Brooklyn Law Review

Volume 79
Issue 2
SYMPOSIUM:
Restatement Of...

Article 17

2014

Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context

Glenn R. Schieck

NOTES

Undercutting Employee Mobility

THE COMPUTER FRAUD AND ABUSE ACT IN THE TRADE SECRET CONTEXT

INTRODUCTION

In 1986, Congressman Bill Hughes stood before the U.S. House of Representatives to describe what type of person the Computer Fraud and Abuse Act (CFAA)[1] was directed toward: "The hacker is . . . a bright, intellectually curious, and rebellious youth," who could "become the white-collar crime superstar of tomorrow."[2] Hughes warned his colleagues that in this new iteration of corporate crime, "[t]he tools of the trade [will not be] Smith and Wesson, but IBM and Apple."[3]

A number of factors contributed to the public apprehension of computer crime reflected in Hughes's statement. Perhaps most important was the sudden and explosive rise of the personal computer, beginning in the late 1970s.[4] While initially popular in the home, personal computers quickly took hold in the workplace in the early 1980s, meaning that a wider variety of

---

[1] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (1988)).

[2] 132 CONG. REC. 7816 (1986) (statement of Rep. William J. Hughes).

[3] *Id.*

[4] As a testament to the explosive growth of personal computers during this time, consider that the Commodore 64, released in 1982, sold between 12.5 and 17 million units, making it to this day the best-selling personal computer of all time. Gareth Halfacre, *The Commodore 64 Turns 30*, BIT-TECH.NET (Aug. 1, 2012), http://www.bit-tech.net/news/hardware/2012/08/01/commodore-64-30/1; *see also* Lisa Fritscher, *Commodore 64: The Best Selling Personal Computer of All Time*, RETRO THING (Oct. 2, 2008), http://www.retrothing.com/2008/10/commodore-64-th.html; Jeremy Reimer, *Total share: 30 Years of Personal Computer Market Share Figures*, ARS TECHNICA (Dec. 15, 2005), http://arstechnica.com/features/2005/12/total-share/3/ (describing the first three highly successful personal computers released between 1977 and 1980: the Commodore PET, the Radio-Shack TRS-80, and the Apple).

valuable and sensitive information was stored in a digital form.[5] As this novel technology quickly became a large part of American work and home life, computers moved into the spotlight of both news and entertainment.[6] A number of movies released during this time depicted and risibly exaggerated the potential for people to commit crime and wreak havoc using computers, adding to public concern.[7] For example, in the movie *WarGames*, "a teenaged computer hacker who, thinking he was merely playing a game, inadvertently accessed a Department of Defense computer system and nearly precipitated thermonuclear war."[8] However the tipping point for legislators like Hughes came in 1984, when the findings of several private reports on cyber crime were "magnified by a groundswell of media attention toward computer crime generated by a number of incidents involving juvenile computer hackers."[9]

Having initially deferred to state-level regulation on the issue of computer crime, Congress ultimately gave in to public sentiment, and in 1984 enacted the CFAA as the first federal legislation directed specifically toward computer crime.[10] The original act was relatively narrow in scope, addressing only a small number of sophisticated computer crimes leveled against the government and financial institutions.[11] But the statute's narrow reach would not last long. A number of subsequent

---

[5] *See* Greggory S. Blundell, *Personal Computers in the Eighties*, BYTE, Jan. 1983, at 168, *available at* http://archive.org/stream/byte-magazine-1983-01/1983_01_BYTE_08-01_Looking_Ahead#page/n175/mode/2up. During "the late 1970's and early 1980's . . . [n]ew managers entering the business community brought with them a keen awareness of computer systems gained from both college study and home use." *Id.*

[6] For example, in 1982 *Time Magazine* awarded its Person of the Year award to the computer, which *Time* deemed "Machine of the Year," making it the first time a non-human received the honor. *A Letter From the Publisher: Jan. 3, 1983*, TIME, Jan. 3, 1983, *available at* http://content.time.com/time/subscriber/printout/0,8816,953629,00.html; *see also* Reimer, *supra* note 4.

[7] *See* Joseph M. Olivenbaum, *<Ctrl><Alt><Delete>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 596 (1997); *see also* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 910 (2003).

[8] Olivenbaum, *supra* note 7, at 596.

[9] Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 460 (1990). One such group of juvenile computer hackers was a collective of Milwaukee area teens known as the 414s, who in 1983 hacked the networks of a number of high profile institutions, including Memorial Sloan-Kettering Cancer Center and Los Alamos National Laboratory. Philip Elmer-Dewitt, *Computers: The 414 Gang Strikes Again*, TIME, Aug. 29, 1983, *available at* http://www.time.com/time/magazine/article/0,9171,949797,00.html.

[10] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)). The short title of the statute was amended to its current form in 1986, when it became the "Computer Fraud and Abuse Act of 1986." Pub. L. 99-474, 100 Stat. 1213 § 1 (1986).

[11] *See* Griffith, *supra* note 9, at 460-61.

amendments, notably in 1986, 1994, and 1996, greatly altered and expanded the CFAA by increasing the number of crimes covered under the act, relaxing pleading standards, creating a private right of action, and expanding the statute's scope to cover not just government and financial institution computers, but any computer connected to the internet.[12]

While the expanded CFAA is still invoked against sophisticated computer hackers,[13] the amendments have also created a dramatic rise in private litigation, in many cases involving defendants with only a rudimentary understanding of computers.[14] For example, a private cause of action exists under the CFAA against anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any . . . computer [in use in interstate commerce]."[15] Since 2000, employers have increasingly invoked these CFAA provisions against so-called "rogue employees" who misappropriate valuable trade secrets from a company before going to work for a competitor.[16] Traditionally, such a scenario would be addressed by state-level trade secret misappropriation statutes, many of which define a trade secret as "information . . . that . . . derives independent economic value . . . from not being generally known [and] is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[17] But when a computer is involved in the misappropriation, the issue appears to fall within the CFAA's ambit.[18] In an attempt to restrict or uphold the CFAA's

---

[12] *See* Part II *infra* (describing the numerous amendments broadening the CFAA's scope and substantive impact).

[13] For example, in 2011, computer programmer and internet activist Aaron Swartz was indicted under three provisions of the CFAA for manipulating MIT's computer network and subsequently "downloading over 4 million documents from JSTOR, a[n academic] research database." Chris Gayomali, *Reddit Co-Founder Aaron Swartz Indicted for Data Theft, Could Face 35 Years in Prison*, TIME, July 19, 2011, *available at* http://techland.time.com/2011/07/19/reddit-co-founder-aaron-swartz-indicted-for-data-theft-could-face-35-years-in-prison/.

[14] *See* Part II *infra* (describing the facts of *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000), in which defendant simply emailed documents from his current employer to his prospective employer).

[15] 18 U.S.C. § 1030(a)2(C) (2012). In this section the term "obtains" has been broadly defined to include even looking at information on a computer. 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 INFO. SOC'Y 405, 416 n.60 (2012) (citing S. REP. No. 99-432, at 6 (1986)).

[16] *See, e.g.*, Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122-23 (W.D. Wash. 2008).

[17] Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985); *see also infra* note 36 (discussing the definition of a trade secret under the UTSA).

[18] 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, 430.

applicability in such contexts, many jurists and commentators have focused on the authorization provision of the CFAA, specifically the requirement that to establish liability, one must access a computer "without authorization or exceed[ing] authorized access."[19] A broad interpretation of authorization, grounded in principles of agency law, holds that an employee can act without authorization even when granted full access to a computer system, by simply taking action at odds with his or her employer's interests.[20] In contrast, a narrow approach to authorization turns not on the employee's actions, but rather on the restrictions put in place by the employer.[21]

Firmly establishing a narrow interpretation of authorization under the CFAA will bring the statute closer to its intended purpose of targeting sophisticated computer criminals. Resolving this issue, however, does not address the fact that reliance on the CFAA threatens to undercut policy considerations of trade secret law. In particular, trade secret law strikes an important balance between protecting valuable company information on the one hand, and promoting the mobility of knowledge-based workers on the other hand. The CFAA undercuts and ignores this balance.[22] As employers increasingly turn to the CFAA as a favorable alternative to state-level trade secret statutes, a more sensible course of action is to amend the CFAA to adopt some limited substantive elements of trade secret law. Such an amendment would serve to diminish the CFAA's utility as an end run on state-level trade secret statutes, and in turn prevent the CFAA from undercutting policy considerations advanced by trade secret law.

