Journal of Criminal Law and Criminology

Volume 104 | Issue 3 Article 4

Fall 2014

"Obtaining" the Right Result: A Novel Interpretation of the Computer Fraud and Abuse Act That Provides Liability for Insider Theft Without Overbreadth

Kevin Jakopchek

0091-4169/14/10403-0605
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 104, No. 3
 Printed in U.S.A.

COMMENTS

"OBTAINING" THE RIGHT RESULT: A NOVEL INTERPRETATION OF THE COMPUTER FRAUD AND ABUSE ACT THAT PROVIDES LIABILITY FOR INSIDER THEFT WITHOUT OVERBREADTH

Kevin Jakopchek*

TABLE OF CONTENTS

* J.D., Northwestern University School of Law, 2014; B.A., University of Notre Dame, 2010. I would like to thank Professor Ellen Mulaney and my friend and classmate Ryan Baggs for their early guidance with the idea that became this Comment, as well as the editors of the *Journal of Criminal Law and Criminology* for their dedicated, meticulous, and patient help.

INTRODUCTION

For major financial trading firms, the money is not really in the stocks they trade; it is in the methods they have developed to trade them. In 2008, financial firms generated an estimated $21 billion in profits from high-frequency trading (HFT).[1] HFT utilizes computers, operating under the control of complex algorithms, to mine dozens of marketplaces for information, while simultaneously executing purchase and sale orders.[2] These computers are able to spot trends, analyze information, and place millions of orders in fractions of a second, giving them a distinct advantage over human traders and slower computers.[3] The algorithms that control the computers are the geese that lay many of Wall Street's golden eggs, and their development and confidentiality are vital to the success of HFT firms.[4]

One of the biggest firms using HFT is Goldman Sachs.[5] Goldman understands the value of its algorithms, richly compensating the employees who develop them. In 2009, Sergey Aleynikov was programming HFT code for Goldman and making $400,000 a year.[6] In return, Aleynikov agreed to Goldman's confidentiality policy that made clear that his work was the intellectual property of the firm, required him to keep all proprietary information in confidence, and barred him from taking any information or using it when his employment ended.[7]

In April 2009, a start-up firm called Teza Technologies was attempting to develop its own HFT system and offered Aleynikov more than $1 million per year to develop part of its algorithm.[8] Teza let Aleynikov know that it was expecting the system to be developed far faster than usual.[9] Aleynikov accepted Teza's offer and set his last day at Goldman for June 5, 2009.[10] In a scene reminiscent of spy capers, at 5:20 p.m. that day—just before his going away party—Aleynikov went to his office, secretly encrypted more than 500,000 lines of Goldman's HFT source code, and uploaded the code to a foreign server.[11] He then deleted the encryption program and tried to

---

[1] Charles Duhigg, *Stock Traders Find Speed Pays, In Milliseconds*, N.Y. TIMES, July 24, 2009, at A1.

[2] *See id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] United States v. Aleynikov, 676 F.3d 71, 74 (2d Cir. 2012).

[7] *See* United States v. Aleynikov, 737 F. Supp. 2d 173, 175 (S.D.N.Y. 2010).

[8] *Aleynikov*, 676 F.3d at 74.

[9] *Id.*

[10] *Id.*

[11] *Id.*

erase the history of his computer commands.[12] Later that evening, he downloaded the source code to his home computer and copied some of the files to other computers.[13] On July 2, Aleynikov flew to Chicago to attend meetings at Teza and brought a flash drive and laptop containing portions of Goldman's HFT code.[14]

Aleynikov was arrested by federal agents when he arrived home from those meetings.[15] He was charged with one count each of violating the Computer Fraud and Abuse Act (CFAA), the Economic Espionage Act (EEA), and the National Stolen Property Act (NSPA).[16] The district court dismissed the CFAA count before trial, but Aleynikov was ultimately tried and convicted under the EEA and the NSPA counts.[17] However, on April 11, 2012, the United States Court of Appeals for the Second Circuit overturned both convictions on Aleynikov's appeal.[18]

The NSPA makes it a crime to "transport[ ], transmit[ ], or transfer[ ] in interstate or foreign commerce any goods, wares, merchandise, securities or money, of the value of $5,000 or more, knowing the same to have been stolen, converted or taken by fraud."[19] The question before the Second Circuit regarding the NSPA was whether the algorithm constituted a "good, ware, or merchandise."[20] Relying on Supreme Court precedent, the Second Circuit concluded that the code did not qualify because "[s]ome tangible property must be taken from the owner for there to be deemed a 'good' that is 'stolen' for purposes of the NSPA."[21] Since the HFT code was intangible property, the court reversed Aleynikov's NSPA conviction.[22]

The EEA conviction appeal also centered on the nature of the HFT code. Here, the Second Circuit asked whether the HFT code was either "produced for" or "placed in" commerce.[23] The district court had ruled that the HFT code was "produced for" commerce because Goldman used it to execute trades.[24] The Second Circuit ruled that because Goldman had no intention of selling or licensing its system to anyone, however, the code

---

[12] *Id.*
[13] *Id.*
[14] *Id.*
[15] *Id.*
[16] *Id.* at 74–75.
[17] *Id.* at 75.
[18] *Id.*
[19] 18 U.S.C. § 2314 (2012).
[20] *See Aleynikov*, 676 F.3d at 76.
[21] *Id.* at 77.
[22] *Id.* at 78–79.
[23] *Id.* at 79.
[24] United States v. Aleynikov, 737 F. Supp. 2d 173, 179 (S.D.N.Y. 2010).

itself was not a product produced for commerce.[25] Indeed, the court noted that Goldman went to "great lengths" to maintain the code's secrecy, as Goldman's profits "depended on no one else having" the code. [26] Thus, the very attribute that made the theft damaging to Goldman—that the value of the source code depended on confidentiality—meant that Aleynikov's theft was not a violation of the EEA.

HFT systems are valuable because they confer traders an advantage over competitors who are not using them.[27] If another firm can gather the same information and make the same trades at the same frequency, the value of Goldman's system is reduced. Such loss is the reason why prosecutors tried to fit three different statutes to Aleynikov's actions. The EEA and NSPA counts' failures illustrate a point that underlies this Comment: traditional statutory regimes are, at times, inadequate to address certain criminal acts presented in the digital age.

This Comment argues that Aleynikov's theft should constitute a violation of federal law, but not the NSPA or EEA. Rather, this Comment focuses on the third statute Aleynikov was originally charged with violating, one specifically enacted to address digital age crimes: the Computer Fraud and Abuse Act (CFAA). In dismissing the CFAA count, the district court looked to persuasive authority that held that the CFAA is only violated when computer users access information that they do not have permission to access for any purpose.[28] Such precedent represents a CFAA narrow interpretation, which developed in response to other cases that applied a broad interpretation.[29] Those cases held that the CFAA implicitly contained use restrictions, meaning that improper information use could violate the statute.[30] The narrow interpretation adopted in the *Aleynikov*

---

[25] *Aleynikov*, 676 F.3d at 82.

[26] *Id.*

[27] *See* Duhigg, *supra* note 1.

[28] *See Aleynikov*, 737 F. Supp. 2d at 192 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009); Univ. Sports Pub. Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 382–84 (S.D.N.Y. 2010); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010); Jet One Grp., Inc. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980 (JS) (ETB), 2009 WL 2524864, at *5 (E.D.N.Y. Aug. 14, 2009)).

[29] For circuits that have followed the broad interpretation, see United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001); *see also infra* Part III.A & B.

