. Supp. 2d 367 (D. Conn. 2001).

[28] Orin Kerr, *Does the federal computer hacking law apply to a laptop not connected to the Internet?* WASH. POST (Aug. 24, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/08/25/does-the-federal-computer-hacking-law-apply-to-a-laptop-not-connected-to-the-internet/?utm_term=.d272f2191091 ("Computers are ubiquitous as tools of modern commerce, and intrastate use of computers often has interstate effects. Computer data created and used in one state is easily moved across state lines, and breaches of computer security among intrastate computers can have an effect on computer use generally.").

[29] The subclauses of the statute are (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). "(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) 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."

[30] 18 U.S.C.S. § 1030(c)(4)(A)(i)(I) (LexisNexis 2017).

[31] *Id.* § 1030(e)(11).

[32] *Id.* § 1030(e)(8).

[33] 56 Misc. 3d 700, 710 (N.Y. Sup. Ct. 2017).

[34] *See, e.g.*, EF Cultural Travel BV v. Explorica, 274 F.3d 577 (1st Cir. 2001); WEC Carolina Energy Sols. L.L.C. v. Miller, 687 F.3d 199, (4th Cir. 2012).

[35] 597 F.3d 263 (5th Cir. 2010).

enabling him to incur fraudulent charges, the Fifth Circuit considered whether "authorized access" or "authorization" may encompass limits placed on the *use* of information.[36] The court "conclude[d] that it may," and "recognized that '[c]ourts have . . . typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."[37] This is in contrast to *LVRC Holdings L.L.C. v. Brekka*, where the Court of Appeals for the Ninth Circuit declared, "No language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."[38] "Rather, the definition of 'exceeds authorized access' in [the CFAA] indicates that Congress did not intend to include such an implicit limitation in the word 'authorization.'"[39] The Fifth Circuit clearly considered "expected norms" and "intended use" even though access *per se* was authorized, while the Ninth Circuit chose to stay textual and rejected any analysis of use.

This contrast is also apparent in other circuits. In *EF Cultural Travel BV v. Explorica, Inc.*, a former employee of a travel organization used information to which he was privy only because of his employment there for a scraper program that enabled his new employer to obtain information from his former employer's website.[40] The First Circuit stated that "If EF's allegations are proven, it will likely prove that whatever authorization Explorica had to navigate around EF's website (even in a competitive vein), it exceeded that authorization by providing proprietary information and know-how to [a third party] to create the scraper."[41] This is in sharp contrast to *WEC Carolina Energy Sols. L.L.C. v. Miller*, where the Court of Appeals for the Fourth Circuit, based on the "ordinary, contemporary, common meaning" of "authorization," declared that "neither ["without authorization" or "exceed authorized access"] of these definitions extends to the improper *use* of information validly accessed."[42]

Evidently, in circuits where courts do not consider the misuse of information, employers are left without any redress, at least under the CFAA. This is why I suggest looking at other common law nations and how their courts have dealt with employees misappropriating confidential information. Courts of the United Kingdom and Canada have applied the springboard doctrine, which recognizes that an employee is "springboarded" into a head start when they take advantage of confidential information belonging to their former employer. This has translated into those same courts issuing springboard injunctions to stop defective employees from gaining head starts. Although it may not be a panacea for employers, the springboard doctrine may provide some meaningful relief.

---

36 597 F.3d 263 (5th Cir. 2010).

37 *Id.* at 271.

38 581 F.3d 1127, 1133 (9th Cir. 2009).

39 *Id.*

40 274 F.3d 577 (1st Cir. 2001).

41 *Id.* at 583.

42 687 F.3d 199, 204 (4th Cir. 2012).

III. HE WENT DATA WAY

With the advent of technology, and the "Internet of Things,"[43] misappropriation and misuse of confidential information by employees has become easier. Portable devices such as tablets, computers, and memory sticks allow employees to take information surreptitiously. The increased use of cloud-based computing systems, which allow the storage and access of data over the internet, means that employers are vulnerable that much more.[44] Utilizing Apple's iCloud, Microsoft's OneDrive, or Google Drive means that an employee can access confidential information anywhere through a synced company tablet. Further, employee mobility has increased as businesses have gone global,[45] and presumably, the concomitant problems such as competition for employees and corporate espionage have increased as well.

Symantec Corporation and the Ponemon Institute released findings of a survey of employees who lost or left a job in 2008.[46] The results should be taken with the caveat that 2008 was a very difficult year[47]—people are more inclined to steal during difficult times. That said, some statistics therein are nonetheless eye-opening. Fifty-nine percent of employees admitted to stealing confidential company information, such as customer contact lists.[48] Of those who admitted to taking data, sixty-one percent reported having an unfavorable view of their former employer.[49] The most commonly identified kinds of records taken included e-mail lists, employee records, customer information including contact lists and non-financial information.[50] To add, the highest percentage of survey responses came from the financial services industry.[51] Here are some further statistics:

53% of respondents downloaded information onto a CD or DVD, 42% onto a USB drive and 38% sent attachments to a personal e-mail account.[52]

82% of respondents said their employers did not perform an audit or review of paper or electronic documents before the respondent left his/her job.[53]

24% of respondents had access to their employer's computer system or network after their departure from the company.[54]

---

[43] Jacob Morgan, *A Simple Explanation of 'The Internet of Things,'* FORBES (May 13, 2014), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#23150dfe1d09 ("[C]oncept of basically connecting any device with an on and off switch to the Internet (and/or to each other). This includes everything from cellphones, coffee makers, washing machines, headphones, lamps, wearable devices and almost anything else you can think of.").

[44] Fahmida Y. Rashid, *The Dirty Dozen: 12 Cloud Security Threats,* INFOWORLD (Mar. 11, 2016), https://www.infoworld.com/article/3041078/security/the-dirty-dozen-12-cloud-security-threats.html (identifying *inter alia* data breaches, system vulnerabilities, account hijacking, malicious insiders, and data loss as cloud security threats).