Specifically, Congress should amend the CFAA to include a requirement that to establish liability, information misappropriated from a protected computer must have been "the subject of efforts . . . reasonable under the circumstances to maintain its secrecy," mirroring a provision in the Uniform

---

[19] 18 U.S.C. § 1030(a)2(C). *See, e.g.*, Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1649 (2003).

[20] *See* Part II *infra* (outlining the agency-based approach to authorization); *see also Shurgard*, 119 F. Supp. at 1125 (citations omitted).

[21] *See* Part II *infra* (outlining the narrow approach to authorization); *see also* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (noting that "'authorization' depends on actions taken by the employer").

[22] *See* Brenton, *supra* note 18, at 447. "From a normative viewpoint, the crux of why trade secret law is better than the CFAA [is because trade secret law] . . . strikes a balance between safeguarding business information and guaranteeing employee mobility."

Trade Secrets Act (UTSA).[23] This amendment would preserve the CFAA's utility as a means of redressing sophisticated data theft and sabotage, while preserving trade secret law's careful balance between protecting valuable confidential information and promoting employee mobility.

Part I examines the historical background of trade secret law, placing particular emphasis on the policy considerations embodied in the law. Part II examines the emergence of the CFAA in the employment context, and the resultant debate over the meaning of authorization under the CFAA. This section considers why employers have increasingly relied on the CFAA over state-level trade secret statutes, and discusses how this reliance has undercut the policy considerations of trade secret law. Part III argues that establishing a narrow reading of "authorization" under the statute will bring the CFAA closer to its original purpose while protecting the policy goals of trade secret law. Part IV proposes borrowing from trade secret law, and enacting a "reasonable efforts" amendment to the CFAA.

A reasonable efforts amendment, combined with a narrow interpretation of authorization, would preserve the CFAA as a means of addressing serious breaches of reasonable data security, while preventing employers from relying on the CFAA's civil remedies as an end run on alternative trade secret statutes. Under this approach, the CFAA would once again be rightly aimed at stopping "bright, intellectually curious, and rebellious"[24] computer hackers instead of targeting opportunistic consultants armed with USB thumb drives.[25]

I. HISTORICAL BACKGROUND OF TRADE SECRET LAW

"Since its emergence in the middle of the nineteenth century, trade secret law has developed primarily as a creature of state common law,"[26] as a way for companies to protect some of their most valuable assets from misappropriation. Because of its organic formulation, trade secret law differs significantly from many other areas of intellectual property law.[27] Where most areas of intellectual property law (such as copyright and patent law)

---

[23] Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985).

[24] 132 CONG. REC. 7816 (1986) (statement of Rep. William J. Hughes).

[25] *See* SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 704, 717 (N.D. Ill. 2009) (where defendants were charged under the CFAA for misappropriating company information by transferring files to external hard drives and USB thumb drives).

[26] Robert G. Bone, *A New Look at Trade Secret Law: Doctrine in Search of Justification*, 86 CALIF. L. REV. 241, 247 (1998).

[27] *Id.* at 244.

establish an individual "right against the world" in a given idea or expression, trade secret law "does not impose liability for mere appropriation. Rather, the appropriator must have acquired, disclosed, or used the information in a wrongful manner."[28]

Proponents of trade secret law argue that this approach adds efficiency to the marketplace in two ways.[29] First, an "incentive-based argument" posits that protecting trade secrets creates incentives for companies and individuals to continue innovating and creating new information without fear of losing it to a competitor, which is beneficial for the overall marketplace.[30] Second, by only protecting information that rises to the level of a trade secret, trade secret law promotes employee mobility, allowing employees to take knowledge and skills gained in previous jobs with them to new jobs, which is beneficial to the marketplace as a whole.[31]

This emphasis on employee mobility complements what appears to be an emerging trend in the employment context, as average tenure decreases and employees move more transiently between employers.[32] As reduced tenure with a given employer becomes more common, employees are trading the expected job security of long-term employment for the prospect of rapid skill development that comes with sporadic short-term and increasingly varied work experiences.[33] By allowing employees to freely utilize a significant amount of the knowledge and skills gained in past jobs without subjecting themselves to potential misappropriation claims by past employers,[34] trade secret law complements this structural shift in the employment context. Based on these considerations, it seems that the real efficiency in trade secret law is in the balance it strikes between protecting information where necessary on the one hand, and allowing for employee mobility on the other.

---

[28] *Id.* (footnotes omitted).

[29] *See, e.g.*, *id.* at 262.

[30] *Id.*

[31] Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 586 (1999) ("These knowledge spillovers supercharge the innovative capacity of the district with renewed agglomeration economies, facilitating the development of new technologies that create a new industrial life cycle.").

[32] *See* Katherine V.W. Stone, *The New Psychological Contract: Implications of the Changing Workplace for Labor and Employment Law*, 48 UCLA L. REV. 519, 554 (2001) ("Whereas previously, careers were understood to unfold in structured ways, by moving up job ladders in internal labor markets or along fixed lattices on organizational flow-charts, recent research on careers has found organizational fluidity.").

[33] *Id.* at 591 ("[T]he employee's right to obtain and use the knowledge is often part of the overall employment package.").

[34] Bone, *supra* note 26, at 244.

While trade secret statutes exist at the state rather than federal level, nationally promulgated guidelines set out by the Uniform Trade Secrets Act heavily inform the state-level statutes, and substantial convergence has developed around UTSA standards.[35] The UTSA defines a trade secret as:

> 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*.[36]

As the UTSA demonstrates, to be considered a trade secret, information must be reasonably protected under the circumstances.[37] This reasonable efforts provision has itself been the subject of substantial debate.[38] While scholars and jurists continue to debate what constitutes a reasonable effort to protect information in a given circumstance, the general consensus is that Congress did not intend for the UTSA to require so called "super reasonable" measures to establish secrecy.[39] A more lenient approach to what constitutes reasonable trade secret protections is largely justified in economic terms: requiring companies to

---

[35] Victoria A. Cundiff, *Reasonable Measures to Protect Trade Secrets in a Digital Environment*, 49 IDEA 359, 362 n.5 (2009) (explaining that the UTSA has been adopted as the model for state-level trade secret legislation "in 46 states and the District of Columbia").

[36] Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985) (emphasis added); *see also* Graham M. Liccardi, Note, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 158 (2008) (footnotes omitted) ("There are three essential elements to a state trade secret misappropriation claim. First, the information must qualify as a trade secret. Second, the plaintiff must have made reasonable efforts to prevent disclosure of its trade secret. Third, the plaintiff must prove that the defendant acquired the trade secret through wrongful means.").

[37] Uniform Trade Secrets Act § 1(4)(ii).

[38] *See, e.g.*, Jermaine S. Grubbs, *Give the Little Guys Equal Opportunity at Trade Secret Protection: Why the "Reasonable Efforts" Taken by Small Businesses Should be Analyzed Less Stringently*, 9 LEWIS & CLARK L. REV. 421, 425 (2005) (arguing that small businesses should have a less stringent burden for making out "reasonable efforts").

[39] Cundiff, *supra* note 35, at 363; *see also* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991) ("If trade secrets are protected only if their owners take extravagant, productivity-impairing measures to maintain their secrecy, the incentive to invest resources in discovering more efficient methods of production will be reduced, and with it the amount of invention.").

overinvest in securing trade secrets, such as creating sophisticated data protection systems, would stifle innovation.[40]

While Herculean efforts to protect data are not required, it is well-established that requiring some degree of protection furthers valuable policy goals.[41] Suppose plaintiff employer sues defendant employee for misappropriating company trade secrets. Requiring reasonably protective efforts under trade secret law provides direct evidence of the defendant employee's wrongdoing, and further suggests that the information was in fact valuable to the employer.[42] From an evidentiary perspective, having protective measures in place helps to shed light on situations where a defendant employee has wrongfully misappropriated information.[43] Put simply, when information is not reasonably protected, it is harder for a fact finder to determine whether an individual acted wrongfully in misappropriating that information. Conversely, when data is reasonably protected, it is easier to infer that the misappropriation was wrongful.[44] In terms of its utility as a proxy for the value of misappropriated information, protective measures serve as a signal to the fact finder the information is considered valuable by its owner and is therefore worthy of judicial protection.[45] As Judge Posner explains, enforcing trade secret law without requiring such reasonably protective efforts would create a meaningless distinction between unprotected information and the public domain, wherein "the plaintiff . . . would enjoy a windfall if permitted to recover damages merely because the defendant took the secret from him, rather than from the public domain as it could have done with impunity."[46] Beyond these more theoretical justifications, requiring plaintiffs to reasonably protect their information serves the very practical goal of "prevent[ing] misappropriation from occurring altogether."[47]

Trade secret misappropriation in the employment context is an undoubtedly serious economic issue for employers,[48] and has only become more widespread by the ease with which

---

[40] *See* Cundiff, *supra* note 35, at 363 (citing WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF INTELLECTUAL PROPERTY LAW 355, 369 (2003)).