[30] *See, e.g.*, *Citrin*, 440 F.3d at 420–21; *EF Cultural*, 274 F.3d at 582; NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1056 (S.D. Iowa 2009); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

trial court criticized these "broad interpretation" or "use restrictions" approaches as overly broad with little textual grounding.[31]

Those criticisms have merit, but the narrow interpretation adopted in *Aleynikov* is also flawed. It renders the CFAA ineffective when employees misappropriate data. This Comment advances a novel interpretation of the CFAA, which would impose liability for employee data theft while avoiding the pitfalls of overbreadth that plague the current broad interpretations.

Part I of this Comment gives a brief background of computer crime, computer misuse statutes, and the CFAA. Part II discusses CFAA provisions that are relevant to employee data theft. Part III provides a summary of the current circuit split regarding insider theft under the CFAA, the split between the narrow and broad interpretation theories. Part IV argues that insider theft should be prohibited by federal law generally and the CFAA specifically, but acknowledges the validity of critiques of the CFAA's current broad interpretation. Finally, Part V advances a new CFAA interpretation that brings insider data theft within the scope of the statute, while eliminating concerns about overbreadth.

I. THE PROBLEM OF DIGITAL THEFT

A. A RISING PROBLEM

It is a truism that computer technology occupies a central place in modern business. It is not just digital communication that is pervasive; businesses have largely discarded paper and boxes for hard drives and servers as the preferred means of storing information. And with the advent of mobile devices (flash drives, laptops, smart phones, etc.) employees can access and transmit electronic data with ease. Given the concurrent dependence on digital storage and ease in digital transmission, it may be no surprise that data theft is a rising problem for businesses.[32] In fact, many data thieves are in positions similar to Sergey Aleynikov: members of a company's management with the ability to take electronic files as they prepare to leave the company (or even after they have left).[33]

A study conducted by accounting and consulting firm KPMG showed that between 2006 and 2008, cases of employee-related data theft more than

---

[31] *Aleynikov*, 737 F. Supp. 2d at 193–94.

[32] *See* Pamela Taylor, Comment, *To Steal or Not to Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 HOUS. L. REV. 201, 205–06 (2012).

[33] *See* Fahmida Y. Rashid, *Electronic Data Theft More Prevalent than Physical Thefts: Survey*, EWEEK (Oct. 18, 2010), http://goo.gl/IjaeGr.

doubled.[34] In roughly 70% of those thefts, the employees moved to a rival company, and a substantial number of thieves used stolen data to start competing businesses themselves.[35] The KPMG study predicted that the number of such insider thefts was "almost certain" to increase further,[36] and a 2010 report on trends in international fraud validated that prediction.[37] In that survey, businesses reported that electronic data thefts outnumbered tangible property thefts and that financial losses from data theft were greater than losses from physical thefts of cash, assets, and inventory.[38]

The firms most threatened by the rise in data theft are those in "information-rich industries" such as financial services, professional services, technology, and communications.[39] These industries both depend most on proprietary information and are plagued by the highest levels of electronic theft. Damage from data theft is not limited to the monetary value of the information; there is a "risk of reputational damage if your firm loses customer data. That itself could be an existential threat to your business."[40] Disturbingly, firms are not well protected against such threats, as surveys of employees show many believe that digital theft is common and can be committed with relative impunity.[41]

B. COMPUTER MISUSE STATUTES AS POTENTIAL REMEDIES

The rise of computer-related crimes was not unanticipated. Starting in the late 1970s, states enacted legislation to combat computer misuse that was not effectively addressed by preexisting law.[42] Abuses such as hacking, distribution of deleterious programming code, denial-of-service attacks, and theft of digital information were not adequately covered by existing law. Trespass and burglary laws, for example, were generally too tied to the physical world, while theft laws were too dependent on true owners being deprived of their property interest.[43]

---

[34] Leslie Paul Machado, *Protecting Against Employee Theft*, HUMAN RES. EXEC. ONLINE (July 12, 2010), http://goo.gl/Nh53zc (citing a 2009 KPMG study).

[35] *Id.*

[36] *Id.*

[37] *See* Rashid, *supra* note 33.

[38] *Id.*

[39] *Id.*

[40] *Id.* (quoting Tommy Helsby, Kroll chairman for Europe, Middle East, and Africa).

[41] *See* Taylor, *supra* note 32, at 206.

[42] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602–15 (2003); *see also* Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 835–36 (2009) (citing Kerr, *supra*, at 1602–07).

[43] Field, *supra* note 42, at 835 n.102, 835–36.

As one commenter described it, "[c]omputer-related criminal conduct presents a challenge . . . because it involves electronic impulses that cannot be seen, touched, moved, or copied as those terms have traditionally been defined, and that therefore seem to fall outside the idea of 'property' as defined over centuries of Anglo-American jurisprudence."[44] This is because "[l]arceny and theft statutes typically require proof that the defendant exercised unauthorized control over the property of another with the intent to deprive the other of all or part of its value."[45]

This problem manifested itself in the case of *Lund v. Commonwealth*, in which the Virginia Supreme Court held that unauthorized use of a computer could not be prosecuted under a larceny statute.[46] Specifically, the court held that "[a]t common law, larceny is the taking and carrying away of the goods and chattels of another with intent to deprive the owner of the possession thereof permanently."[47] Because the computer owner was not deprived of possession, the larceny statute was inapplicable.[48] The *Aleynikov* case provides a more recent example of this dilemma, with the Second Circuit holding the NSPA inapplicable to intangible property, such as the stolen source code.[49]

But states were not alone in enacting computer misuse laws. The U.S. Congress also enacted a new, specific computer crime statute. The CFAA[50] was Congress's first federal computer crime law.[51] Enacted in 1984, Congress updated it in 1986, 1990, 1994, 1996, 2001, and 2008.[52]

II. THE CFAA STATUTE

The CFAA section most relevant to employee theft of digital information is 18 U.S.C. § 1030(a)(2)(C), which holds as criminally liable those who "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any

---

[44] Joseph M. Olivenbaum, *<Ctrl><Alt><Del>: Rethinking Federal Computer Crime Legislation*, 27 SETON HALL L. REV. 574, 577 (1997).

[45] Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 BUS. LAW. 1395, 1400 (2007).

[46] 232 S.E.2d 745, 748 (Va. 1977).

[47] *Id.*

[48] *See id.*

[49] *See* United States v. Aleynikov, 676 F.3d 71, 74 (2d Cir. 2012).

[50] *See* Kerr, *supra* note 42, at 1598 n.11 (explaining that the name "Computer Fraud and Abuse Act" technically refers only to the 1986 amendments to the statute, but that in practice both courts and commentators use the name and its acronym for the entire statute).

[51] *Id.* at 1615.

[52] 18 U.S.C. § 1030 (2012); Kerr, *supra* note 42, at 1615.

protected computer."[53] Violation of § 1030(a)(2)(C) is a misdemeanor unless it is committed "for purposes of commercial advantage or private financial gain,"[54] in furtherance of any "criminal or tortious act,"[55] or if the value of information obtained is greater than $5,000.[56]

Also relevant is § 1030(g), which creates a civil remedy for some victims of CFAA violations.[57] Consequently, much of the case law regarding § 1030(a)(2)(C) interpretation has occurred in civil cases. Subsequent criminal cases have not distinguished between statutory CFAA interpretations in criminal and civil contexts.[58] Thus, this Comment relies on both civil and criminal CFAA cases' interpretive developments.

The statute also defines a number of terms, and two definitions are particularly pertinent. "Protected computer" is defined as 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."[59] That broad definition means that "protected computer" effectively encompasses any computer connected to the Internet.[60]

The second term, and the most significant one for this Comment, is the phrase "exceeds authorized access," which the statute defines 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."[61] This provision applies to "insider" situations, such as employee data theft.