[45] MERCER, https://www.imercer.com/content/employee-mobility.aspx.

[46] SYMANTEC, https://www.symantec.com/about/newsroom/press-releases/2009/symantec_0223_01.

[47] Steve Denning, *Lest We Forget: Why We Had A Financial Crisis*, FORBES (Nov. 22, 2011), https://www.forbes.com/sites/stevedenning/2011/11/22/5086/#661fbff6f92f.

[48] SYMANTEC, *supra* note 4.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] SYMANTEC, *supra* note 4.

[53] *Id.*

[54] *Id.*

The CFAA can encompass intellectual property. Thus, the scale and scope of the loss of intellectual property in the United States is relevant. According to the Commission on the Theft of American Intellectual Property, annual losses are approximately $300 billion.[55] This can have a downhill effect, as businesses are less likely to innovate if they believe that confidential information to which they have devoted much time and effort is highly susceptible to theft or misappropriation.

IV. THE IMPACT ON BUSINESSES AND EMPLOYERS

After an employee misappropriates confidential information, the negative effects on a business can include immediate financial loss as well as future financial loss due to damaged public perception. If a colleague mentions Equifax, you will likely recall the indelible Equifax data breach from 2017.[56] The credit-reporting agency was reportedly named defendant in over fifty class action lawsuits after the incident.[57] Consider also the discouragement of shareholders and investors,[58] as well as lost company morale.[59] It goes without saying that the effects are multiplied manyfold for small businesses because comparatively, they have fewer resources to use as a "financial cushion."[60] When considering the impact on businesses and employers, hear it directly from one of them:

Our businesses and relationships with customers are dependent upon our ability to maintain the confidentiality of our [own] and our customers' trade secrets and confidential information (including customer transactional data and personal data about our employees, our customers and our customers' customers). Unauthorized access to such information may occur, resulting in theft, loss or other misappropriation. Any theft, loss or other misappropriation of confidential information could have a material adverse impact on our competitive positions, our relationships with our customers and our reputation and could subject to regulatory inquiries and enforcement, civil litigation and possible financial liability or costs.[61]

---

[55] THE COMMISSION ON THE THEFT OF AMERICAN INTELLECTUAL PROPERTY, http://www.ipcommission.org/report/ip_commission_report_052213.pdf.

[56] Seena Gressin, *The Equifax Data Breach: What to Do*, FTC (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

[57] Anthony Giorgianni, *Should You Participate in a Class Action Against Equifax?*, CONSUMER REPORTS (Sept. 19, 2017), https://www.consumerreports.org/lawsuits-settlements/should-you-participate-class-action-against-equifax/.

[58] *See* Wendy Robinson, *The Effects of Corruption on Business*, AZCENTRAL, https://yourbusiness.azcentral.com/effects-corruption-business-15261.html (last visited Jan. 26, 2018) (pointing out entrepreneurs' risk of accruing losses through a decline in sales and misuse of scarce resources among others).

[59] John Freedman, *How Fraud Hurts You & Your Organization*, CHRON, http://smallbusiness.chron.com/fraud-hurts-organization-58563.html (last visited Jan. 26, 2018) ("The effect of fraud on a company's culture and morale can be shattering . . . Even if employees leave the company, they may carry an association with a fraudulent company into their next place of employment, even if they were not involved with the fraud at all.").

[60] *See generally How Big of a Problem is Employee Theft and Fraud?*, INCORP, https://www.incorp.com/help-center/business-articles/employee-theft-and-fraud-part1 (last visited Jan. 26, 2018) ("The smallest organizations suffered the largest losses because they typically employ fewer anti-fraud controls. In addition, fraud affected small businesses disproportionately because they have fewer resources.").

[61] FORM 8-K, http://www.wikinvest.com/stock/State_Street_(STT)/Filing/8-K/2009/F3484803.

Worth mentioning are the typical, common-sense examples of confidential information such as lists of customers or clients, price lists, market research data, information about new products, and employee remuneration. Information which is not commonly considered confidential but may be subject to protection include knowledge acquired by an employee as part of his or her duties during employment.[62] Employers frequently have agreements with respect to the knowledge that high-value employees hold.

V. THE SPRINGBOARD DOCTRINE

The springboard doctrine is not a novel concept. It is a legal sobriquet for situations where one is "springboarded" into an advantageous position at the expense of another. In 1960, the English court in *Terrapin Ltd v. Builders Supply Co (Hayes) Ltd* elucidated the concept.[63] The Terrapin plaintiff designed, and the defendant manufactured, prefabricated portable buildings that were high in demand after the Second World War.[64] The plaintiff communicated to the defendant its design for the buildings along with full manufacturing details, specifications, technical information, and know-how.[65] The plaintiff also disclosed a modification for the purposes of the parties' venture.[66] After their contract, however, the defendant offered for sale prefabricated buildings that had many of the features of the plaintiff's original design as well as modification, and the plaintiff moved for an interlocutory injunction.[67] It is in this case that the classic and immortal statement of the springboard doctrine was made by Justice Roxburgh:

[T]he essence of this branch of the law, whatever the origin of it may be, is that a person who has obtained information in confidence is not allowed to use it as a springboard for activities detrimental to the person who made the confidential communication, and springboard it remains even when all the features have been published or can be ascertained by actual inspection by any member of the public . . . Therefore, the possessor of the confidential information still has a long start over any member of the public. It is, in my view, inherent in the principle upon which the *Saltman* case rests that the possessor must be placed under a special disability in the field of competition in order to ensure that he does not get an unfair start.[68]

It is in this context that other nations' courts have granted springboard injunctions, and it seems apropos where a defective employee takes confidential information and is "springboarded" into an advantageous position at the expense of his or her former employer. The nature of confidential information makes it difficult for a court to assign value to the

---

[62] *See* Andrew Tobin, Industrial and Employment Law Factsheet: Protecting confidential information and business goodwill before, during and after employment, HOPGOODGANIM LAWYERS, http://www.hopgoodganim.com.au/page/Publications/Industrial_and_Employment_Law_Factsheet_Protecting_confidential_information_and_business_goodwill_before_during_and_after_employment (last visited Jan. 26, 2018).