[41] *See* Cundiff, *supra* note 35, at 363.

[42] *See Rockwell Graphic Sys., Inc.*, 925 F.2d at 178.

[43] *Id.*

[44] *Id.*

[45] *Id.* at 179.

[46] *Id.*

[47] Cundiff, *supra* note 35, at 363.

[48] *See* Liccardi, *supra* note 36 ("In September of 2003, Former FBI Director Robert Mueller stated that U.S. businesses are losing more than $200 billion dollars annually from theft of intellectual property.").

computing technology allows for the transfer of data.[49] The findings of a 2009 study by the Ponemon Institute, a privacy think tank, highlight the extent to which employees are misappropriating company data when they leave a job.[50] According to the study, which surveyed 945 adults who had changed jobs in some way over the past year, 59% had stolen some sort of company data before leaving their job, ranging from email lists and non-financial business information to employee records and financial information.[51] Survey respondents cited several reasons for the high levels of data theft, including the increasing mobility of employees, feelings of entitlement to the information, and the desire to leverage the information in a new job.[52] Nearly 80% of those surveyed freely admitted that they knew they were not allowed to take the information.[53]

Despite the widespread misappropriation of company data by departing employees, companies seem to be doing surprisingly little to address this problem.[54] For example, only 15% of companies surveyed made a practice of conducting electronic assessments of documents and files taken by employees upon termination, and of companies that did conduct such assessments, the majority were either superficial or incomplete.[55] Further, 24% of departing employees reported that their access to company data systems continued after termination, and in over 30% of cases, terminated employees retained access to company data systems for over a week after being terminated.[56] While many employers attempt to prohibit data theft by including relevant language in employment and non-disclosure agreements, simple steps such as ensuring that computer access is revoked upon termination, and taking stock of laptops and mobile devices issued to employees remain

---

[49] *See* Brian Krebs, *Data Theft Common by Departing Employees*, WASH. POST, Feb. 26, 2009, http://articles.washingtonpost.com/2009-02-26/news/36791861_1_data-theft-employer-job.

[50] PONEMON INST. LLC, DATA LOSS RISKS DURING DOWNSIZING: AS EMPLOYEES EXIT, SO DOES CORPORATE DATA 2 (2009), *available at* http://media.techtarget.com/Syndication/NATIONALS/Data_Loss_Risks_During_Downsizing_Feb_23_2009.pdf (last visited Oct. 13, 2013).

[51] *Id.*

[52] *Id.* at 4, 10. Respondents to the study who took data before leaving their jobs reported the most common ways to take digital files were "downloading information onto a CD or DVD[,] . . . on to a USB memory stick[, or] . . . sending documents as attachments to a personal email account." *Id.*

[53] *Id.* at 2.

[54] *See id.*

[55] *Id.*

[56] *Id.* at 4.

underutilized.[57] In an increasingly digital and virtual workplace, technological advances "present new reasons—and new ways—to implement" data protection.[58] For example, employers can now utilize sophisticated and increasingly inexpensive options such as data and email encryption, multi-level passwords, and even the ability to remotely wipe sensitive data from company-issued laptops and mobile devices.[59] While many such measures have gone overlooked,[60] employers have relied increasingly on the protections afforded by the CFAA in protecting their trade secrets.

II. EMERGENCE OF THE CFAA IN THE EMPLOYMENT CONTEXT

When Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[61] the act was relatively narrow in scope, providing criminal penalties for the unauthorized use of a computer for just three reasons:

> to obtain classified United States defense or foreign relations information with the intent . . . to harm the United States, to obtain information contained in a financial record of a financial institution[, and] to use, modify, destroy, or disclose information in, or prevent authorized use of, a computer operated for or on behalf of the United States.[62]

Just two years after the CFAA's passage, the Justice Department, frustrated with having to address emergent computer crime under outdated mail and wire fraud provisions of the criminal code, urged Congress to broaden coverage under the CFAA.[63] Congress responded in turn by "expand[ing] the scope of the Act to encompass additional significant types of computer crime."[64] Over the years, the statute "has been amended

---

[57] *Effective Practices: What Technology Issues Should an Employer Consider When Terminating an Employee?*, SOCIETY FOR HUMAN RES. MGMT. (July 13, 2012), http://www.shrm.org/TemplatesTools/hrqa/Pages/TechnologyConsiderationRelatedtoEmployeeTermination.aspx [hereinafter *Effective Practices*].

[58] Cundiff, *supra* note 35, at 364.

[59] *Id.* at 361.

[60] *Effective Practices*, *supra* note 57.

[61] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, 98 Stat. 2190 (codified as amended at 18 U.S.C. § 1030 (2012)).

[62] Griffith, *supra* note 9, at 460.

[63] Pamela Taylor, *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, 207 (2012); *see also* Shaw v. Toshiba Am. Info. Sys., Inc., 91 F. Supp. 2d 926, 930 n.6 (E.D. Tex. 1999).

[64] Griffith, *supra* note 9, at 474.

eight . . . times,"[65] with the most substantial amendments enacted in 1994 and 1996.

In 1994, as part of the Violent Crime Control and Prevention Act of 1994, Congress added a private cause of action to the statute, allowing anyone harmed by a CFAA violation to seek compensatory and injunctive relief.[66] For such a major amendment to the CFAA, there is no clear record of the congressional intent behind the decision to establish a private cause of action.[67] While the precise legislative intent may not be readily apparent, Professor Galbraith notes that "[t]he sponsors of the amendment made clear . . . that they certainly and expressly did not want to open the floodgates to frivolous litigation."[68] An onslaught of private litigation was not a real concern at the time because when the private cause of action was added, the CFAA only applied to "federal interest computers," which were defined as those computers "operated by the government or a financial institution."[69]

Galbraith points out that this dynamic changed drastically in 1996, when the statute was amended to increase the number of computers covered under the CFAA.[70] Specifically, the 1996 amendment replaced the term "federal interest computer" with the term "protected computer," and proceeded to define a protected computer as any computer previously covered under the act, as well as any computer "used in or affecting interstate or foreign commerce or communication."[71] This amendment "effectively extended the statute's reach to include any computer connected to the

---

[65] Kapitanyan, *supra* note 15, at 414.

[66] Section 1030(g) provides in part that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

[67] *See* Brenton, *supra* note 18, at 453. Because the amendment was passed as part of the Violent Crime Control and Prevention Act of 1994, which consisted of over 300 pages of legislation, the legislative history has been called challenging to review. *Id.* While the Senate Report mentions that a civil remedy will deter crime by providing aggrieved individuals with a means to obtain relief, "the language in the remainder of the report pointing to malicious computer hacking as the motivating force behind the statute further argues against a broad scope for the legislation." *Id.*

[68] Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 329 (2004) (quotation omitted).

[69] *Id.*

[70] *Id.* at 330.

[71] 18 U.S.C. § 1030(e)2(B). This definition was later expanded to include computers used outside of the United States that impacted interstate commerce. *See* United States v. Ivanov, 175 F. Supp. 2d 367, 374 (D. Conn. 2001).

