THE COMPUTER FRAUD
AND ABUSE ACT: HACKING INTO
THE AUTHORIZATION DEBATE

Alden Anderson*

ABSTRACT: The Computer Fraud and Abuse Act (CFAA) makes it a federal crime for a person to intentionally access a computer without authorization or to exceed authorized access and thereby obtain information from any protected computer. The CFAA also provides civil remedies against individuals who violate the Act. While the Act broadly defines what constitutes exceeding authorized access, it does not define authorization. Although the CFAA was originally passed to criminalize computer hacking, employers have recently used the CFAA’s vague language to contend that employees who misuse employer information violate the Act. This has created a split among the Circuit Courts over whether an employee who misuses employer information pursuant to authorized physical computer access “accesses a computer without authorization” or “exceeds authorized access” and can thus be prosecuted or held liable for civil damages under the Act. This article examines those competing interpretations and argues that permitting employers to bring misappropriation claims under the Act is inconsistent with the CFAA’s legislative history and basic propositions of federalism. Specifically, allegations that an employee misused an employer’s information are often based on trade secret violation claims and claims that the employee breached his employment contract or duty of loyalty. These are state claims and an employer should not be permitted to use the CFAA’s ambiguous language to pursue them in federal court under a substantially lower burden of proof than state and federal statutes that address these specific claims. This article proposes that Congress should amend the CFAA so courts know it creates criminal and civil liability for unauthorized computer access that is the result of employee computer hacking and not simply for using information in a way that is contrary to the employer’s interests. Alternatively, the judiciary should not permit employers to use the CFAA to bring these claims into federal court.


*J.D. Candidate, Sandra Day O’Connor College of Law, Arizona State University; B.A., 2010, magna cum laude, Government, University of Texas at Austin. The author thanks Professor Dennis S. Karjala for his thoughtful comments and suggestions during the writing of this work.
In the 1970s, few people could have imagined the impact that computers would have today in the way people do business and communicate.¹ In just a few decades, computers have evolved and now play a vital role in our daily lives. By 2008, there were over one billion personal computers in use around the world and that number is expected to double by 2014.² While computers undoubtedly have simplified our lives in some respects, they have also created an avenue for widespread crime. From 2009 to 2011, there was a seventeen-fold increase in computer attacks on American infrastructure.³ These attacks were initiated by criminal gangs, computer hackers and even foreign governments.⁴ For example, both the New York Times and The Wall Street Journal have been victims of computer hacking traced back to China.⁵ The depth of the attack imposed on the New York Times had the potential to completely destroy its entire computer network.⁶ However, cyber attacks are not limited to news media outlets. General Keith Alexander, the director of the National Security Agency, stated that cyber attacks are “causing ‘the greatest transfer of wealth in history’” and estimated that the global cost of cyber crimes is $1 trillion.⁷

Congress first addressed the need to criminalize cyber attacks by passing the Computer Fraud and Abuse Act (CFAA) in 1984.⁸ The Act was later amended to provide civil actions to those who have suffered damage or loss as a result of one of the crimes listed in the statute. While it is not difficult to conclude that a person who hacks into a computer system and steals information is a criminal under the Act, a dispute among circuit courts has arisen about whether an employee who has been given permission to access an employer’s data could also be subjected to civil and criminal liability under the Act if he uses the information in a way that is contrary to the employer’s interest.

This comment will argue that the CFAA was created to criminalize computer hacking, and courts that permit employers to bring misappropriation claims under the CFAA are fundamentally misapplying its provisions. The comment is divided in three Parts. Part I discusses the CFAA’s broad language that has led to a circuit split and outlines the competing approaches about

---

4. Id.
6. Id.
8. Booms, supra note 1, at 545.
whether employers can bring misappropriation claims under the statute. Part II argues that an interpretation that permits employers to bring misappropriation claims under the CFAA is flawed. Part III proposes ways in which Congress or the judiciary could solve the dispute by clarifying that the CFAA should only be used to impute civil and criminal liability on computer hackers.