[63] Terrapin Ltd v. Builders Supply Co (Hayes) Ltd [1960] RPC 128.

[64] *Id.*

[65] *Id.*

[66] *Id.*

[67] Terrapin Ltd v. Builders Supply Co (Hayes) Ltd [1960] RPC 128.

[68] *Id.*

information, and as such, damages can be a poor form of remedy.[69] It also very well may be that by the time trial takes place, any period of restraint will have expired.

In any case, a springboard injunction is not permanent; "[a]lthough a man must not use [confidential] information as a springboard to get a start over others, nevertheless that springboard does not last forever. If he does use it, a time may come when so much has happened that he can no longer be restrained."[70] This comports with the general sentiment in employment law that healthy competition should not be limited.

So, why should the springboard doctrine or injunction be imported? As pointed out earlier, courts have interpreted the CFAA in different ways, which could leave employers in some circuits without relief. But why are preliminary injunctions in this context inadequate? The stakes are simply too high. If courts have differing interpretations of the "exceeds authorized access" provision, businesses or employers cannot reliably depend on the judicial system. Damage to the reputation and goodwill of a business is inherently irreparable, but the burden is too onerous where there may still be disputed issues of fact.

I do not consider the differences between the springboard injunction and a permanent injunction or a temporary restraining order. Springboard injunctions are not permanent; thus, comparing it to a permanent injunction would not be useful. Temporary restraining orders essentially require the same elements as a preliminary injunction, so a separate analysis is unnecessary. With all that said, I expound below on the differences between a springboard injunction and a preliminary injunction.

A. The Differences Between a Springboard Injunction and a Preliminary Injunction

In the United States, trial courts more or less consider the following elements when granting a preliminary injunction: (1) whether the plaintiff is likely to succeed on the merits; (2) whether the denial will result in irreparable harm to the plaintiff; (3) whether granting the injunction will not result in irreparable harm to the defendant; (4) whether granting the injunction is in the public interest.[71]

On the other hand, to obtain a springboard injunction the employer must prove the following: (1) that there is unlawful activity on the part of the former employee; (2) that the former employee has as a result gained an unfair competitive advantage over the employer; (3) that the nature and period of the competitive advantage are more than "ephemeral" or "short term"; (4) that the advantage still exists at the date that the springboard injunction is sought and will continue unless the relief sought is granted.[72]

As a prima facie matter, a plaintiff employer need not prove irreparable harm to obtain a springboard injunction. The bar is lower for a springboard than a preliminary injunction. Irreparable harm required for a preliminary injunction is defined as, "potential

---

[69] *See* PAUL STANLEY, THE LAW OF CONFIDENTIALITY: A RESTATEMENT 126 (2008) ("[W]here a person intends to use arguably confidential information to compete against the claimant, the difficulties of quantifying loss or profits militates against regarding damages as an adequate remedy.").

[70] Potters-Ballotini Ltd v. Weston Baker [1977] R.P.D. & T.M. Cas. 202, 206 (C.A.).

[71] *See, e.g.*, P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, L.L.C., 428 F.3d 504, 508 (3d Cir. 2005).

[72] *See, e.g.*, Sun Valley Foods Ltd v. Vincent [2000] FSR 825.

harm which cannot be redressed by a legal or an equitable remedy following a trial"[73]; it must "be of peculiar nature, so that compensation in money cannot atone for it."[74] "Establishing a risk of irreparable harm" is not enough for a plaintiff to obtain a preliminary injunction;[75] the movant must overcome a "very high bar."[76] For businesses and employers, not having to prove this very high bar makes a springboard injunction significantly more appealing.

Of course, there is good reason for requiring a showing of irreparable harm for preliminary injunctions. They are "drastic" remedies.[77] A party seeking a preliminary injunction is asking a court to affect the rights of another party when the judge has limited information. However, the absence of the "irreparable harm" element in springboard injunctions need not be a great cause for concern. Where interference with customer relationships is involved, the Seventh Circuit has recognized that "it is not practicable to calculate damages to remedy this kind of harm."[78] In a copyright infringement action, the Ninth Circuit noted, "one wonders how [plaintiff] could prove how many sales it lost because of the presence of [defendant's] infringing software."[79] Other courts have shared similar thoughts.[80] Similarly, where an employee misappropriates information to his or her former employer's detriment, how exactly is the latter supposed to calculate money damages? Therefore, requiring a showing of irreparable harm is not always practical or accurate. This is why I propose the springboard injunction. After all, economics is a subject, not a technique, and applying the "measuring rod of money" can lead to other problems.[81]

In *Terrapin*, the English court accepted that Terrapin's business prospects and goodwill would be susceptible to damage if confidential information was going to be used against it in competition. A monetary remedy could not make it whole.[82] The court referred

---

[73] *See, e.g.,* Trico Equip., Inc. v. Manor, No. 08-5561, 2009 U.S. Dist. LEXIS 50524, at *22 (D.N.J. June 13, 2009).

[74] Campbell Soup Co. v. ConAgra, Inc., 977 F.2d 86, 92 (3d Cir. 1992) (quoting ECRI v. McGraw-Hill, Inc., 809 F.2d 223, 226 (3d Cir. 1987)).

[75] Spacemax Int'l L.L.C. v. Core Health & Fitness, L.L.C., No. 2:13-4015-CCC-JAD, 2013 U.S. Dist. LEXIS 154638, at *4-5 (D.N.J. 2013).