Internet."[72] While the bill's sponsors made clear that the amendment was designed to increase the protection of private information stored on both government and civilian computer networks, the legislative history seems to indicate that the expansion was narrowly directed at protecting industries that were beginning to rely on computers as a central part of their technical infrastructure.[73] In any case, it is apparent that the sponsors did not foresee the sweeping reach that the amendment would ultimately create.[74]

While Congress took numerous steps to broaden the CFAA's scope, the statute's pleading standard remained relatively unchanged.[75] The result was a statute that, perhaps inadvertently, covered a wide range of activities, many of which could hardly be classified as hacking.[76] In one provision commonly invoked in private causes of actions, the CFAA imposes liability on an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[77] Another provision establishes liability when an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [over] . . . $5,000 in any 1-year period."[78] A third provision covers

---

[72] Galbraith, *supra* note 68, at 330. The legislative history of the 1996 amendment seems to suggest that the amendment's framers underestimated the pervasive rise of personal computing that would come to define the amendment's scope. S. REP. No. 104-357, at 7 (1996) ("[I]ncreasingly computer systems provide the vital backbone to many other industries, such as transportation, power supply systems, and telecommunications.").

[73] *See* S. REP. No. 104-357, at 7 (1996).

[74] Galbraith, *supra* note 68, at 331 ("Noticeably absent from the legislative history . . . is any suggestion that Congress intended to widen dramatically the protection of the CFAA to include all information and all computer systems on the Internet, such as non-copyrightable data contained on publicly accessible websites.").

[75] In fact, all eight amendments to the CFAA since 1986 have only served to expand the act "by adding substantive offenses, lowering levels of scienter, or increasing penalties." Kapitanyan, *supra* note 15, at 415. Further, because the amendments have continued to expand coverage under the CFAA, some courts have elected to interpret ambiguity in the statute in favor of an expansive reading. *See, e.g.*, United States v. Middleton, 231 F.3d 1207, 1211 (9th Cir. 2000).

[76] *See, e.g.*, United States v. Rodriguez, 628 F.3d 1258, 1261, 1263 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (U.S. 2011) (Social Security Administration employee charged under the CFAA for using his SSA computer access to obtain information related to women he was romantically interested in).

[77] 18 U.S.C. § 1030(a)2(C) (2012). *See* Kapitanyan, *supra* note 15, at 416 n.60 (quotation omitted).

[78] 18 U.S.C. § 1030(a)4.

individuals who intentionally cause damage to a protected computer by "transmission of a program [or] code."[79]

After establishing one of these substantive offenses, the CFAA allows a private party to obtain compensatory and injunctive relief after showing the existence of one of five factors, including "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[80] Courts have read "loss" here as encompassing both "(1) the loss in value of trade secrets . . . and confidential information that was not previously known to the public, and (2) the loss of competitive advantage."[81]

As a result of the CFAA's expanded scope and straightforward pleading requirements, the "floodgates to frivolous litigation"[82] feared by the sponsors of the 1994 amendment were inevitably burst open. In fact, "[s]ince 2002, complaints alleging a cause of action under the CFAA have increased nearly 600[] percent."[83] A far cry from the "bright, intellectually curious, and rebellious youth"[84] described by Congressman Hughes in 1986, many defendants in recent CFAA litigation know little more about computers than how to send an email, operate a USB flash drive, or set up a Myspace profile.[85]

While trade secret statutes have existed for years at the state level,[86] the expanded CFAA arguably created a second basis for liability for trade secret misappropriation claims so long as a computer was involved.[87] Where such claims would

---

[79] *Id.* § 1030(a)5(A); *see* Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006).

[80] 18 U.S.C. § 1030(c)(4)(A)(i)(I). "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in §§ (I), (II), (III), (IV), or (V) of § (c)(4)(A)(i)." *Id.* § 1030(g) (footnote omitted).

[81] *See e.g.* C.H. Robinson Worldwide, Inc. v. Command Transp., LLC, No. 05 Civ. 3401, 2005 WL 3077998, at *3 (N.D. Ill. Nov. 16, 2005).

[82] Galbraith, *supra* note 68, at 329 (quotation omitted).

[83] Sebastian E. Kaplan, *The Rise of the Computer Fraud and Abuse Case*, FENWICK & WEST LLP 1 (2012), http://www.fenwick.com/fenwickdocuments/2012-03-20_rise_computer_fraud_abuse_case.pdf.

[84] 132 CONG. REC. 7816 (1986) (statement of Rep. William J. Hughes).

[85] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009) (complaint based on emailing documents from a work account to a personal email address, as well as accessing a website using a username and password furnished by the employer); United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (criminal prosecution based on setting up a fake Myspace profile in violation of the website's terms of service); SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 704 (N.D. Ill. 2009) (complaint based on data saved to USB thumb drives); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123 (W.D. Wash. 2000) (complaint based on emailing documents from work email to defendant employer).

[86] Bone, *supra* note 26, at 247.

[87] Brenton, *supra* note 18, at 430.

otherwise be raised at the state level, likely under a UTSA-inspired statute, the CFAA offers employers a number of benefits over the state-level trade secret statutes.

First, the CFAA offers substantially simpler pleading requirements compared to equivalent state-level trade secret law.[88] While trade secret law focuses on whether the material taken rises to the level of a trade secret and whether the plaintiff took reasonable efforts in protecting the information,[89] the CFAA "puts no qualification on the nature or character of the information taken—it focuses squarely and solely on the actions of the defendant in obtaining it."[90] In other words, where trade secret law requires a plaintiff to establish (1) the existence of a trade secret, (2) reasonable protective efforts, and (3) wrongful misappropriation, the CFAA focuses only on the third element, whether the misappropriation was wrongful.[91]

In addition to its simpler pleading requirements, the CFAA "provides [plaintiffs with] a basis for federal jurisdiction."[92] By bringing a CFAA claim, employers may bring suit against the defendant's new employer as well as the individual, and also seek injunctive relief, elements not widely available under the UTSA-influenced state laws.[93] Further, the CFAA allows employers to effectively enforce non-compete agreements that would be otherwise unenforceable under state law in cases where former employees use misappropriated information to compete in a new position.[94] And because of supplemental jurisdiction under 28 U.S.C. § 1367(a), bringing a CFAA claim in federal court does not preclude employer plaintiffs from raising state trade secret claims.[95] In some cases, employers have recovered

---

[88] For example, a typical state claim for trade secret misappropriation under the UTSA requires the plaintiff to show that the misappropriated information was secret, that the plaintiff derived economic value from its secrecy, and that reasonable efforts were made to maintain the information's secrecy. *See* Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985). Under the CFAA, a plaintiff is not required to establish any of these elements.

[89] Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985).

[90] Brenton, *supra* note 18, at 434.

[91] Liccardi, *supra* note 36, at 158.

[92] Kapitanyan, *supra* note 15, at 418.

[93] *Id.*

[94] Peter J. Pizzi, *Disloyal Employees: Computer Abuse Law Turns on Meaning of "Without Authorization*," N.Y. L.J., Sept. 5, 2006, at 5, *available at* http://www.connellfoley.com/sites/default/files/pjp_nylj_disloyal_employees_0.pdf.

[95] 28 U.S.C. § 1367(a) (2011) ("[I]n any civil action of which the district courts have original jurisdiction, the district courts shall have supplemental jurisdiction over all other claims that are so related to claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution."). In fact, courts may continue to exercise supplemental jurisdiction over pendent state claims after dismissing the underlying federal claim. *See, e.g.*, Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., No. 10 Civ. 450, 2013 WL

damages under both state-level trade secret and CFAA provisions in the same action.[96]

While the expanding amendments to the CFAA opened the doors to private litigation in 1996, it was not until 2000 that employers began to realize the CFAA's utility in the trade secret context.[97] That year, the U.S. District Court for the Western District of Washington held in *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* that the revamped CFAA could apply to a "rogue employee."[98]

In *Shurgard*, the plaintiff, Shurgard Storage Centers, Inc., had been an "industry leader" in the development and maintenance of self-storage facilities in the United States and abroad for over 25 years.[99] In a market with a high barrier to entry, Shurgard created "a sophisticated system" to determine potential storage facility sites, markets, and strategies.[100] The defendant, Safeguard Self Storage, Inc., was a direct competitor of Shurgard, and relatively new to the industry, having entered the market just three years before the suit.[101] Shurgard alleged in its complaint that Safeguard had offered a job to Eric Leland, a regional development manager with Shurgard, who was entrusted with access to a wide array of Shurgard's business and marketing information.[102] The complaint alleged that before leaving Shurgard to work for Safeguard, Leland "sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff."[103] The complaint further alleged that Leland continued to share propriety information with Safeguard after leaving Shurgard, and that Safeguard continued to target other Shurgard employees based on their intimate knowledge of Shurgard's business and marketing plans.[104]

In denying Safeguard's motion to dismiss, the District Court upheld the plaintiff's CFAA claim by finding that

---

4498993, at *1 (W.D. Mich. Aug. 19, 2013) (issuing an opinion on purely state claims after dismissing the underlying CFAA claim last year).