III. THE CIRCUIT SPLIT REGARDING CFAA'S REACH

In deciding cases of employee digital theft, courts have focused on the word "authorized" in "exceeded authorized access."[62] Two main

---

[53] *Id.* § 1030(a)(2)(C).

[54] *Id.* § 1030(c)(2)(B)(i).

[55] *Id.* § 1030(c)(2)(B)(ii).

[56] *Id.* § 1030(c)(2)(B)(iii).

[57] *Id.* § 1030(g).

[58] *See, e.g.*, United States v. Nosal, 676 F.3d 854, 856 (9th Cir. 2012) (en banc) (citing as authoritative the CFAA interpretations from the civil case *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)).

[59] 18 U.S.C. § 1030(e)(2)(B).

[60] *See* Kerr, *supra* note 42, at 1663.

[61] 18 U.S.C. § 1030 (e)(6).

[62] *See, e.g.*, *Brekka*, 581 F.3d at 1129 ("We affirm. Because [Christopher] Brekka was authorized to use LVRC's computers while he was employed at LVRC, he did not access a computer 'without authorization' . . . ."); NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1056 (S.D. Iowa 2009) ("The issue for the Court to decide is whether an employee

interpretation branches of that word have emerged: broad interpretation, which has led to findings of liability, and narrow interpretation, which has led to employees being held not liable in civil cases or not guilty in criminal cases.[63] The broad interpretations impose restrictions on how insiders use information,[64] while the narrow theory ignores use and focuses solely on whether the insider has permission to view data.

Two main theories have emerged to justify a broad interpretation: agency theory and contract theory.[65] Instead of defining "authorized access" by whether someone has permission to access information, these theories look to their duties and responsibilities relating to access. Courts derive these duties from other legal principles, namely the law of agency and contract.[66]

A. BROAD INTERPRETATION THROUGH AGENCY THEORY

The agency approach asserts that in the employer–employee context, "authorized access" is governed by the same law that governs the employer–employee relationship: the law of agency.[67] The theory specifically focuses on the duty of loyalty that employees owe employers.[68] That duty requires employees to act solely for the benefit of their employer and, most relevantly, means that an employee's authority to act for the employer is terminated when "without knowledge of the principal, he acquires adverse interests or is otherwise guilty of a serious breach of

---

may act 'without authorization' or 'exceeds authorized access' when he accesses confidential and proprietary business information . . . that he has permission to access, but then uses that information in a manner inconsistent with the employer's interest or in violation of other contractual obligations . . . .").

[63] *Compare* Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (imposing liability when an employee used information that he otherwise had permission to access for work purposes), *with Brekka*, 581 F.3d at 1129 (refusing to impose liability when an employee used information that he otherwise had permission to access for work purposes).

[64] *See, e.g.*, *Citrin*, 440 F.3d at 420; EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001) (imposing liability when an employee provided confidential information to a competitor); *Artino*, 638 F. Supp. 2d at 1058–59 (imposing liability when a company vice president accessed the company's customer list and e-mailed it to himself for use in future competition).

[65] *See* Field, *supra* note 42, at 822–23.

[66] *See Citrin*, 440 F.3d at 420–21 (evaluating authority using principles of agency law); *Explorica*, 274 F.3d at 582 (evaluating authority through the lens of contract law using a confidentiality agreement).

[67] *See* Kerr, *supra* note 42, at 1633–34.

[68] *Id.*

loyalty to the principal."[69] In the employer–employee context, the duty of loyalty is breached at the moment the employee resolves to compete with or otherwise harm the employer.[70] In the context of the CFAA, then, this theory means that authorization to access any information is implicitly revoked by the employee's breach of the duty of loyalty.[71] Consequently, even if an employee has permission to access information for work purposes, he still violates the CFAA by accessing such information with an intent that violates the duty of loyalty.

The Seventh Circuit adopted this interpretation in *International Airport Centers, L.L.C. v. Citrin*.[72] In that case, an employee deleted all of the data on one of his employer's laptops.[73] The employee had permission to access the computer and the specific data for work purposes.[74] The court held that when the employee resolved to destroy the files, however, he breached his duty of loyalty, which implicitly revoked his permission to access the data.[75] The CFAA claim against him therefore survived a motion to dismiss.[76] In a different case, the U.S. District Court for the Western District of Washington held that defendants stated a sufficient CFAA claim against an employee who e-mailed confidential information to a competitor when he was preparing to jump ship.[77] The employee had allegedly breached his duty of loyalty and therefore would be unauthorized to access the information.[78]

The agency approach's broad scope means it can be said to be the most employer-friendly approach, as simply acquiring interests adverse to the employer can revoke authorization and result in liability.[79] Accordingly,

---

[69] *See Citrin*, 440 F.3d at 421 (quoting State v. DiGiulio, 835 P.2d 488, 492 (Ariz. Ct. App. 1992); RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).

[70] *See id.* at 420–21 (holding that authority to access information ends when an employee acquires adverse interests).

[71] *See* Field, *supra* note 42, at 823.(citing Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000)).

[72] *Citrin*, 440 F.3d at 420–21.

[73] *Id.* at 419.

[74] *Id.*

[75] *Id.* at 420 ("For his authorization to access the laptop terminated when . . . he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee.").

[76] *See id.* at 420–21.

[77] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1123, 1129 (W.D. Wash. 2000).

[78] *Id.* at 1125 ("[T]he authority of the plaintiff's former employees ended when they allegedly became agents of the defendant.").

[79] *See* Field, *supra* note 42, at 824 (calling the agency theory "undoubtedly the most employer-favorable approach, since simply characterizing the employee's actions as against the employer's interests will likely result in liability").

this theory ensures that virtually any fact pattern involving "insider" digital theft results in liability under the CFAA.[80]

B. BROAD INTERPRETATION THROUGH CONTRACT THEORY

Other courts have looked to the law of contracts to define the scope of "authorization" under the CFAA. This approach looks at explicit terms of employment (e.g., employment agreements, employee handbooks, published policies) to define what access is authorized.[81] In one case applying contract theory, *EF Cultural Travel v. Explorica Inc*., former employees provided information to their former employer's competitor.[82] The First Circuit looked to those employees' employment contracts and determined that their disclosure likely violated a confidentiality provision therein.[83] Because the contract governed the scope of the authorization to access information, the First Circuit reasoned that if the defendant's allegations were proven, the employees violated the agreement and exceeded authorization, making them potentially liable under the CFAA.[84]

In *United States v. Czubinski*, the First Circuit employed similar reasoning by examining an employee handbook signed by an IRS employee.[85] The handbook rules of conduct limited computer access to "only those accounts required to accomplish . . . official duties."[86] The court determined that the IRS employee exceeded his authorized access under the CFAA when he browsed acquaintances' tax returns, even if the defendant did not obtain anything "of value" to sustain a conviction under the specific subpart.[87]

This contract-based approach has the advantage of expressly delineating what access is or is not permitted for each individual. It also allows some flexibility, as prohibited conduct adjusts to the terms of the contract, and employers can adjust for more or less leeway for their employees' access to information depending on the sensitivity of information or other considerations.

---

[80] Kerr, *supra* note 42, at 1634 (declaring that "the apparent effect of *Shurgard* is to criminalize an employee's use of an employer's computer for anything other than work-related activities").

[81] Field, *supra* note 42, at 827 ("The contract-based interpretation requires the computer user to violate a contract before that user's access can be found to be unauthorized.").

[82] 274 F.3d 577, 579–80 (1st Cir. 2001).

[83] *Id.* at 583–84.

[84] *Id.* at 583.

[85] *See* 106 F.3d 1069, 1071 (1st Cir. 1997).

[86] *Id.* at 1071 n.1.

[87] *See id.* at 1078 (reversing Richard Czubinksi's conviction but finding that he "unquestionably exceeded authorized access to a Federal interest computer").