[76] Coalition for Common Sense in Gov't Procurement v. United States, 576 F. Supp. 2d 162, 168 (D.D.C. 2008).

[77] Uniformed Firefighters Ass'n v. New York, 79 N.Y.2d 236, 241 (N.Y. 1992).

[78] Foodcomm Int'l v. Barry, 328 F.3d 300, 304 (7th Cir. 2003). *See also* Cross Wood Products, Inc. v. Suter, 422 N.E.2d 953 (Ill. App. Ct. 1981) ("Not only did Cross Wood lose pecuniary profits when Suter actually made sales to Cross Wood customers (injury type 1), Cross Wood also lost its competitive position . . . We believe that this second type of harm was of an intangible though very real nature . . . The injury is therefore classified as irreparable.").

[79] Cadence Design Sys. v. Avant! Corp., 125 F.3d 824, 831 (9th Cir. 1997).

[80] *See* Budish v. Gordon, 784 F. Supp. 1320, 1337 (N.D. Ohio 1992) (finding that if the defendant was not enjoined from selling infringing books, there would be no reasonable manner for the plaintiff to prove how many sales he lost due to the defendant's competing books); Roland Machinery Co. v. Dresser Indus., Inc., 749 F.2d 380, 386 (7th Cir. 1984) ("In saying that the plaintiff must show that an award of damages at the end of trial will be inadequate, we do not mean wholly ineffectual; we mean seriously deficient as a remedy for the harm suffered . . . The damage award may come too late to save the plaintiff's business. He may go broke while waiting, or may have to shut down his business but without declaring bankruptcy.").

[81] ROBERT E. GOODIN ET AL, DISCRETIONARY TIME: A NEW MEASURE OF FREEDOM 8 (2008) ("Economists value things that are literally bought and sold directly at their sale price. But many things of value to us are not bought and sold. Economists bravely persist in trying to bring them 'indirectly into relation with the measuring rod of money' . . . .").

[82] Terrapin Ltd v. Builders Supply Co (Hayes) Ltd [1960] RPC 128.

back to the decision in *Shelfer v. City of London Electric Lighting* where it was held that "a person committing a wrongful act . . . is not entitled to ask the court to sanction his doing so by purchasing his neighbor's rights, by assessing damages in that behalf."[83]

In addition, with a springboard injunction, an employer does not need to prove that they are likely to succeed on the merits. Confidential information can be time-sensitive, and if an employer is denied an injunction because they could not prove this element without a fully-developed record, the harm that they suffer would be extremely disproportional. Consider also that when a judge rules that there is no likelihood of success on the merits, he or she is letting the plaintiff suffer irreparable harm. The judge will subsequently be in a "lock-in" situation because, when asked to decide whether the plaintiff was right or wrong, he or she faces internal and external pressures to justify the earlier decision.[84]

With the springboard injunction, an employer also does not need to prove that granting the injunction is in the public interest. This element has been read to also mean that "the injunction would not serve the 'public interest.'"[85] A perceivable disservice to the public interest would be punishing and holding the new employer vicariously liable for the defective employee's nefarious actions. However, the new employer was never entitled to the confidential information that the employee brought over and the impact on third parties is certainly something that courts may consider. If the new employer had no hand in any misappropriation, then they should not be liable, as many courts have already held. Discretion should be exercised when issuing springboard injunctions.

A springboard injunction is worth considering even when a restrictive covenant exists in a parties' employment contract. Restrictive covenants are frequently subject to litigation and they can easily be invalidated on public policy grounds.[86] One court has stated: "It is not the initial breach of a covenant which necessarily establishes the existence of irreparable harm but rather the threat of the unbridled continuation of the violation and the resultant incalculable damage to the former employer's business that constitutes the justification for equitable intervention."[87] More obviously, an employer would not be able to touch a former employee beyond the time and geographical limitations imposed by a covenant.

---

[83] Shelfer v. City of London Electric Lighting Co [1895] 1 Ch. 287.

[84] *See* Kevin J. Lynch, *The Lock-in Effect of Preliminary Injunctions*, 66 FLA. L. REV. 779, 781 (2015) ("Even when faced with information that an initial decision has not achieved the expected results, decision makers are biased towards continuing investment in that course of action. The lock-in effect thus introduces a systemic bias to sequential decision-making.").

[85] *See* Am. Hosp. Supply Corp. v. Hosp. Prods., Ltd., 780 F.2d 589 (7th Cir. 1986); Brunswick Corp. v. Jones, 784 F.2d 271 (7th Cir. 1986); Syntex Ophthalmics, Inc. v. Tsuetaki, 701 F.2d 677 (7th Cir. 1983); A.J. Canfield Co. v. Vess Beverages, Inc., 796 F.2d 903 (7th Cir. 1986).

[86] *See* Gillian Lester, *Choice of Law and Employee Restrictive Covenants: An American Perspective*, 31 COMP. LAB. L. & POL'Y J. 389, 390 ("A broad set of public policy concerns informs the reasonableness test: courts are concerned with protecting employees from hardship, often citing inequality of bargaining power as a basis for giving special scrutiny to non-compete agreements. Courts also articulate a general resistance to restraints on trade. There is a strong imperative that the restriction be no greater in terms of duration, geographic scope, and limitation on vocational activities than is reasonably necessary to protect the interests of the employer.").

[87] John G. Bryant Co. v. Sling Testing & Repair, Inc., 369 A.2d 1164, 1167 (Pa. 1977).

B. Obtaining the Springboard Injunction

In order to obtain the springboard injunction, the claimant will have to prove that the defective employee committed an unlawful activity. In the employment context, the employer could show, for example, that the employee circumvented a computer security screen, sent confidential information via e-mail, or that they physically took confidential files away from the premises in contravention of the company handbook. It is not difficult to think of all the ways by which an employee might unlawfully take information away in today's technological era.