[96] *See e.g.* Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004) (plaintiff "awarded $150,000 on each of three" violations under the CFAA and an additional $60,000 for violations of the Idaho Trade Secrets Act).

[97] Kapitanyan, *supra* note 15, at 418.

[98] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1128 (W.D. Wash. 2000).

[99] *Id.* at 1122.

[100] *Id.* at 1123.

[101] *Id.*

[102] *Id.*

[103] *Id.*

[104] *Id.*

Leland's emails to defendant Safeguard were sent "without authorization," despite the fact that Leland had been employed by Shurgard and had full access to the information in question at the time of the transfer.[105] To reach that conclusion, the court applied concepts of general agency law to the employee's computer usage.[106] Specifically, the court relied on § 112 of the *Restatement (Second) of Agency*, which states that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[107] Applying this rule to the facts of the case, the court found that the employee's authorization terminated the moment the employee "obtained and sent the proprietary information to the defendant via e-mail."[108] The court went on to uphold the other two claims asserted under the CFAA,[109] but it was this broad, agency-based interpretation of authorization that seemed to open the door to future claims by employers under the CFAA.[110] Following the court's decision in *Shurgard*, employers quickly realized that the CFAA provided a favorable alternative to state-level trade secret claims, and private actions alleging claims under the CFAA began to increase sharply.[111]

A. The Debate over Authorization in the CFAA

As private CFAA complaints increase in the employment and trade secret contexts, courts continue to struggle with the concept of authorization, which appears to be

---

[105] *Id.* at 1124, 1129.

[106] *Id.* at 1125.

[107] *Id.* (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

[108] *Id.* In so doing, the court relied on a formulation of authorization that far pre-dated the invention of the computer. The opinion makes no attempt to show that the CFAA's drafters intended authorization to be defined in terms of agency law rather than in a technological sense. *Id.*

[109] *Id.* at 1126-27. The court held that Safeguard had established a claim under § 1030(a)(4), which covers an individual who "'knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value [over $5,000].'" *Id.* at 1125 (quoting 18 U.S.C. § 1030(a)(4) (2012)). The court also found that Safeguard had established a claim under § 1030(a)(5)(C), which creates liability for any individual who "'intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.'" *Id.* at 1126 (quoting 18 U.S.C. § 1030(a)(5)(C)).

[110] Kapitanyan, *supra* note 15, at 423 ("Although *Shurgard* was the first case of its kind, it certainly has not been the only attempt to offer a viable interpretation of the elusive concept.").

[111] Kaplan, *supra* note 83, at 1 ("Since 2002, complaints alleging a cause of action under the CFAA have increased nearly 600%[.]").

the only provision potentially limiting the CFAA's broad scope. The authorization requirement found in many of the CFAA's substantive sections provides that someone is only liable under the CFAA if he or she "... accessed a computer without authorization or exceeds authorized access."[112] Thus, whether an employee is authorized, or whether an employee has exceeded his or her authorized access has in many cases determined the success or failure of a CFAA claim.[113] To complicate the issue, the CFAA fails to provide a definition of the term "authorization" as it relates to the statute,[114] and it only provides a definition for the term "exceeds authorized access," leaving courts to interpret the phrase "without authorization."[115] The CFAA defines "exceeds authorized access" 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."[116]

While a plain reading suggests that "exceeds authorized access" was intended to cover employees who misappropriate information from their current job, a number of courts have instead applied the term "without authorization" to current employees by adopting an agency-based approach to authorization.[117] To reach this conclusion, some courts have argued that under principles of agency law, authorization to access a computer terminates at the moment an employee breaches a duty of loyalty to his or her employer.[118]

Other courts have rejected this broad agency interpretation.[119] These courts have held that because the CFAA is primarily a criminal statute, ambiguous terms should be decided in favor of lenity.[120] Under this approach, if a term is unclear, it should be interpreted in favor of the defendant and against the government.[121] Thus, the argument runs, it is improper to hold that someone who has been granted permission to access to a computer system can access the computer without authorization, because authorization begins and ends with the

---

[112] Specifically, 18 U.S.C. § 1030(a)(1), (2), (4), & (5)(B)–(C) all contain similar language related to authorization.

[113] *Compare* Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006), *with* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009).

[114] *Brekka*, 581 F.3d at 1132.

[115] 18 U.S.C § 1030(e)(6).

[116] *Id.* (quotations omitted).

[117] *See Citrin*, 440 F.3d at 420; *Shurgard*, 119 F. Supp. 2d at 1125.

[118] *Citrin*, 440 F.3d at 420-21.

[119] *See Brekka*, 581 F.3d at 1133.

[120] *Id.* at 1134 (citing United States v. Carr, 513 F.3d 1164, 1168 (9th Cir. 2008)).

[121] *Id.*

employer's granting and rescinding access.[122] As private litigants continue to test the outward boundaries of the CFAA's applicability in the employment context, these contrasting interpretations have resulted in a sizable and developing circuit split that has garnered much attention.[123]

While first articulated in *Shurgard*,[124] the agency-based approach to authorization under the CFAA gained prominence in *International Airport Centers, L.L.C. v. Citrin*,[125] which was at the time considered "the primary appellate interpretation of the authorization language in the CFAA."[126] Jacob Citrin was an employee of International Airport Centers (IAC), tasked with investigating real estate properties that IAC was interested in buying.[127] After working at IAC for eight years, Citrin decided to quit his job and compete directly with his former employer.[128] According to the facts alleged by IAC, Citrin "fraudulently misappropriated" a host of IAC information including confidential information and work product,[129] before deleting all of the files on his laptop using a "secure-erasure program" to prevent any recovery of the deleted files.[130] IAC sued Citrin under a number of CFAA provisions, including § 1030(a)(5)(B), which establishes liability against any individual who "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage."[131]

In reversing the district court's dismissal of IAC's suit, Judge Posner, writing for the Seventh Circuit Court of Appeals, determined that despite the fact that Citrin was employed by IAC at the time he accessed the computer, his access was nonetheless "without authorization."[132] To reach this conclusion,

---

[122] *Id.* at 1135.

[123] *See, e.g.*, Audra A. Dial & John M. Moye, *Fourth Circuit Widens Split Over CFAA and Employees Violating Computer Use Restrictions*, KILPATRICK TOWNSEND (Sept. 10, 2012), http://www.martindale.com/members/Article_Atachment.aspx?od=305497&id=1585568&filename=asr-1585570.CFAA.pdf.

[124] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

[125] Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

[126] Amber L. Leaders, *Gimme A Brekka!: Deciphering "Authorization" Under the CFAA and How Employers Can Protect Their Data*, 6 WASH. J.L. TECH. & ARTS 285, 289 (2011).

[127] *Citrin*, 440 F.3d at 419.

[128] *Id; see also* Brief for Respondent, Citrin, 440 F.3d 418 (No. 06-2073), 2006 WL 1354181, at *2.

[129] Int'l Airport Centers LLC v. Citrin, 2005 WL 241463, at *1 (N.D. Ill. Jan. 31, 2005).

[130] *Citrin*, 440 F.3d at 419.

[131] 18 U.S.C § 1030(a)(5)(B) (2012).

[132] *Citrin*, 440 F.3d at 420.

Judge Posner employed the agency approach introduced in *Shurgard*[133] and determined that Citrin's authorization had ended the very moment he decided he would delete the incriminating files from his work computer.[134] Posner reasoned that Citrin's "authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files . . . in violation of the duty of loyalty that agency law imposes on an employee."[135]

While *Citrin* is one of the most notable examples of the agency-based approach to authorization under the CFAA,[136] a number of courts have followed the Seventh Circuit's lead and adopted a broad reading of authorization. In *United States v. John*, the Fifth Circuit found that even where an employee has full access to a computer system, he or she can still act without authorization because authorization under the CFAA encompasses "*the use* of information obtained by permitted access to a computer system and data available on that system."[137] In *United States v. Rodriguez*, the Eleventh Circuit held that an employee of the Social Security Administration with full permission to view sensitive personal information on SSA computers, but who accessed that information in romantic pursuit of a number of women in his church study group, likewise violated the CFAA because his computer use violated a written SSA policy.[138]

Some commentators have leveled a number of similar but distinct criticisms at the broad, agency-based approach to authorization under the CFAA. Perhaps the most common criticism of the agency approach is that such an interpretation almost certainly reaches more employee conduct than legislatively intended.[139] For example, under the agency approach, one could argue that "[a]n employee who checks their personal email at work, in violation of company policy, would be a criminal."[140] Finding no clear support in the legislative record, this

---

[133] *See supra* Part II, explaining the *Shurgard* court's reliance on the *Restatement (Second) of Agency* to interpret the phrase "without authorization."