C. NARROW INTERPRETATION

The narrow interpretation of the CFAA arose as a response to the broad theories. Courts were worried that those theories rely heavily on principles extrinsic to the statute, conflate statutory terms, and could encompass acts that Congress did not intend the CFAA to address.[88] Because of those worries, courts developed the narrow theory, claiming that it focused on a plain language reading of the statute and the word "authorized."[89]

The first court to develop such a theory was the Ninth Circuit in *LVRC Holdings LLC v. Brekka*.[90] In *Brekka*, an employer sued its former employee under the CFAA after the employee e-mailed data to himself and then used that data to compete with his former employer.[91] The district court had held that because the employee had permission to access the information, he could not be liable under the CFAA, and the appellate court upheld the district court's narrow reading of the statute.[92] *Brekka* stressed that the term "authorization" has no technical or ambiguous meaning, and that the dictionary definition should govern.[93] The Ninth Circuit looked to the plain language in reducing the question to whether an employer gave the employee permission to access specific information and, if access had been granted, no violation could occur.[94] Thus, if a person was granted access to a customer list for a specific purpose, for instance, he could not be prosecuted under the CFAA for any action taken regarding that customer list, regardless of the action.

Under this interpretation, courts do not analyze use (or misuse), but rather only ask whether the employee was allowed to access the information in the course of employment.[95] This inquiry limits the application of "exceeding authorized access" only to those situations where an employee has authorization to access a computer but then "hacks" into information he

---

[88] United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (discussing "innocuous" acts that broad CFAA interpretations would criminalize).

[89] *See*, *e.g.*, *id.* at 863; LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

[90] *Brekka*, 581 F.3d 1127.

[91] *See id.* at 1129–30.

[92] *See id.* at 1132, 1137.

[93] *Id.* at 1133 (citing RANDOM HOUSE UNABRIDGED DICTIONARY 139 (2001) and adopting its definition of "authorization" as persuasive in defining "exceeds authorized access")

[94] *See id.*

[95] *See* Field, *supra* note 42, at 825 (explaining that "where an employee has been affirmatively granted the ability to use and access a computer database or system, his authorization cannot be challenged under the code-based interpretation").

does not have permission to access.[96] For example, an employee might use the computer he is allowed to use to access an encrypted file on the employer network that he is not allowed to access.[97]

This narrow type of analysis is also exemplified in the criminal case *United States v. Nosal*.[98] In *Nosal*, a former employee who had set up a competing company convinced some of his former colleagues to use their access to obtain data from a confidential database.[99] The district court originally held Nosal liable under the CFAA by applying a broad interpretation.[100] After *Brekka*, Nosal moved for, and was granted, reconsideration of its motion to dismiss.[101] The district court then granted dismissal, as *Brekka* explicitly rejected the broad-interpretation reasoning that supported the court's original denial.[102] Ultimately, the Ninth Circuit affirmed.[103] The former colleagues, as current employees, were allowed by their employer to access the information as part of their jobs.[104] According to the court, because the current employees were allowed to access the information, the CFAA did not make them liable for sending Nosal the data.[105]

IV. THE CIRCUIT COURTS' FLAWED APPROACHES

For a variety of reasons, the CFAA should be interpreted as extending liability to insider theft of digital information. Policy justifications, in the form of the rising danger of digital theft, privacy concerns, and the nature of the Internet, support the need for a federal statute criminalizing insider digital information theft. Further, the CFAA's history indicates that it was indeed intended to extend liability to such crimes. Finally, the statutory

---

[96] *See id.*

[97] Kerr, *supra* note 42, at 1604 ("For example, a person can hack into a corporate network and see secret files that the person is not supposed to view. In such a case, the hacker will have exceeded her privileges on the network; she will see more than the network was configured to allow her to view.").

[98] 676 F.3d 854 (9th Cir. 2012) (en banc).

[99] *Id.* at 856.

[100] *See* United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at *5 (N.D. Cal. Apr. 13, 2009).

[101] *See* United States v. Nosal, No. C 08-0237 MHP, 2010 WL 934257 (N.D. Cal. Jan. 6, 2010).

[102] *See id.* at *5–6.

[103] *Nosal*, 676 F.3d 863.

[104] *Id.* at 864.

[105] *Id.* at 863 ("For our part, we continue to follow in the path blazed by *Brekka* and the growing number of courts that have reached the same conclusion. These courts recognize that the plain language of the CFAA 'target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation.'" (citations omitted)).

language itself, particularly the express statutory definition of "exceeds authorized access" supports liability and cannot be construed consistently with the narrow interpretations. However, the current forms of the broad interpretations are also unworkable due to the overbreadth of what they criminalize. Thus, this Comment advances a third theory, consistent with congressional intent, which would criminalize insider data theft without the overreach of the current broad interpretations.

A. POLICY CONCERNS JUSTIFY A FEDERAL PROHIBITION ON INSIDER DIGITAL INFORMATION THEFT

Three policy concerns support extending liability to insider digital information theft through a federal law. First, the growing harms of digital theft warrant additional protection. Second, such liability will help to protect the privacy interests of third parties whose concerns may not be adequately internalized by the companies that possess their data. Third, the federal government is better situated to police digital theft than the states.

As discussed, digital theft is a present and growing problem for businesses, now costing companies more than theft of physical objects.[106] Further, the ease of transmitting digital information leaves employees with a sense of invulnerability when it comes to committing digital theft.[107] The CFAA's dual criminal and civil nature provides the deterrent effect traditionally associated with criminal prohibition, and the civil provisions allow businesses the opportunity to seek restitution. Indeed, the significant dangers presented by digital theft have influenced judicial decisions in both Australia and England to extend laws against unauthorized access to also proscribe access for unauthorized purposes.[108]

Another policy rationale is that criminalization of digital theft protects third-party privacy.[109] Third parties, such as customers and clients, may provide firms with personal information that those firms use in the course of business for tasks, such as marketing. Many of the privacy-related concerns may not be sufficiently internalized to firms and their data security policies and procedures.[110] That is to say, those who bear the social costs of privacy breaches, the data subjects, do not have control over the security

---

[106] *See supra* note 34–38 and accompanying text.

[107] *See supra* note 41 and accompanying text.

[108] *See, e.g.*, R v. Bow Street Metro. Stipendiary Magistrate, *ex parte* Gov't of the United States, [2000] 2 UKHL 216 (interpreting U.K. Computer Misuse Act similarly); DPP (Vic) v Murdoch, [1993] 1 VR 406, 409–11 (Austl.) (interpreting State of Victoria Computer Trespass Act to apply to a bank employee).

[109] Winn, *supra* note 45, at 1420–22 (explaining that criminalization would protect third-party privacy in a discussion of the pros and cons of a criminalization scheme).

[110] *Id.* at 1420.

measures adopted by those who aggregate the data. In these instances, criminalization may provide a deterrent effect to protect third-party privacy that would otherwise be absent in a scheme that only provided for civil recourse or no recourse at all.