The claimant employer will then have to show that the employee was "springboarded" into an advantageous position. In the CFAA context the employer could show that by accessing and misusing confidential information the defendant employee was able to accomplish a business objective that otherwise would not have been accomplished. Again, the CFAA can be more useful than other intellectual property-based laws because it is broader—it does not require a showing that the defendant misappropriated a trade secret. Of course, it can be applied to trade secret actions as well.

Further, an "ephemeral" or "short term" advantage will not be sufficient to justify the issuance of a springboard injunction. The advantage that the defendant enjoys must exist at the time the injunction is requested. The claimant's counsel should ask, "what is the effect and extent to which the defendant has gained an illegitimate advantage"?

Courts may also consider what impact the springboard injunction will have on the defendant. Indeed, a springboard injunction is an equitable remedy.[88] In *Universal Thermosensors v. Hibben*, the United Kingdom court declined to issue a springboard injunction to the plaintiff because granting it would have put the claimant in a better position than it would have been in.[89] The balancing of each side is reminiscent of the sliding scale approach to preliminary injunctions that former Judge Richard Posner conceived in *American Hospital Supply Corp v. Hospital Products*.[90] If the probability of the defendant's success on the merits multiplied by the potential harm to the defendant exceeds that of the plaintiff, a preliminary injunction should not be issued.[91]

---

[88] Samuel L. Bray, *The System of Equitable Remedies*, 63 UCLA L. REV. 530, 552-53 (2016) ("Compensation is imperfect. It operates only after violations have occurred, and so it can prevent violations only through the rough and inexact medium of deterrence . . . The solution to these problems is fairly obvious: There must be some way for courts to compel action or inaction. In contemporary American law, this is usually done by means of an equitable remedy, especially the injunction, accounting for profits, constructive trust, equitable lien, subrogation, equitable rescission, specific performance, and reformation.").

[89] *See* Universal Thermosensors Ltd v. Hibben and others [1992] 3 All ER 257 ("Holding back [a competing business] even for a period of six or twelve months from July 1990, would not have the effect simply of restoring the parties to the competitive position that each sought to occupy and that each would have occupied but for the defendant's misconduct. If it did, such a form of injunction would be fair and just. But the injunction would have a much more far-reaching effect. As already noted, the injunction would put the plaintiff in a better position than if there had been no breach of confidence.").

[90] 780 F.2d 589 (7th Cir. 1986).

[91] *Id.* at 593.

VI. CASE STUDIES: THE UNITED KINGDOM AND CANADA

A. United Kingdom

A look at decisions from the United Kingdom is instructive because they provide the clearest applications of the springboard doctrine. To note, the doctrine has found acceptance in Australia[92] and Hong Kong[93] as well.

In *Roger Bullivant Ltd. v. Ellis*, Ellis, the former Managing Director of Bullivant, took confidential information with him including a card index with the details of Bullivant's contacts. He then set up a competing business and used the card index to contact those clients in direct competition.[94] The High Court granted a springboard injunction prohibiting Ellis from entering into any contract made with or through any of the contacts in the card index until judgment.[95] Ellis argued that the injunction should not apply to any customers with whom he was able to make contact without using the card index.[96] The High Court concluded that "having made deliberate and unlawful use of Bullivant's property, he cannot complain if he finds that the eye of the law is unable to distinguish between those whom, had he so chose, he could have contacted lawfully and those whom he could not."[97]

QBE Management Services (UK) Ltd. v. Dymoke also provides a clear application of the springboard doctrine.[98] It was established that senior QBE employees secretly planned to take other QBE's employees to a rival business.[99] In addition to poaching colleagues, the senior employees also accessed QBE's confidential information, which they used to secure finance for their new venture.[100] They also solicited customers without informing QBE.[101] The High Court concluded that there could not be a clearer case for springboard relief and granted an injunction for twelve months from the date of resignation to remedy the head start the employees had unlawfully gained.[102]

In *UBS Wealth Management (UK) Ltd. v. Vestra Wealth LLP*, a former employee of UBS created a competing business, recruited employees from UBS, and resigned.[103] The court concluded that springboard relief is not confined to cases involving the abuse of confidential information but can operate to prevent, "any future or further serious economic loss to a previous employer caused by former staff members taking an unfair advantage of any serious breaches of their contract of employment."[104] In this case, an injunction until trial was granted preventing the defendants soliciting or dealing with any UBS client.[105]

---

92 APT Technology Pty Ltd v. Aladesaye [2014] FCA 966.

93 ICAP (Hong Kong) Ltd v. BGC Securities (Hong Kong) LLC & ORS [2005] 3 HKC 137.

94 Roger Bullivant Ltd. v. Ellis [1987] IRLR 491.

95 *Id.*

96 *Id.*

97 *Id.*

98 QBE Management Services (UK) Ltd. v. Dymoke [2012] IRLR 458.

99 *Id.*

100 *Id.*

101 *Id.*

102 *Id.*

103 UBS Wealth Management (UK) Ltd v. Vestra Wealth LLP [2008] EWHC 1974 (QB).

104 *Id.*

105 *Id.*

B. Canada

The springboard doctrine, or "théorie du templin," is widely accepted in Canada. Justice Guthrie from the Quebec Superior Court remarked, "What is really being protected in situations of this nature is the original process of mind. The protection is enforced against persons who wish to use the confidential information without spending the time, trouble and expense of going through the same process."[106] A foray into Canadian cases shows clear applications of the doctrine.