[134] *Citrin*, 440 F.3d at 420.

[135] *Id.*

[136] Leaders, *supra* note 126, at 289.

[137] United States v. John, 597 F.3d 263, 271 (5th Cir. 2010).

[138] United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (2011).

[139] Kaplan, *supra* note 83, at 1.

[140] David J. Rosen, *Limiting Employee Liability Under the CFAA: A Code-Based Approach to "Exceeds Authorized Access"*, BERKELEY TECH. L.J. 737, 750 (2012) (quoting Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1586-86 (2010)).

broad scope is only compounded by the probability that the vast majority of employees remain unaware that such a wide range of their workplace conduct could lead to civil and even criminal liability. The "agency approach 'gives employees insufficient notice of what line distinguishes computer use that is allowed from computer use that is prohibited.'"[141] This lack of clarity is particularly troubling in an increasingly fluid workplace, where employees switch jobs with greater frequency, and seek to bring their skills and experience with them.[142] Further, the line between personal and work-based computing is constantly blurring, which can lead employees to take unlawful action that they do not have any reason to believe is unlawful.[143]

Another common argument leveled against the agency approach is one of statutory construction:

> [T]he agency approach, if applied to the text of §§ 1030(a)(2) and (a)(4), would collapse the distinction between "without authorization" and "exceeds authorized access." If an employee's authorization to access a computer ceases as soon as she does something that is not in her employer's interests, then "exceeds authorized access" likely becomes textually superfluous and meaningless.[144]

Put differently, arguing that an employee acts "without authorization" as soon as the employee acts contrary to his or her employer's interests would render the "exceeds authorized access" provision absurd. Under this reading an employee could only "exceed[] authorized access" by wrongfully misappropriating data while continuing to maintain an appropriate agent-principal relationship. Because such misappropriation would have to be aligned with the employer's interests, it seems impossible for an employer to successfully claim injury under this provision.[145]

---

[141] *Id.* (quoting Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1586 (2010)).

[142] *See generally* KATHERINE V. W. STONE, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATION FOR THE CHANGING WORKPLACE 74-83 (2004); *see also* Krebs, *supra* note 49.

[143] "[M]ore employees are storing their business and customer contacts online at services like LinkedIn.com, some employees may not believe they are doing anything wrong when they take customer lists and other internal company data when they move on to a new job." Krebs, *supra* note 49.

[144] Rosen, *supra* note 140, at 751 (footnotes omitted).

[145] An online commenter attempts to provide a hypothetical fulfilling such a definition of "exceeds authorized access":

> Scenario: Boss asks employee to print out his schedule for the coming week. Employee, without asking Boss, uses Boss' CPU to print it from the cloud. In the process of printing it out, Employee also sends the pre-meeting notes from the same file to the printer in her office. Employee then faxes the pre-meeting notes to a competitor who sends her $6k.

While this broad view of authorization still has firm support in some circuits, "[a] growing number of cases are adopting the narrow view."[146]

On the other side of the circuit split is a narrower interpretation of authorization, "holding that the CFAA prohibits improper 'access' of computer information, rather than misuse or misappropriation of such information."[147] Under this narrow view, also called the "[p]lain [l]anguage [i]nterpretation,"[148] "[a]uthorization begins and ends with the employer, not the employee . . . . An employee acts without authorization only if the employer never gives permission or affirmatively rescinds permission."[149] The Ninth Circuit's decision in *LVRC Holdings, LLC v. Brekka* is considered the leading view on the narrow interpretation of CFAA authorization.[150]

Joseph Brekka was hired by LVRC, a residential addiction treatment center, to oversee various operations within the facility, including marketing programs.[151] "At the time [he] was hired [by LVRC], Brekka owned and operated" two consulting businesses that used internet marketing to connect patients with addiction care facilities.[152] While working for LVRC and continuing to run his own businesses, Brekka emailed a number of documents related to his work for LVRC to his personal email account.[153] In addition, after resigning from LVRC, Brekka continued to use login credentials issued to him by LVRC to access a system which provided internet traffic statistics relating to LVRC's website.[154] Upon learning of the emails Brekka sent to his personal account and the continued access to the internet traffic site, LVRC brought a federal action under the CFAA. LVRC alleged that Brekka's conduct violated two provisions of the CFAA,[155] both of which require

---

Not legal advice. Don't rely., Comment to *Recent Developments—Both in the Courts and in Congress—on the Scope of the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), http://www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act/.

146 Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., No. 10 Civ. 450, 2012 WL 2524008, at *4 (W.D. Mich. June 29, 2012).

147 *Id.* at *3.

148 Leaders, *supra* note 126, at 290.

149 *Id.* at 291.

150 *Id.*

151 LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

152 *Id.*

153 *Id.* at 1129-30.

154 *Id.* at 1130.

155 Section 1030(a)(2) provides for relief against any individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C.

that the individual either acted "without authorization," or "exceed[ed] authorized access."[156] In upholding the district court's motion to dismiss the claim, the Ninth Circuit rejected the agency reading of authorization, noting that "[n]o language in the CFAA supports [the] argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest."[157] Instead the court defined authorization "as taking [its] ordinary, contemporary, common meaning."[158] Under this interpretation, the fact that LVRC had given permission to use the computer meant that Brekka had authorization at the time of access, and thus there was no cause of action under the CFAA.[159]

A number of courts have agreed with the reasoning set forth in *Brekka*, adopting a narrow, "plain language" interpretation of authorization under the CFAA.[160] Most recently, the Fourth Circuit, in *WEC Carolina Energy Solutions, LLC v. Miller*, joined the Ninth Circuit's narrow interpretation.[161] In *WEC*, the plaintiff alleged that Mike Miller, a former WEC employee who began working for a direct competitor, had emailed a number of proprietary WEC documents to himself before quitting, and had subsequently used those documents in a presentation given to a potential client on behalf of his new employer.[162] The court held that WEC's policy prohibiting employees from downloading proprietary information to personal computers did not constitute a revocation of authorization, and while the information may have been misappropriated, it did not occur via unauthorized access.[163] While support is not as clear at the circuit level, a number of district courts have signaled their support for a narrow reading.[164]

---

§ 1030(a)(2)(C) (2012). Section 1030(a)(4) provides for relief against any individual who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value." 18 U.S.C. § 1030(a)(4).

156 18 U.S.C. § 1030(a)(2), (4); *Brekka*, 581 F.3d at 1131.

157 *Brekka*, 581 F.3d at 1133.

158 *Id.* at 1132 (quoting Perrin v. United States, 444 U.S. 37, 42 (1979)).

159 *Id.* at 1137.

160 *See* Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., No. 10 Civ. 450, 2012 WL 2524008, at *3-4 (W.D. Mich. June 29, 2012); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010).

161 WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 203 (4th Cir. 2012); *see also* Nicholas J. Wagoner, *4th Circuit Deepens Division Over Scope of Computer Fraud and Abuse Act*, CIRCUIT SPLITS (Aug. 2, 2012), http://www.circuitsplits.com/2012/08/4th-circuit-deepens-division-over-scope-of-computer-fraud-abuse-act.html.

162 *Miller*, 687 F.3d at 201-02.

163 *Id.* at 207.

164 *See Dana Ltd.*, 2012 WL 2524008, at *5; *Orbit One Commc'ns, Inc.*, 692 F. Supp. 2d at 386.