I. BACKGROUND INFORMATION
AND ANALYZING THE CIRCUIT SPLIT

A. CFAA Provisions

The CFAA is a predominately criminal statute that establishes seven computer crimes in seven subsections. These crimes include accessing a computer “without authorization” or “exceeding authorized access” to obtain information that requires protection from disclosure for reasons of national defense or foreign relations; accessing a computer without authorization or exceeding authorization to obtain government, credit or financial information; accessing a nonpublic government computer without authorization; transmitting a program, information, code or command that causes damage without authorization to a protected computer; trafficking in passwords through which a computer may be accessed without authorization if the trafficking affects interstate or foreign commerce or if the computer is a government computer; and transmitting any communication in interstate or foreign commerce containing a threat to damage a protected computer. Its broadest provision criminalizes “whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer.” The statute also permits those who suffer damage or loss by someone who commits one of the crimes listed in the Act to bring a civil action against the violator in certain circumstances. In recent years, employers have used this provision of the CFAA to bring suit against employees who misappropriate the employers’ computer data. The circuit courts are currently split over whether such claims are cognizable under the CFAA. Specifically, the circuits are divided about what constitutes accessing a computer without authorization and exceeding authorized access.

Although the phrase “without authorization” appears ten times throughout the CFAA, Congress has failed to provide a definition of authorization. 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 com-

10. Id. § 1030(a)(2).
11. Id. § 1030(a)(2)(A)–(B).
12. Id. § 1030(a)(5)(A).
13. Id. § 1030(a)(6).
14. Id. § 1030(a)(7).
15. Id. § 1030(a)(2)(C).
16. Id. § 1030(g).
puter that the accessor is not entitled so to obtain or alter.”

Courts have determined that this term can be interpreted two ways. It could refer to an employee who is authorized to access specific data but accesses unauthorized data by hacking an employer’s computer. Under this narrow view, an employee would exceed authorized access by looking at his employer’s customer lists when he is only permitted to review his employer’s product information. The Ninth and Fourth Circuits have adopted this approach. Alternatively, the term could refer to an employee who has unrestricted physical access to a computer, but is limited in the way that he can use the computer’s data. Under this broader view, an employee exceeds authorized access when he is authorized to access customer lists solely to do his job, but then sends them to a competitor. The Fifth and Seventh Circuits have adopted a version of this approach and move a step further by contending that this action would have been without authorization. The significance of this split cannot be overstated. An employer in a jurisdiction that adopts the broader view can bring federal CFAA claims against his employees for misappropriation of information regardless of whether the misappropriation would trigger liability under state trade secret laws. Moreover, an employee in such a jurisdiction would be subject to criminal liability while an employee in a jurisdiction that adopts the narrow approach could misappropriate the same employer’s information without being subjected to either criminal or civil liability under the CFAA. This article argues that courts should uniformly adopt the narrow approach. However, it is imperative to first examine both views to fully understand the nature of the current circuit split.

B. Analyzing the Circuit Split

Competing court interpretations over whether an employee acts without authorization or exceeds authorized access when he misappropriates his employer’s computer data have led to a clear circuit split over the meaning and application of CFAA criminal and civil provisions. The Ninth and Fourth Circuits have interpreted these terms narrowly, concluding that an employee cannot be held civilly or criminally liable unless he hacked into his employer’s

---

17. Id. § 1030(e)(6).
18. United States v. Nosal, 676 F.3d. 854, 856–57 (9th Cir. 2012). A hacker is “a person who illegally gains access to and sometimes tampers with information in a computer system.” MERRIAM WEBSTER’S COLLEGIATE DICTIONARY 559 (11th ed. 2006). While hacking refers to many activities, it includes “breaking passwords; creating ‘logic bombs;’ e-mail bombs; denial of service attacks; writing and releasing viruses and worms; viewing restricted, electronically-stored information owned by others; URL redirection; adulterating Web sites; or any other behavior that involves accessing a computing system without appropriate authorization.” Peter T. Leeson & Christopher J. Coyne, The Economics of Computer Hacking, 1 J.L. Econ & Pol’y 511, 514 (2005).
19. Nosal, 676 F.3d. at 857.
20. Id.
21. Id.
22. See Int’l Airport Centers v. Citrin, 440 F.3d. 418 (7th Cir. 2006); United States v. John, 597 F.3d 263 (5th Cir. 2010).
computer system. Conversely, the Fifth and Seventh Circuits have interpreted the CFAA more broadly and have concluded that an employee can be held liable for misusing an employer’s information. While both the Fifth and Seventh Circuits ultimately reach this conclusion, they rely on different reasoning to arrive at that result. The Seventh Circuit relies on the law of agency to conclude that an employee accesses his employer’s computer data without authorization when he violates his duty of loyalty to his employer. The Fifth Circuit has concluded that an employee who accesses the data with the employer’s permission acts without authorization if he violates one of his employer’s policies. The circuit split and key court opinions are outlined below.