One instance in which the CFAA served this purpose was the case *United States v. Rodriguez*.[111] In that case, a Social Security Administration (SSA) agent used the SSA database to obtain information about female acquaintances, including his ex-wife, his former girlfriend, his former colleague's daughter, and a waitress who worked at a restaurant he frequently visited, among others.[112] The SSA had a computer-use policy, reinforced through training, which instructed employees that access to database information was only allowed for legitimate business purposes.[113] Even though Roberto Rodriguez refused to sign annual forms acknowledging that he received the polices in writing,[114] the court noted that the SSA still told Rodriguez he was not authorized "to obtain personal information for nonbusiness reasons."[115] Applying contract theory, the Eleventh Circuit held that Rodriguez had exceeded his authorized access when he perused the information for personal gain and was guilty of a CFAA violation.[116]

A second rationale for federal criminal liability is that the nature of digital theft requires regulation by federal authorities, as opposed to regulation by states. One issue relates to jurisdiction. Consider, for instance, a hypothetical situation involving an employee who works in California for a company incorporated in Delaware with its principal place of business in New York. The employee downloads information stored on servers in Illinois, and then uploads that information to a competitor based in Florida. Which state's digital theft law shall apply? The application of federal law not only eliminates complex jurisdictional and choice-of-law questions for the courts; it also provides clearer guidance for citizens regarding prohibited conduct. Second, coupling the geographically dispersed nature of computer crime and the fact that one goal of the CFAA it to provide a civil recourse, a national statute would facilitate plaintiffs' pursuit of remedies. Finally, given the possibility of such diffuse

---

[111] 628 F.3d 1258 (11th Cir. 2010); *see also* Andrew T. Hernacki, Note, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1556–57 (2012) (discussing *Rodriguez*'s application to theft of third-party information).

[112] *Rodriguez*, 628 F.3d at 1260–62.

[113] *Id.* at 1260.

[114] *Id.*

[115] *Id.* at 1263.

[116] *See id.* at 1263–64.

geographic scope and the technological complexity of computer crime, federal investigators—with national reach and superior resources—may be better suited for such enforcement than local authorities.

Indeed, Orin Kerr, a leading advocate of a narrow CFAA interpretation, notes the potential value of a federal law criminalizing insider digital theft.[117] Referring to cases of insider liability, Kerr wrote: "I don't think these facts should fit under 18 U.S.C. 1030 because they deal with a different kind of problem; it's hard to fit them in to 1030 without causing incredibly broad liability. But I do think it's fair to want to criminalize such conduct with a different statute."[118] Kerr even went so far as to draft his own potential statute to criminalize insider digital theft,[119] and he defended his draft by arguing that it was "necessary" because courts have held, as they did in *Aleynikov*, that the NSPA does not cover digital information.[120] That one of the leading advocates for a narrow CFAA interpretation thinks that *some* law criminalizing insider digital theft is "necessary" demonstrates the strength of the policy arguments in favor of criminalizing that conduct. But in Part V, this Comment shows that an entirely new statute is unnecessary to counter Kerr's fears of CFAA overbreadth. I advocate for a novel CFAA interpretation that focuses on the word "obtain" in the definition of "exceed authorized access." This interpretation shows that the CFAA, as written, can achieve necessary, but limited, insider theft liability.

B. CFAA LEGISLATIVE HISTORY SHOWS IT SHOULD BE INTERPRETED TO CRIMINALIZE INSIDER DIGITAL[121]

The CFAA's Congressional Reports make clear that one of Congress's central purposes in enacting the CFAA was to protect against information misappropriation. Indeed, while advocates of a narrow interpretation maintain that the statute is concerned only with access, not misuse, the entire history of the statute indicates that it was largely driven to combat a

---

[117] Orin Kerr, *What About the Insiders? A Second Proposal to Change the Computer Crime Statutes*, THE VOLOKH CONSPIRACY (Jan. 23, 2013, 9:44 PM), http://goo.gl/3fHUCN.

[118] *Id.*

[119] *Id.*; Orin S. Kerr, *18 U.S.C. 1031, Employee Misuse of Computer Information: January 22, 2013 Draft*, THE VOLOKH CONSPIRACY, http://goo.gl/ALvt0m (last visited June 2, 2014).

[120] Kerr, *supra* note 117.

[121] The 2001 and 2008 amendments do not affect the construction of 1030(a)(2) and are not discussed here. For a discussion of the effect of those amendments, see Taylor, *supra* note 32, at 207–08.

specific misuse: theft.[122] CFAA amendments and their corresponding reports also indicate that Congress intended to expand the Act to cover insider theft, and that the scope of insider "authorization" is indeed affected by the *purpose* of authorization.[123]

The first version of the CFAA, passed in 1984, was primarily aimed at "protecting classified information on government computers, as well as protecting financial records and credit information on government and financial institution computers."[124] While the computers and information covered under the CFAA were originally limited, one purpose, even in the initial bill, was to prevent electronic data theft. A 1984 House Report states that the proposed legislation was necessary because "[i]t is obvious that traditional theft/larceny statutes are not the proper vehicles to control the spate of computer abuse and computer-assisted crimes."[125] As one court stated, the reason that such statutes were not proper vehicles was because "they generally do not define property to include electronically processed or stored data."[126] This was the exact concern discussed previously in Part II.

The 1986 amendments expanded the Act to provide liability for other forms of fraud and related activities in connection with access to devices and computers.[127] Congress, however, specifically limited such prohibitions to "Federal interest computers."[128] As the committee explained, the goal was "to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature."[129] With the Internet's advent and expansion, this jurisdictional limitation disappeared as "almost all computer use has become interstate in nature."[130]

While the Act was then limited to such "Federal interest"[131] computers, the Senate Reports reveal that the 1986 amendments were intended to expand the actions covered to allow prosecutors to fit the

---

[122] *See* S. REP. NO. 104-357, at 5 (1996) (explaining that the legislative intent behind the passage of the CFAA includes addressing "the problem of computer crime"); *see also* note 139 and accompanying text.

[123] *See infra* notes 136–37 and accompanying text.

[124] Mark D. Weller & Ronald J. Shaffer, *Making a Federal Case Out of Employee Theft of Trade Secrets*, 26 ACC DOCKET 96, 98 (2008).

[125] H.R. REP. NO. 98-894, at 9 (1984).

[126] Black & Decker (US), Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008).

[127] *See* Kerr, *supra* note 42, at 1629–30.

[128] S. REP. NO. 99-432, at 10.

[129] *Id.* at 4.

[130] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

[131] S. REP. NO. 99-432, at 10.

"square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets."[132]

The 1986 amendments also added the key phrase in insider theft situations—"exceeds authorized access"—which one commentator has argued was added to "remedy the misuse-of-legitimate-access problem" in that the 1984 Act "did not cover individuals who caused harm with authorized access."[133] In presenting the "exceeds authorized access" language for a full vote, the House Committee on the Judiciary noted that it did not intend to extend liability "to any type or form of computer access that is for a legitimate business purpose. Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected."[134] This is the most important language from the 1986 House Report.

The Report does not say that "any access that is pursuant to an express or implied authorization would not be affected" but rather "any access *for a legitimate purpose* that is pursuant to an express or implied authorization would not be affected."[135] This discussion of the addition of the "exceeds authorized access" provision demonstrates Congress's intent to address the purpose and use of information access by insiders, those who could have a legitimate purpose for accessing the information, and not simply the access itself.

The 1996 amendments further broadened the reach of the statute. Those amendments, among other changes, substituted the phrase "protected computer" for "federal interest computer."[136] The Senate Report stated the 1996 amendments' purpose was to broaden the CFAA to "ensure that the theft of intangible information . . . is prohibited *in the same way* theft of physical items are protected."[137] As courts have recognized, the Senate Report on the 1996 amendments illustrates the broad scope that they were intended to reach.[138] This conclusion is further bolstered by the Report's declaration that the CFAA "facilitates addressing in a single statute the

---

[132] *Id.* at 14 (quotation marks and citation omitted).

[133] Hernacki, *supra* note 111, at 1549.

[134] H.R. REP. NO. 98-894, at 21 (1984).

[135] *Id.* (emphasis added).

[136] *See* Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1128 (W.D. Wash. 2000) (noting Congress intended with the 1996 amendments to broaden the scope of the CFAA).

[137] S. REP. NO. 104-357, at 7 (1996) (emphasis added).