In *Apotex Fermentation Inc. v. Novopharm Ltd.*, plaintiff's former employee took with him documents relating to the technology he developed for Lovastatin, a "miracle" anti-cholesterol drug with great international market potential.[107] The former employee was hired by the defendant to develop commercial quantities of Lovastatin.[108] The defendant was "fully aware of and took advantage of [former employee's] breach of confidentiality to the distinct benefit of Novopharm."[109] The court stated that "it was entirely appropriate, and indeed necessary, in these circumstances for the scope of the [springboard] injunction to prohibit entirely Novopharm's activity with respect to Lovastatin."[110]

In *Matrox Electronic Systems Ltd. v. Gaudreau*, the plaintiff applied for an injunction against three of its former employees to stop them from using trade secrets and confidential information that they obtained through employment with the plaintiff.[111] The plaintiff developed a graphic design software and the defendants created their own that was modeled on the same software.[112] The former employees' software competed with that of the plaintiff and they took significantly less time to create it.[113] The court stated, "There is no doubt that during their employment with Plaintiff, individual Defendants' access to the '...systèmes, méthodes, procédés, inventions, créations (designs)... programmes, plans logiciels, dessins négatifs (blueprints), idées et projets...' concerning the IMPRESSION product, gave them a 'springboard.'"[114]

In *Pharand Ski Corp. v. Alberta*, the plaintiff claimed that the defendant misappropriated its site selection of Mt. Allan as well as its ideas for the area as a commercial skiing area.[115] The province was in search of a viable site for the 1988 Winter Olympic Games, but in or around the same time period, they also put out a "Proposals Call" for private developers to indicate their interest in developing an alpine ski area. In response, the plaintiff proposed Mt. Allan, which was provided to the defendant in confidence.[116] The defendant later used Mt. Allan. The court stated that the defendant used the information "as a springboard for itself and for the developer it selected after terminating the proposals call process . . . [t]he cost of the facilities at the other venues which the Government was

---

106 Matrox Electronic Systems Ltd. v. Gaudreau, [1993] Q.J. No. 1228.

107 Apotex Fermentation Inc. v. Novopharm Ltd. 1998 CarswellMan 318 (Manitoba Court of Appeal 1998).

108 *Id.*

109 *Id.*

110 *Id.*

111 Matrox Electronic Systems Ltd. v. Gaudreau, [1993] Q.J. No. 1228.

112 *Id.*

113 *Id.*

114 *Id.*

115 Pharand Ski Corp. v. Alberta, [1991] A.J No. 471.

116 *Id.*

considering could have doubled [$30 Million] in the estimations of Deputy Minister MacDonald."[117]

VII. NATIONAL LABOR RELATIONS ACT SECTION 10(j): THE LABOR COUNTERPART

The springboard injunction is not as foreign as it seems; a similar injunction already exists in the field of labor law. Thus, as guidance for the CFAA in the employment context, a look at the NLRA may be useful. The National Labor Relations Board ("NLRB") exercises jurisdiction over labor disputes that arise under the NLRA. Under section 10(j) of the NLRA, the NLRB can seek temporary injunctions against employers or unions "to protect the process of collective bargaining and employee rights under the Act, and to ensure that Board decisions will be meaningful."[118] Section 10(j) states:

The Board shall have power, upon issuance of a complaint as provided in subsection (b) charging that any person has engaged in or is engaging in an unfair labor practice, to petition any district court of the United States . . . within any district wherein the unfair labor practice in question is alleged to have occurred or wherein such person resides or transacts business, for temporary relief or restraining order.[119]

Congress enacted section 10(j) because it recognized that administrative proceedings can be long-drawn-out; therefore, remedies can frequently be frustrated. The Senate Report on 10(j) states:

Experience under the National Labor Relations Act has demonstrated that by reason of lengthy hearings and litigation enforcing its orders, the Board has not been able in some instances to correct unfair labor practices until after substantial injury has been done. Under the present act the Board is empowered to seek interim relief only after it has filed in the appropriate circuit court of appeals its order and the record on which it is based. Since the Board's orders are not self-enforcing, it has sometimes been possible for persons violating the act to accomplish their unlawful objective before being placed under any legal restraint and thereby to make it impossible or not feasible to restore or preserve the status quo pending litigation.[120]

This immediately calls to mind the same scenario with the springboard doctrine. By the time trial takes place, the "springboard" period will have expired.

Consider section 10(j) in the context of union-organizing campaigns. In *Hooks ex rel. NLRB v. Ozburn-Hessey Logistics, L.L.C.*, the respondent committed numerous violations of the NLRA and discouraged employees from supporting the United Steelworkers Union.[121] Respondent's managers threatened employees with reprisals if they supported union. Managers confiscated and destroyed pro-union literature on tables in addition to calling the police to remove two union organizers who were distributing pro-union literature.[122] The

---

117 *Id.*

118 *10j Injunctions*, NLRB, https://www.nlrb.gov/what-we-do/investigate-charges/10j-injunctions (last visited on Jan. 29, 2018).

119 29 U.S.C.S. § 160(j) (LexisNexis 2017).

120 S. Rep. No. 105, 80th Cong., 1st Sess. 27 (1947).

121 775 F. Supp. 2d 1029 (W.D. Tenn. 2011).

122 *Id.*

petitioner argued that, without an injunction, any relief ultimately ordered would be futile. Respondent committed numerous unlawful employment practices that have "chilled" employees' support for the union. The court granted the injunction and stated that doing so "is in the public interest to effectuate the policies of the NLRA and to protect the NLRB's remedial powers."[123]

In *Barker ex rel. NLRB v. A.D. Conner Inc.*, the respondent, a fuel hauling company, allegedly violated federal labor laws, and a Regional Director for the NLRB petitioned for section 10(j) injunctive relief.[124] A.D. Conner was a company owned by William McEnery, but when it shut down a number of drivers transferred to a non-union company owned by McEnery.[125] There was evidence to support that the employer shut down the first plant in order to avoid collective bargaining and labor obligations. The court stated that "Management never responded to the Union's request for information."[126] Management "refused to recognize the Union's representation of these 16 drivers and has refused to abide by the terms of the expired collective bargaining agreement."[127] In granting the 10(j) injunction, the court stated "Diminution in Union support in the interim increases the likelihood that the employees will be irreparably deprived of Union representation when the Board finally issues its order."[128]

The springboard injunction is 10(j)'s symmetrical counterpart in labor and employment law. If, in *QBE Management Services*, the court had not granted the springboard injunction, the former employees would have gained an unlawful head start.[129] It would have been futile to do anything about the head start later on, much like how any relief ultimately ordered would have been futile in *Hooks*.[130] Thus, any court that considers the springboard doctrine is not treading into uncharted waters.