For example, the court in *Dana Limited v. American Axle and Manufacturing Holdings, Inc.* in Michigan's Western District, indicated that the Sixth Circuit is likely to rely on the Ninth Circuit's reasoning and adopt the narrow interpretation of authorization.[165] In *Orbit One Communications, Inc. v. Numerex Corp.*, the District Court for the Southern District of New York indicated that the Second Circuit is likely to join in adopting a narrow interpretation.[166] In addition to support from the district courts, the Ninth Circuit recently reaffirmed its prior rule in *United States v. Nosal*, in which a former employee of an executive search firm convinced a number of former colleagues to help him start a competing firm by "us[ing] their log-in credentials to download source lists, names and contact information from a confidential database on the company's computer."[167]

B. Legislative Proposals to Amend the CFAA

In addition to increasing jurisprudential support, it seems that a narrow interpretation of authorization may be gaining favor with legislators, albeit slowly.[168] Senator Patrick Leahy proposed an amendment to the CFAA as part of the Cybersecurity Act of 2012 that would enhance the CFAA's penalties, while officially adopting a narrow view of authorization.[169] Specifically, the amendment would alter § 1030(e)6, to provide that 'without authorization'

> does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer, if such violation constitutes the sole basis

---

[165] *Dana Ltd.*, 2012 WL 2524008, at *4-5.

[166] *Orbit One Commc'ns, Inc.*, 692 F. Supp. 2d at 386.

[167] United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012).

[168] *See* Orin Kerr, *Recent Developments—Both in the Courts and in Congress—on the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), http://www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act/; *see also* Tony Romm, *After Activist Aaron Swartz's Death, a Tough Slog for Aaron's Law*, POLITICO (Feb. 8, 2013, 4:48 AM), http://www.politico.com/story/2013/02/activist-aaron-swartz-death-aarons-law-87332.html (explaining that legislative efforts to narrow the CFAA are at "the beginning of a new and lengthy political journey.").

[169] Cyber Crime Protection Security Act, S.3414, 112th Cong. § 8 (proposed amendment, 2012), *available at* http://www.lawfareblog.com/wp-content/uploads/2012/07/Leahy-Cybercrime-Amendment-to-S3414JEN12557.pdf.

> for determining that access to a protected computer is unauthorized.[170]

Essentially, the amendment would preclude the agency interpretation by providing that a breach of an agreement such as a computer use policy cannot, by itself, establish liability under the CFAA. Not surprisingly, the Department of Justice voiced support for the stricter penalties proposed by the amendment, while opposing the narrowed scope.[171]

While the Senate voted down the Cybersecurity Act, Leahy's amendment was revived in early 2013, following the suicide of Aaron Swartz, a computer programmer and internet activist who had been indicted two years earlier under the CFAA for attempting to download and distribute a vast portion of JSTOR's academic research database.[172] Following Swartz's death, Congresswoman Zoe Lofgren introduced a legislative amendment to the CFAA dubbed "Aaron's Law," that essentially mirrored the Leahy amendment.[173] It would amend the CFAA to establish that "unauthorized access does not include access in violation of an agreement or contractual obligation, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or employer."[174] Despite apparent widespread public support for the narrowing language included in Aaron's Law, the language was notably absent from draft changes to the CFAA distributed to the House Judiciary Committee in 2013.[175] In fact, the amended language

---

[170] *Id.*

[171] Greg Nojeim & Jake Laperruque, *Why Fibbing About Your Age is Relevant to the Cybersecurity Bill*, CTR. DEMOCRACY & TECH. (July 30, 2012), https://www.cdt.org/blogs/greg-nojeim/3007why-fibbing-about-your-age-relevant-cybersecurity-bill; *see also* Kerr, *supra* note 168.

[172] Timothy B. Lee, *"Aaron's Law, Congressional investigation in wake of Swartz suicide*, ARS TECHNICA (Jan. 16, 2013), http://arstechnica.com/tech-policy/2013/01/aarons-law-congressional-investigation-in-wake-of-swartz-suicide/.

[173] In fact, the language of the two amendments are almost completely identical, save for a few stylistic changes. *See* Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (introduced by R. Zoe Lofgren), *available at* http://www.lofgren.house.gov/images/user_images/gt/stories/pdf/aarons%20law%20-%20lofgren%20-%20061913.pdf.

[174] Lee, *supra* note 172 (internal quotation omitted). Perhaps reflecting the lack of legislative understanding of the CFAA, "Aaron's Law" would not have had any impact on Swartz's conviction under the CFAA, as Swartz would have been equally liable under the narrow view of authorization which the amendment would have established. Andy Greenberg, *"Aaron's Law" Suggests Reforms to Computer Fraud Act (But Not Enough to Have Protected Aaron Swartz),* FORBES (Jan. 16, 2013, 8:58 AM), http://www.forbes.com/sites/andygreenberg/2013/01/16/aarons-law-suggests-reforms-to-hacking-acts-but-not-enough-to-have-protected-aaron-swartz/.

[175] *See* H.R., 113th Cong. (2013), *available at* http://www.scribd.com/doc/132249133/House-Judiciary-Committee-discussion-draft (a discussion draft concerning changes distributed to House Judiciary Committee).

before the House Judiciary Committee would actually expand the CFAA's scope by increasing maximum penalties and punishing attempted CFAA violations as seriously as actual offenses.[176] Thus, while narrowing the CFAA's authorization language may be gaining popular support, it seems that legislative action is still far off.[177]

C. The CFAA's Impact on Policy Goals of Trade Secret Law

Considering the rise of the CFAA in the trade secret and employment context against the backdrop of substantive trade secret legislation, it is apparent that the CFAA undercuts several of the goals advanced by trade secret law.[178] As discussed, trade secret law strikes an important "balance between safeguarding business information and guaranteeing employee mobility."[179] This balance results from the emphasis that trade secret law places on the character of misappropriated data. While it is important for companies to protect sufficiently valuable information, it is equally important that employees be allowed to bring their skills and experiences with them to new jobs.[180]

By ignoring the character of the information misappropriated, the CFAA disrupts this balance, eroding both the evidentiary and value-identifying purposes furthered by the Uniform Trade Secrets Act requirement of reasonably protective measures.[181] For the courts, the fact that a defendant has to overcome reasonably protective measures to misappropriate a trade secret serves a strong evidentiary function, indicating that the misappropriation was indeed wrongful.[182] Further, the protections serve to put both the court, as well as the defendant, on notice that the information at issue was valuable to the employer and that a judicial remedy is therefore appropriate.[183] In contrast, the CFAA offers no such protection, and does not

---

[176] *See id.*; *see also* Orin Kerr, *House Judiciary Committee New Draft Bill on Cybersecurity is Mostly DOJ's Proposed Language from 2011*, VOLOKH CONSPIRACY (Mar. 25, 2013, 5:30 PM), http://www.volokh.com/2013/03/25/house-judiciary-committee-new-draft-bill-on-cybersecurity-is-mostly-dojs-proposed-language-from-2011/.

[177] *See* Orin Kerr, *The Prospects for Reform of the Computer Fraud and Abuse Act*, VOLOKH CONSPIRACY (Feb. 9, 2013, 6:38 PM), http://www.volokh.com/2013/02/09/the-prospects-for-reform-of-the-computer-fraud-and-abuse-act/.

[178] *See* Brenton, *supra* note 18, at 447.

[179] *Id.* at 449.

[180] *Id.*

[181] *See supra* Part II (discussing the theoretical goals furthered by requiring reasonable protective efforts in trade secret law).

[182] *See supra* Part II.

[183] *See supra* Part II.

require anything that would put an employee on notice that such information is secretive and worth protecting. It could be argued that the CFAA's authorization provision sufficiently puts an employee on notice as to whether information is fair game or not. However, this argument fails under the broad agency-based definition of authorization under the CFAA adopted by some courts, under which an employee's actions, rather than an employer's restrictions on access determine whether the employee acts without authorization.[184]

Beyond eroding the theoretical policy considerations of trade secret law, the CFAA's lack of a reasonably protective measures requirement may discourage employers from adequately investing in data protection, which is economically inefficient.[185] In the Ponemon Institute's 2009 study gauging CEO, COO, and CFO attitudes toward investment in data protection, executives pointed to many benefits of investing in data protection beyond reducing the risk of data loss or theft.[186] Executives noted that investment in such protection also resulted in increased customer trust, decreased "customer churn," reduced risk of penalty under e-discovery laws and other regulations, and "reduc[ed] . . . operational inefficiencies by creating more efficient uses of data."[187] The study further suggested a "very healthy [return on investment] for such data protection systems."[188]

In addition to the general success and secondary benefits created by effective data protection programs, there remains the very practical and obvious consideration that data protection will prevent misappropriation in the first place.[189] By preventing data theft through simple security investments, employers save the cost of litigating preventable disputes, and society benefits by reducing the load placed on an already overburdened federal court system.[190] Despite the widespread benefits and availability of effective data protection systems, the CFAA in its current form includes no requirement that an employer take even marginal

---

[184] *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010), *cert. denied*, 131 S. Ct. 2166 (2011); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

[185] *See* PONEMON INST. LLC, *supra* note 50, at 14.