[138] *See* Guest-Tek Interactive Entm't Inc. v. Pullen, 665 F. Supp. 2d 42, 45 (D. Mass. 2009) ("[A] narrow reading of the CFAA ignores the consistent amendments that Congress has enacted to broaden its application."); *Shurgard Storage Ctrs.*, 119 F. Supp. 2d at 1129 (noting that the legislative history "demonstrates the broad meaning and intended scope" of the CFAA terms).

problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology."[139]

Finally, one section of the Report specifically counters the common retort that the CFAA should not cover computer theft of information because other laws exist to combat such theft:

> The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. . . . This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items is protected. In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.[140]

Taken together, this legislative history makes clear that one of the CFAA's central purposes is to protect against digital information theft. Indeed, while advocates of a narrow interpretation maintain that the statute is concerned only with access, not misuse, the statute's history indicates that it was largely driven to combat the specific misuse and theft of information.

Further, Congress has continually broadened the CFAA's scope, expanding it to cover theft by private entities and by not only those outside the entity (such as hackers) but also by those within the entity (such as employees).[141] In so doing, it identified the purpose as prohibiting information theft *in the same way* that tangible property theft is prohibited. Businesses are protected against employees thieving tangible property that they are permitted to use for work purposes. Consequently, businesses should similarly be protected from the theft of information that employees are permitted to access for work purposes. But even drawing such a parallel is not necessary. In the Reports concerning the 1986 amendment that added the "exceeds authorized access" language at issue, Congress made explicit that the purpose of access is part of the inquiry.[142]

---

[139] S. REP. NO. 104-357, at 5.

[140] S. REP. NO. 104-357, at 7–8; *see also Shurgard Storage Ctrs.*, 119 F. Supp. 2d at 1128 (declaring this language in the Senate Report to be "dispositive" evidence of the legislative intent behind the CFAA).

[141] Kerr, *supra* note 42, at 1662 (explaining that Congress's addition of the "exceeding authorized access" prohibition was directed at misuse committed by insiders).

[142] *See supra* notes 133–34 and accompanying text.

C. CFAA TEXT DEMONSTRATES THAT IT APPLIES TO INSIDER DIGITAL THEFT

Beyond the policy concerns and legislative history, the idea that the term "exceeds authorized access" includes liability for insider theft is supported by the textual incoherence that otherwise results. Proponents of the narrow interpretation contend that "exceeds authorized access" only applies to insiders when they employ their authorized use of a computer to access specific files they are not authorized to access, and that their use of that information is irrelevant. This interpretation ignores the statutory definition, effectively rendering "exceeds authorized access" to mean: "to access a computer with authorization and to use such access to *access* or alter information in the computer that the accesser is not entitled to *access* or alter." Such an interpretation cannot stand for three reasons.

First, this is a statute entitled "Computer Fraud and Abuse Act," not the "Computer Improper Access Act," and the words "Fraud" and "Abuse" convey that it is concerned—indeed primarily concerned—with information use and not its mere access.

Second, the definition of the term reads not just "obtain or alter" but "*so* to obtain or alter." The inclusion of the word "so" implies a concern with the manner in which data is obtained or altered and not simply with permission to access data.[143] The narrow interpretation simply ignores the presence of that duly enacted word.[144] This ignorance is no mere semantic detail; the prohibition on "altering" demonstrates that ignoring "so" could produce absurd results. Take, for example, an employee who is authorized to access a spreadsheet only to input data and, in an act of sabotage, deletes the entire spreadsheet. By virtue of her authorization to input data, that employee is entitled to "alter" the spreadsheet. If we ignore the word "so," we ignore the limited manner in which the employee is entitled to alter the data. Thus, the narrow interpretation discarding of the word "so" means any minimal authorization to alter data gives carte blanche for all alterations, including sabotage and destruction.

Third, it is contrary to the entire statute's text to read "obtain" to mean "access." The CFAA as a whole uses the word "access," or a derivative thereof, eighteen times—four times in the very definition at issue.[145] If the

---

[143] *See* United States v. Nosal, 642 F.3d 781, 785 (9th Cir. 2011), *rev'd*, 676 F.3d 854 (2012) (en banc).

[144] *Id.* at 785–86.

[145] 18 U.S.C. § 1030 (2012) (using the word "access" or a derivative thereof twice in subsection (a)(1), twice in subsection (a)(2), twice in subsection (a)(3), twice in subsection (a)(4), once in subsection (a)(5)(B), once in subsection (a)(5)(C), once in subsection (a)(6), once in subsection (a)(7)(A), four times in subsection (e)(6), and twice in subsection (e)(10)).

drafters intended "obtain" to mean "access," they would have simply used the word one more time.

Fourth, the additional prohibition on altering information also serves to further elucidate the impropriety of conflating "obtain" with "access."[146] In order to alter information, one must access it first. Thus, the narrow interpretation's conflation of "obtain" with "access" renders the word "alter" redundant; if the initial access violates the statute, it does so regardless of what is done with that information. For a theory whose merit lies in its "textual" approach, the narrow interpretation's credibility is undermined by these inconsistencies.

D. CURRENT BROAD LIABILITY THEORIES ARE ALSO FLAWED

The narrow interpretation's flaws do not mean, however, that its criticisms of the broad theories are unfounded. Indeed, as currently applied, the theories supporting broad interpretation are themselves untenable.

The law of agency as a means of determining employee liability is vague and malleable.[147] For instance, it is uncertain how "adverse" an interest must be to result in a breach of loyalty that would lead to CFAA liability.[148] Numerous other questions also remain. For example, what about interests that may not be parallel to the employer's but are not directly adverse? What if an employee is retrieving information for his own personal purposes but is not using it to the detriment of the employer? Does accessing the Internet to waste time while on the clock violate the duty of loyalty and revoke an employee's authorization? Can loyalty be restored after it is breached? Can permission to access information be restored after it is implicitly revoked? Is it fair to give someone explicit permission to do something and then implicitly revoke that permission without express notice? While the law of agency provides answers to these questions, the more salient point is—are employees (or employers) aware of those answers? As one student note put it, "[b]road interpretations, including those that would find liability for . . . breaches of agency law

---

[146] *See id.* § 1030(e)(6).

[147] *See* Field, *supra* note 42, at 843.

[148] *Id.* at 844 ("A court could determine either that acquiring any adverse interest to his employer left him without authorization, or it could find that the employee's actions did not constitute a serious enough breach of loyalty to find a termination of authorization. Both outcomes are arguably allowable under section 112 [of the Restatement (Second) of Agency] . . . .").

duties, raise significant problems of overbreadth and vagueness necessitating a more narrowly-tailored approach."[149]

Contract theory also has the potential to lead to unfair and unintended CFAA prosecutions. As the *Nosal* court pointed out:

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies . . . . [U]nder the broad interpretation of the CFAA, such minor dalliances would become federal crimes.[150]

Some may respond that such an argument is a mere technicality and rely on prosecutorial discretion to prevent such charges. The *Nosal* court addressed that argument as well, stating, "[w]hile it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you *could* be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement."[151] A federal circuit court adopting the current broad interpretations, then, could invite arbitrary and discriminatory enforcement.

Further, broad interpretation supported by contract theory could potentially lead to prosecutions for violating websites' terms of service.[152] Given that the vast majority of online services have "clickable" terms of service agreements that are pages long and are rarely read, people may unwittingly expose themselves to criminal liability for innocuous actions that they have no idea are prohibited.[153] The *Nosal* court cited one example: most social media websites have terms of service that prohibit lying. But "[l]ying on social media websites is common: People shave years off their age, add inches to their height and drop pounds from their weight."[154] Such lies may seem innocuous, but "[t]he difference between puffery and prosecution may depend on whether you happen to be someone [a federal prosecutor] has reason to go after."[155]

---

[149] Hernacki, *supra* note 111, at 1564 (internal citation omitted); *see also id.* at 1568 (criticizing the agency approach for interpreting "exceeds authorized access" in a way that implicates unconstitutional vagueness).