VIII. VICARIOUS LIABILITY

It is important to address the topic of vicarious liability—also known as *respondeat superior*—because it is a common law concept in employment law that comes up frequently.[131] Absent an indemnification clause, an employer is liable for an employee's unlawful acts as long as the employee was acting within the scope of employment.[132] The CFAA does not explicitly mention anything about vicarious liability.[133] Thus, it is not surprising that there has been a circuit split as to whether a new employer should be subject to

---

123 *Id.* at 1050.

124 807 F. Supp. 2d 707 (N.D. Ill. 2011).

125 *Id.*

126 *Id.* at 727.

127 *Id.* at 728.

128 *Id.* at 729.

129 QBE Management Services (UK) Ltd. v. Dymoke [2012] IRLR 458.

130 775 F. Supp. 2d 1029 (W.D. Tenn. 2011).

131 Thomas M. Winn III, *Labor and Employment Law*, 37 U. RICH. L. REV. 241, 260 (2002) ("Under the doctrine of respondeat superior—literally, 'let the master answer'—an employer is liable for the tortious acts of its employee if the employee was performing his employer's business and acting within the scope of his employment . . . .").

132 *Id.*

133 There is simply no mention of vicarious liability in 18 U.S.C. § 1030.

vicarious liability when a former employee carries away confidential information. So what happens when an employee commits such an act?

In *Calence, L.L.C. v. Dimension Data Holdings*, the plaintiff claimed that the defendant "hatched a plot" to open a competing office by stealing plaintiff's employees, and also that the plaintiff's former employees assisted in the plan by providing the defendant with confidential information.[134] The United States District Court for the Western District of Washington, which ruled against the CFAA claim, stated that "plaintiff points to no evidence in the record that corporate defendants directed either of those individuals to take any of the alleged improper actions. Accordingly, the Court finds no basis for the CFAA claim."[135]

This contrasts with *SBM Site Services L.L.C. v. Garett*.[136] The plaintiff, a provider of facility support services, maintained a "Knowledge Portal," containing customer lists, forms and procedures to operate the business.[137] The defendant, who worked as a senior vice president for plaintiff, left and joined a competitor.[138] He sent confidential information to executives of his new employer.[139] The court stated that "[i]t is reasonable to infer that Garrett accessed SBM's laptop during the time that he was employed with [new employer] and in the scope of such employment.[140] Plaintiff's Amended Complaint therefore states a claim for violation of the CFAA against [new employer]."[141] It should be noted that the defendant in *Garett* retained his former employer's laptop for 3 weeks after his employment ended.[142] He retained it for 2 weeks after he started work.[143] The new employer's executives received the confidential information despite plaintiff vice president not having resigned yet.[144]

In *Charles Schwab & Co. v. Carter*, the District Court for the Northern District of Illinois remarked that "[a]ny presumption of vicarious liability . . . cannot apply when doing so would conflict with clear congressional intent."[145] However, it concluded that "Defendants affirmatively urged Carter to access Schwab's computer system beyond his authorization for their benefit."[146] Imposing vicarious liability "would further the CFAA's purpose" which is to "punish those who intentionally access computer files and systems without authority and cause harm."[147] This is in contrast to the New Hampshire District Court's declaration in *Doe v. Dartmouth-Hitchcock Med. Ctr.* that "the CFAA is essentially a criminal statute.[148] It

---

134 2007 U.S. Dist. LEXIS 38043 (W.D. Wash. 2007).

135 *Id.* at 16.

136 2012 U.S. Dist. LEXIS 24130 (D. Colo. 2012).

137 *Id.* at 4.

138 *Id.* at 4.

139 *Id.* at 7.

140 *Id.* at 4.

141 *Id.* at 13.

142 *Id.* at 13.

143 *Id.* at 14.

144 *Id.* at 14.

145 2005 U.S. Dist. LEXIS 21348, at *22 (N.D. Ill. 2005).

146 *Id.* at 18.

147 *Id.* at 22.

148 Doe v. Dartmouth-Hitchcock Med. Ctr., No. 00-100-M, 2001 U.S. Dist. LEXIS 10704, at *12 (D.N.H. 2001). ("Expanding the private cause of action created by Congress to include one for vicarious liability against

creates only a limited private right of action 'against *the violator*,' that is, against a person who violates the statute with the requisite criminal intent."[149] Its "unequivocal purpose is to deter and punish those who intentionally access computer files and systems . . . ."[150]

There is no affirmative duty on an employer to inquire about the source or ownership of information.[151] The new employer will not be held liable unless they had some knowledge or involvement in the employee misappropriating confidential information.[152] Then, to reach these former employees, the former employer will have to rely on a non-compete agreement.[153] But in reality, not everyone signs a non-compete agreement, or if there is one, it may be invalidated because it is too broad.[154] They may restrict employees for short periods of time.[155] Further, if specific money damages are included in an agreement and payment is an option, in contrast to employers, employees may not have the "deep pockets" that will provide claimants with meaningful remedy under the CFAA.[156] Then, the next best option would be to pursue a springboard injunction against the employee.