[186] *Id.* at 4-5.

[187] *Id.* at 3.

[188] *Id.*

[189] Cundiff, *supra* note 35, at 363.

[190] *See, e.g.*, Press Release, Diane Feinstein Senate Office, *Senator Feinstein Introduces Legislation to Reduce Caseload in Overburdened Federal Courts* (May 17, 2011), http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=ff6add36-5056-8059-7638-184ec11315cd.

efforts to protect its data in order to make out a claim, allowing it to serve as an end run on trade secret law.

III. POLICY REASONS FOR ESTABLISHING A NARROW READING OF AUTHORIZATION

A formal legislative or judicial adoption of the narrow interpretation of authorization, as laid out in *Brekka*, would prevent the CFAA from undercutting trade secret law. By requiring that an employee do more than simply violate an employer's acceptable use policy to exceed authorized access, proposals such as Leahy's amendment and "Aaron's Law" would functionally establish a rudimentary reasonable efforts requirement in the CFAA.[191] By requiring that a defendant have breached some form of protection beyond a written computer use policy effectively means that to bring a claim under the CFAA, employers would have to restrict computer access beyond merely instituting a written computer use policy. This requirement could serve, at least in part, the evidentiary purpose of requiring reasonably protective efforts.[192] When an employee misappropriates information in violation of only a computer use policy, such a violation carries little, if any, evidentiary value in demonstrating to the fact finder that the employee's actions were wrongful.

By requiring the breach of a computer use policy along with the breach of some other form of protection, Leahy's proposed amendment would demonstrate to fact finders, at least to some degree, that the misappropriation might have been wrongful.[193] Requiring more than a breach of an employer's computer use policy would also serve to more effectively put employees on notice as to when their conduct is wrongful and potentially illegal. Conceding that the amendment would be helpful in an evidentiary sense, it likewise presents a vagueness that could quickly become a source of judicial disagreement: while the breach of a computer use policy cannot be the *sole* basis for finding a lack of authorization,[194] what protection would be sufficient? Limiting physical access to a computer system would almost certainly be enough, but courts could also find

---

[191] *See* Uniform Trade Secrets Act § 1(4)(ii) (1985).

[192] *See* Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 178 (7th Cir. 1991).

[193] Cyber Crime Protection Security Act, S. 3414, 112th Cong. § 8 (proposed amendment, 2012), *available at* http://www.lawfareblog.com/wp-content/uploads/2012/07/Leahy-Cybercrime-Amendment-to-S3414JEN12557.pdf.

[194] *Id.*

that the breach of a computer use policy, along with the breach of some other policy, such as a confidentiality agreement or non-compete agreement, is sufficient. This limiting provision would be helpful, but could create a new type of confusion in computer use jurisprudence.

IV. A "REASONABLE EFFORTS" AMENDMENT TO THE CFAA

Establishing a narrow reading of authorization would be a step in the right direction, but does not go far enough to prevent the CFAA from undermining the policy goals of trade secret law. This is primarily because, even under a narrow view of authorization, the CFAA is still only concerned with the nature of the misappropriation, and fails to consider the character of the information misappropriated.[195] Where trade secret law distinguishes between that information which merits protection and that information which does not, the CFAA, under either a broad or narrow reading, makes no such distinction.[196] But it is this very distinction that, in trade secret law, preserves the balance between employee mobility on the one hand (by declining to protect some information), and encouraging innovation on the other (by protecting information that merits such protection).[197]

Even under a narrow reading of authorization, an employer could still bring a CFAA claim over misappropriated data regardless of whether that data merited the protection it received.[198] Further, while narrowing the CFAA's scope may mirror the evidentiary benefits of reasonable effort provisions in trade secret law, a narrowed CFAA serves none of the value identifying functions performed by reasonable efforts in trade secret law.[199] By not requiring information to be reasonably protected to make out a claim, the CFAA does nothing to signal to either courts or employees that a particular file or document is so valued by an employer that it merits special protection. By focusing only on authorization to access the information in the first place, the CFAA establishes one broad level of protection

---

[195] Brenton, *supra* note 18, at 434.

[196] *See* § 1030(a)(2)(C) (providing liability for anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer").

[197] *See* Bone, *supra* note 26, at 262.

[198] For example, even under a narrow interpretation, an employee would be liable for downloading non-secret marketing materials or client lists if the materials were downloaded from a network which the employee did not have permission to access.

[199] *See Rockwell Graphic Sys., Inc.*, 925 F.2d at 179.

for all information contained on a given computer system, regardless of whether that information is private or public, valuable or worthless.[200] Lastly, by failing to consider the character of the information misappropriated, a narrowly interpreted CFAA perpetuates an inefficient labor market, where employees are unsure what information they may take with them to new positions, and what information belongs to their employer.[201] While narrowing the scope of the CFAA by legislative amendment is certainly a step in the right direction, even a narrowly interpreted CFAA threatens to erode the careful policy considerations behind trade secret law.

Amending the CFAA to include a requirement that misappropriated information must have been subject to reasonably protective measures would eliminate most, if not all, concerns that the CFAA impinges too greatly on trade secret law. Specifically, Congress should amend the CFAA's authorization provision such that it applies to anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer, provided that such information is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[202]

By amending this provision, the CFAA would more closely mirror the substantive pleading requirements of trade secret law,[203] lowering the incentive for employers to favor the CFAA over state-level trade secret statutes. Such an amendment would uphold the balance established by trade secret law between protecting valuable proprietary information, while allowing employees to utilize for their own individual benefit information that does not warrant protection.[204] By requiring employers to show that they reasonably protected their information, the CFAA would provide valuable evidence to fact finders indicating that a defendant was wrongful in misappropriating that information, while also signaling to courts and employees that the information was important enough to merit such protection.[205]

---

[200] *See* § 1030(a)(2)(C). Notice how the provision does not qualify the term "information" in any way.

[201] *See* Dan L. Burk & Brett H. McDonnell, *The Goldilocks Hypothesis: Balancing Intellectual Property Rights at the Boundary of the Firm*, 2007 U. ILL. L. REV. 575, 592 (2007).

[202] This proposed amendment draws language directly from the Uniform Trade Secrets Act. *See* 18 U.S.C. § 1030(a)(2)(C); Uniform Trade Secrets Act § 1(4)(ii) (1985).

[203] Uniform Trade Secrets Act § 1(4)(i)-(ii) (1985).

[204] *See* Bone, *supra* note 26, at 262.

[205] *Rockwell*, 925 F.2d at 178.

This amendment would also serve to keep the CFAA adaptable in a constantly changing technological environment. Those securities measures considered reasonable today may be wholly unsatisfactory several years from now. As technology advances and the cost of sophisticated data protection decreases, this fact-sensitive approach would allow courts to hold employers to an appropriate and contemporary standard of data protection.[206]

Most importantly, amending the CFAA to include a reasonable efforts provision would bring the statute more closely in line with its original purpose—to provide much needed protection at the federal level against the threat of serious security breaches executed by sophisticated computer hackers.[207] There is no question that an employer should be adequately protected against individuals who wrongfully hack into a computer system and steal valuable information. That said, there is no reason that employers should be excused from the responsibility of protecting their information in a reasonable manner, simply because that information is stored on a computer. By amending the CFAA to include a reasonable efforts provision, Congress will ensure that employers continue to enjoy protection against sophisticated data theft, and in exchange, need only protect their information in a manner that is considered reasonable under the circumstances to maintain its secrecy.

Glenn R. Schieck[†]

---

[206] Cundiff, *supra* note 35, at 364.

[207] *See* 132 CONG. REC. 7816 (1986) (statement of Rep. William J. Hughes).

[†] J.D. Candidate, 2014, Brooklyn Law School. B.S., 2008, Cornell University School of Industrial and Labor Relations. I wish to thank the *Brooklyn Law Review* staff for their assistance in the editing process, Stephen Popernik for his substantial assistance traversing trade secrets law, and Cori for her constant support.