[150] United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (en banc).

[151] *Id.*

[152] Kerr, *supra* note 42, at 1600 (explaining that "[a]n example [of a violation under contract theory] would be use that violates the Terms of Service that an ISP imposes on its customers").

[153] *See Nosal*, 676 F.3d at 860–62.

[154] *Id.* at 862.

[155] *Id.*

These concerns are not hypothetical. In *United States v. Drew*, Lori Drew was prosecuted under the CFAA on the theory that the fake profile she created violated MySpace's terms of service.[156] Drew created the fake profile to start an "insult" war to bully one of her seventh grade daughter's classmates.[157] Creation of the fake profile, according to the prosecution, violated the website's terms of service and meant that Drew had "exceeded authorized access," violating the CFAA.[158] While Drew's actions and motivations may have been despicable, Congress passed the CFAA to protect digital property rights, not prevent cyber-bullying. If the theory is that the breach of terms of service creates the CFAA violation, then the breach of any terms of service agreement would lead to the same result, even those breaches much more innocuous than Drew's.[159]

V. THE "OBTAIN" THEORY

The circuit split is focused on the merits of the narrow interpretation or the broad interpretations.[160] But there lies another path. It provides liability for insider theft, like the broad interpretations, while accounting for concerns of overbreadth that motivate use of the narrow interpretation. This approach contends, unlike the narrow interpretation, that the CFAA does inherently contain restrictions on information use. Unlike the current broad interpretations, this approach argues that the CFAA itself limits the scope of use restrictions. Indeed, this Comment submits that the statute contains two specific use restrictions: the prohibitions on "altering" and "obtaining."[161]

---

[156] United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) ("[A] central question [in the prosecution] is whether a computer user's intentional violation of one or more provisions in an Internet website's terms of services (where those terms condition access to and/or use of the website's services upon agreement to and compliance with the terms) satisfies the first element of section 1030(a)(2)(C).").

[157] *See id.* at 452; *see also* Nicholas R. Johnson, Note, *"I Agree" to Criminal Liability: Lori Drew's Prosecution Under § 1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561, 561–65.

[158] *See Drew*, 259 F.R.D. at 457.

[159] Drew was convicted on the CFAA charge, *id.* at 453, but the conviction was dismissed post-verdict by Central District of California Judge George H. Wu, who held that the conviction violated void-for-vagueness doctrine. *Id.* at 467–68. The important point, though, is that prosecutors operating under a contract theory could, and in fact did, bring CFAA charges against someone for creating a fake profile.

[160] *Nosal*, 676 F.3d at 862 ("We remain unpersuaded by the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty." (citing United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); and Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006))).

[161] *See* 18 U.S.C. § 1030(e)(6) (2012).

In fact, in patterns involving insider theft, the overlooked "obtain" restriction is key.

The CFAA defines "exceeds authorized access" to mean 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."[162] As argued earlier, the narrow interpretation effectively ignores the word "so" and equates "obtain" with "access."[163]

Consider again an employee who has permission to use a computer and permission to access a given file. He e-mails the file to his personal e-mail address for the purpose of launching competition with his employer. According to the narrow interpretation, no violation has occurred because the employee had permission to access and use the information for his employment.[164] But the statute does not prohibit accessing information that the accesser is not entitled to access or alter. It prohibits obtaining information the obtainer is *not so entitled to obtain or alter*.

Instead of counterintuitively assigning "obtain" the meaning of "access," courts should take the approach ostensibly favored by those who advocate the narrow approach—interpreting the statute based on the plain meaning of its words. The *Merriam Webster Dictionary* defines "obtain" as "to gain or get (something) usually by effort."[165] *Black's Law Dictionary* does not define "obtain" but does define "acquire" as "to gain possession or control of; to get or obtain."[166] *The Law Dictionary*, meanwhile, defines "obtain" as "[t]o acquire; to get hold of by effort; to get and retain possession of."[167] All these definitions seem to imply a more permanent act than mere transitory access. While an employee may very well be authorized to access information, the grant of access does not mean the employee is authorized to permanently acquire the information. If prosecutors and courts give "obtain" its plain meaning, then an employee violates the statute once he uses authorized access to personally acquire or,

---

[162] *Id.*

[163] *See supra* Part III.C; *see also Nosal*, 676 F.3d at 858 ("If an employee circumvents the security measures, copies the information to a thumb drive and walks out of the building with it in his pocket, he would then have obtained access to information in the computer that he is not 'entitled *so* to obtain.'").

[164] *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) ("[A]n employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it.").

[165] *Obtain*, MERRIAM WEBSTER DICTIONARY ONLINE, http://goo.gl/aA2YJA (last visited June 2, 2014).

[166] BLACK'S LAW DICTIONARY 26 (9th ed. 2009).

[167] *Obtain*, THE LAW DICTIONARY FEATURING BLACK'S LAW DICTIONARY FREE ONLINE LEGAL DICTIONARY (2d ed.), http://goo.gl/wD9s1o.

"gain control of," information he is not "so entitled" to "acquire or, gain control of."

This interpretation is consistent with the statute's intent to create laws analogous to theft and trespass that can be applied to the digital world. For instance, an employee may be entitled to use a piece of a company's physical property, and even to take that property home with her, but that does not permit her to permanently acquire it. The distinction between this scenario and digital theft is that a true owner is not deprived of the electronic files.[168]

That distinction is precisely why traditional property laws failed in their application to digital information and precisely the reason for which specialized computer abuse laws were enacted.[169] Giving plain meaning to the term "obtain," a court should interpret the statute to bar digital information theft by defining the CFAA from the perspective of the violator, acquiring something he is not entitled to acquire, as opposed to the true owner, losing a property interest. It would thus not only be consistent with goals articulated in the specific legislative history of the CFAA but with the key motivation for computer misuse statutes in general.

Further, this plain language definition of "obtain" resolves the textual incoherency in the narrow interpretation. As previously discussed, the narrow approach conflates the meaning of "obtain" with "access," even though the drafters used the word "access" throughout the statute when they intended that meaning. Also, interpreting "obtain" to mean "access" makes the inclusion of "alter" redundant. If "obtain" had its plain meaning—"acquisition"—there were would be no redundancy; rather, the statute would prohibit two separate, specific uses of information: misappropriation and unauthorized alteration. This interpretation is consistent with the plain language definition, the language chosen throughout the statute, and the purpose of computer misuse legislation. Moreover, it leads to results consistent with the intent of the legislature.

By recognizing some liability for misuse, this interpretation gives meaning to the word "so" in "so entitled." It imposes liability on the employee who, while authorized to alter a database to input information, sabotages and destroys the database. Now, under the "obtain" theory, the scope of "so entitled" still must be defined. Here, the principles of the contract and agency theories are useful but with an important limitation: not every violation of contract or agency amounts to a CFAA violation; rather, only those actions that can be construed as "acquiring" or "altering" information constitute violations. Gone are the murkier grounds of minor

---

[168] *See* Kerr, *supra* note 42, at 1611.

[169] *See supra* Part I.B.

violations of computer-use policies (such as personal web surfing) or terms of service.

Still unresolved is the criticism that the contract and agency theories import principles extrinsic to the statute's text.[170] Ultimately, though, this criticism falls flat. Congress chose the phrase "so entitled" without further definition. As the narrow interpretation argues, words should take their common meaning, and law regarding contract and agency does indeed commonly define the scope of what employees are allowed to do. Where authorization is explicit, such as in an employment contract, the explicitly defined scope should govern.