IX. ADOPTING THE SPRINGBOARD

There are two ways in which the springboard doctrine can be adopted: courts can exercise their discretion or Congress can incorporate springboard principles into the CFAA. The Federal Rules of Civil Procedure outline some basic requirements in regard to injunctions. "Every order granting an injunction and every restraining order must: (A) state the reasons why it is issued; (B) state its terms specifically; and (C) describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required."[157]

The Supreme Court has stated that district courts have "the discretion to issue a broad injunction in cases where "a proclivity for unlawful conduct has been shown."[158] The district court may "even enjoin certain otherwise lawful conduct when the defendant's conduct has demonstrated that prohibiting only unlawful conduct would not effectively protect the plaintiff's rights against future encroachment."[159] When the beneficiary of an junction's seeks to "enforce [the injunction] more effectively, equity countenances the

---

persons who did not act with criminal intent and cannot be said to have violated the statute, like the Dartmouth defendants, would be entirely inconsistent with the plain language of the statute.").

149 *Id.*

150 *Id.* at 13.

151 *See* Fox v. Millman, 45 A.3d 332, 347 (N.J. 2012).

152 *Id.*

153 *Id.*

154 *Id.*

155 *Id.*

156 *Id.*

157 Fed. R. Civ. P. 65(d)(1).

158 McComb v. Jacksonville Paper Co., 336 U.S. 187, 192 (1949) (finding that injunction barring violations of Fair Labor Standards Act was justified based on defendant's "record of continuing and persistent violations" of law).

159 Russian Media Grp., L.L.C. v. Cable Am., Inc., 598 F.3d 302, 307 (7th Cir. 2010) (citing FTC v. Nat'l Lead Co., 352 U.S. 419, 428-30 (1957)).

modification of a injunctive decree if a better appreciation of the facts in light of experience indicates that the decree is not properly adapted to accomplishing its purposes."[160]

Under the CFAA, any person who suffers damage or loss may "obtain compensatory damages and injunctive relief or other equitable relief."[161] In the context of antitrust injunctions, the Supreme Court has emphasized that "the trial is charged with inescapable responsibility to achieve [the injunctions] objective, although it may, if circumstances warrant, accept a formula for achieving the result by means less drastic than immediate dissolution or divestiture." Thus, any court that issues a springboard injunction would not be ruling by judicial fiat; it would merely be exercising the discretion granted to it. Of course, "[i]n exercising their sound discretion, courts of equity should pay particular regard for the public consequences in employing the extraordinary remedy of injunction."[162]

However, even though trial courts have the power to modify injunctions, the springboard doctrine should still be incorporated into the remedies available under the CFAA. As an example for legislators, the Illinois Trade Secrets Act ("ITSA") provides that a court may enjoin the "actual or threatened misappropriation" of a trade secret.[163] A party seeking an injunction under the ITSA must therefore prove both the existence of a trade secret and its misappropriation.[164] In 1947, Congress passed the Taft-Hartley Act which included the labor injunction.[165] The Endangered Species Act imposes on all federal agencies mandatory obligations to insure that any action authorized, funded, or carried out by them does not jeopardize existence of endangered species.[166] Thus, in *Tenn. Valley Auth. v. Hill*, the Supreme Court declared that refusal to enjoin the action would have ignored the "explicit provisions of the Endangered Species Act."[167] Similar to the ITSA and the NLRA, the CFAA should be amended to incorporate "springboard" principles. Congress can "intervene and guide or control the exercise of the courts' discretion."[168] Discretion exercised by courts is displaced only by a "clear and valid legislative command."[169] This route would ensure that the political process plays its part; people can participate by scrutinizing the statute or adding to it.

X. CONCLUSION

The CFAA is particularly relevant in an era where the definition of "computer" may continue to change. With the proliferation of new technology, employers will face a growing

---

[160] Philip Morris USA, Inc. v. Otamedia Ltd., 331 F. Supp. 2d 228, 246 (S.D.N.Y. 2004) ("The Court has 'authority to enjoin actions otherwise lawful when such action is deemed ... necessary to correct the evil effects of unlawful conduct.' . . . To be sure, as [defendant] points out, federal courts hesitate to sweep within an injunction a needlessly broad range of lawful conduct so as effectively to enjoin unlawful conduct.").

[161] 18 U.S.C.S. § 1030(g) (LexisNexis 2017).

[162] Weinberger v. Romero-Barcelo, 456 U.S. 305, 312 (1982).

[163] Illinois Trade Secrets Act, P.A. No. 85-366 (codified at ILL. ANN. STAT. ch. 140, 1 351- 359 (Smith-Hurd Supp. 1991)).

[164] *Id.*

[165] The Taft-Hartley Act is officially entitled the Labor Management Relations Act, 1947, ch. 120, 61 Stat. 136 (1947).

[166] 16 U.S.C.S. § 1536 (LexisNexis 2017).

[167] 437 U.S. 153 (1978).

[168] Weinberger v. Romero-Barcelo, 456 U.S. 305, 313 (1982).

[169] Porter v. Warner Holding Co., 328 U.S. 395, 398 (1946).

challenge to rein in former employees and the misappropriation of confidential information. The effects are indeed cataclysmic and businesses can be decimated. Consider small and mid-sized businesses that cannot afford litigation to drag on interminably. Businesses do not have to spend precious resources on litigation.

Despite these growing challenges, employers in some circuits will not find relief under one federal statute. That is why the springboard injunction should be considered by American courts or Congress. It is not as foreign as it seems. A similar legal mechanism exists already—section 10(j) of the NLRA is the springboard injunctions symmetrical counterpart in labor law.[170] Both mechanisms are utilized in situations where it may be too late to cure the plaintiff's injury by the time a trial court renders a decision.

In the employment context not all courts choose to apply the concept of *respondeat superior* and not all employees sign non-compete agreements. When they do the agreements may expire quickly. In those instances the springboard injunction can provide meaningful relief. As an alternative to courts exercising their discretion, the CFAA should be amended to incorporate springboard principles. Other common law nations, including the ones discussed above, have acknowledged and addressed the problem set forth in this Note. It is time that the United States follows suit and adopts a new solution to an unsolved problem.

[170] 29 U.S.C.S. § 160(j) (LexisNexis 2017).