Oftentimes, employees' authorization to act is not explicit but implicit. In the employment context, however, the law of agency is the very thing that defines the scope of implicit authorization. Congress knew that and chose not to provide any contrary definition. Without the bounds of agency law, any implicit authorization to access information becomes a blanket authorization of access and use. Further, in the context of implicit authorization, it is the potential violator who is asking the court to infer the existence of authorization. Since it is to the violator's benefit to make the inference that authorization exists at all, it is only fair to also allow an inference as to the scope of that authorization.

The important distinction is that while the "obtain" interpretation theory may still incorporate extrinsic bodies of law, it limits the influence of that extrinsic law based on the words of the CFAA itself. The CFAA would not be violated every time people exceed the access authorized by their employment contracts or agency relationships. Rather, insiders would only violate the CFAA by obtaining or altering information that their agency or contracts did not *so entitle them to obtain or alter*.

Of course, because of the nature of digital information, it is hard to define when information is being merely accessed as opposed to obtained. Nevertheless, using the *Black's Law Dictionary* definition of the word "acquire," it becomes fair to say that information is "obtained" when the user maintains "control over" the information or the ability to access the information even after authorization has expired.[171] For instance, when an employee e-mails proprietary information to a personal e-mail address, he creates a way of accessing the information independent of the access granted by the information owner. This definition is consistent with the

---

[170] *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) (arguing that "[n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer").

[171] *See supra* note 166 and accompanying text.

point raised above that, in terms of digital misappropriation, theft is defined not as the loss of property interest by the true owner, but the illegitimate gain of such an interest by the acquirer.

This definition raises a potential question in regards to a common factual situation: what happens when an employee transmits information to a personal e-mail or computer for the purpose of working from home, but later uses that information for other purposes? The answer, again, lies in the definition of "exceeds authorized access." The prohibition is not merely on "obtaining information" but "obtaining or altering information that the accesser is *not entitled to so* obtain or alter."[172] The use of "so" indicates that the entitlement to obtain or alter can be conditioned.[173] If the employer has imposed no restraint on the information, no violation has occurred. If, however, the employer has made clear that it is the owner of property, and that any "control over" information is allowed only for the purposes of working from home, then the employee is not entitled to control it for other purposes. When the employee pursues other purposes, he asserts control over information in a way that he is not entitled to and thus violates the CFAA.

A potential criticism of the "obtain theory" is that the misappropriation of information may already be actionable. As *Aleynikov* illustrates, though, a federal cause of action is not always available.[174] Further, the information that is worth protecting because of privacy concerns may not reach the level of trade secrets protected by state law.[175] Even if other actions were available, Congress addressed in debate over the CFAA the potential of duplicative liability.[176] Such concerns were dismissed, though, as the statute was passed with the congressional reports noting that while the theft may implicate other rights, under the CFAA "the crux of the offense . . . is the abuse of a computer to obtain the information."[177]

---

[172] 18 U.S.C. § 1030(e)(6) (2012) (emphasis added).

[173] *See* United States v. Nosal, 642 F.3d 781, 785 (9th Cir. 2011), *rev'd*, 676 F.3d 854 (2012) (en banc).

[174] *See* United States v. Aleynikov, 676 F.3d 71, 74 (2d Cir. 2012).

[175] *See generally Personal Data Threat to Millions As Company Hacking Reaches New High*, KPMG (Nov. 12, 2012), http://goo.gl/hHAOFm.

[176] *See* Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 458–59 (1990) ("Witnesses at committee hearings on the need for a federal computer crime statute testified that . . . existing federal statutes could be used to prosecute computer assisted crimes [before the CFAA was passed].").

[177] S. REP. NO. 104-357, at 7–8 (1996).

CONCLUSION

The CFAA is designed to update property protections for the changing conditions of the modern world. Traditional laws of trespass, burglary, and larceny were not sufficient to address issues of computer misuse. Traditional trespass and burglary laws require a physical invasion that simply does not occur in the world of digital trespass. Theft laws, too, are insufficient due to their reliance on the victim's loss of a property right. When digital information is stolen, it is almost always copied and extracted, leaving the original owner with the same information as before the theft.

Congress enacted the Computer Fraud and Abuse Act and its amendments to directly combat the insufficiencies of existing law. Together, they were meant to protect computer owners from threats ranging from hacking, to denial-of-service attacks, to destructive worms or viruses, to information theft. Indeed, information theft is directly mentioned multiple times in the legislative history of both the original 1984 CFAA and its subsequent amendments. Further, Congress drew an explicit distinction in that the Act's legislative history between theft that occurs by outsiders, hacking into systems, and theft that occurs by insiders, abusing their privileges to access information.[178]

It is not only good policy to combat both sorts of misconduct—insider and outsider theft—the CFAA legislative history indicates that combating such misconduct was the intent of the statute. That intent is manifest in the alternative prohibitions on accessing computers "without authorization" or "in excess" of authorization." However, circuit courts have split into two broad camps regarding the exact nature of insider misconduct prohibited by the statute. The narrow interpretation camp maintains that the prohibition only refers to information within a system that an insider does not have explicit authorization to access. To those in the narrow camp, "exceeding authorized access" only occurs when an insider is allowed to access a computer, but hacks into files to which authorization does not extend. The broad interpretation camps maintain that exceeding authorized access refers not just to the situations discussed above, but also to situations in which an employee accesses information that she is authorized to access but does so for purposes that violate her authorization.

The broad interpretation contains two subsets: agency theory and contract theory. Agency theory maintains that when an agent acts upon interests adverse to her principal, the authorization associated with the principal–agent relationship is revoked. Contract theory maintains that the scope of employees' authorization can be, and is, limited by the defined

---

[178] *See supra* note 137 and accompanying text.

prohibitions in their contracts. If employees access information in violation of those contract provisions, their access is unauthorized and violates the CFAA.

The narrow and broad interpretations each have their advantages. The narrow interpretation creates a bright-line rule to easily identify prohibited conduct, and relies on the text of the statute, rather than any extrinsic law, for its basis. The broad interpretation and both of its supporting theories seem to better cover the spirit of the law, but extend liability beyond improper access to misuse (or abuse) of information. These theories extend liability to insider theft of information that employees have permission to access, which reaches a result seemingly consistent with the legislative history and intent.

All three of these approaches also have drawbacks. The narrow theory does not extend to situations that the CFAA is intended to cover. Under that theory, as long as an accesser has permission to access a specific piece of information, no action taken with that information violates the CFAA. In contrast, the broad theories both have little grounding in statutory text and are potentially dangerous due to their abilities to be overly broad.

A novel approach, however, is consistent with the text of the statute, extending liability to insider theft without posing the potential of overbroad prosecution. Without utilizing extrinsic principles, the very text of the statute identifies two specific improper uses—"obtaining" or "altering" information in a way that is not entitled. If the term "obtain" were given its plain meaning of "acquisition," then the CFAA by its terms would indeed extend criminal liability for insider theft. This approach is consistent with the purposes of computer misuse statutes as it resolves the difficulties relating to victims' lost property interests. Instead of focusing on the owner's deprived property interest, it focuses on the thief, who acquires something to which he is not entitled.

Not only is this interpretation consistent with the policy goals behind computer misuse statutes. It is also consistent with the specific legislative history of the CFAA. That history identifies theft and insider theft as a concern with which the Act is addressed. Like the broader theories, the "obtain" theory extends coverage to such conduct. Unlike those theories, however, it does not pose the potential of overbroad applications because it specifically limits liability to the two enumerated misuses: unentitled "altering" and "obtaining."