C. Narrow Approach

The Ninth Circuit has adopted the view that an employee exceeds authorized access by hacking an employer’s computer. In United States v. Nosal, David Nosal, a former Korn/Ferry employee, left the company and convinced his former colleagues to use their login credentials to download information from a confidential Korn/Ferry database on the company’s computer and to transfer the information to Nosal to help him start a competing business. Although the employees were authorized to access the database, Korn/Ferry had a policy that employees were not permitted to disclose this information. The government indicted Nosal for trade secret theft, mail fraud, conspiracy and a violation of the CFAA under 18 U.S.C. § 1030(a)(4) for aiding and abetting the Korn/Ferry employees in exceeding their authorized access with intent to defraud. The government argued that the employees exceeded authorized access of Korn/Ferry’s computer data by violating the company’s computer use policy. The court rejected this argument and held that the phrase “exceeds authorized access” is limited to violations of restrictions on access to information, not restrictions on use. The court reasoned that the government’s broad interpretation would alter the CFAA “from an anti-hacking statute to an expansive misappropriation statute” and would criminalize any unauthorized use of information obtained from a computer.

The court noted that this interpretation would make criminals of large groups of people who had little reason to suspect they had committed a federal crime and that Congress unlikely intended to criminalize “conduct beyond that

---

24. See Citrin, 440 F.3d. 418; John, 597 F.3d 263.
25. See Citrin, 440 F.3d. 418.
26. See John, 597 F.3d 263.
27. Nosal, 676 F.3d. at 863.
28. Id. at 856.
29. Id.
30. Id.
31. Id. at 857.
32. Id. at 863–64.
33. Id. at 857–59.
which is inherently wrongful, such as breaking into a computer.”\textsuperscript{34} Specifically, the court examined § 1030(a)(2)(c), which makes it a crime to exceed authorized access to a computer connected to the Internet, and determined that the government’s proposal of basing criminal liability on violations of private computer use policies can “transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.”\textsuperscript{35} The court noted that most employers have computer-use policies that prohibit activities such as g-chatting with friends, playing games, shopping or watching sports highlights.\textsuperscript{36} Employees are seldom disciplined for occasional personal use of work computers, but under the government’s broad interpretation of the CFAA, these activities would become federal crimes.\textsuperscript{37} The court applied the rule of lenity to conclude that if Congress wanted to incorporate misappropriation liability into the CFAA, it should have done so more clearly in the Act.\textsuperscript{38}

The Fourth Circuit has also adopted the view that an employee only exceeds authorized access by hacking. In \textit{WEC Carolina Energy Solutions v. Miller}, Mike Miller and Emily Kelly, former WEC Carolina Energy Solutions, Inc. (WEC) employees, were accused of downloading WEC’s confidential documents and emailing them to Miller’s personal email address and of downloading confidential information to a personal computer.\textsuperscript{39} After leaving WEC, Miller allegedly used this information to make a presentation on behalf of Arc, a competing company.\textsuperscript{40} WEC claimed that Miller and Kelly violated the CFAA because they violated WEC policies that forbade them from downloading confidential and proprietary information to a personal computer.\textsuperscript{41} WEC argued that the defendants breached their fiduciary duties to WEC and as a consequence of the breach, they either acted with no authorization or exceeded their authorization when they accessed the information.\textsuperscript{42} The court rejected these claims and held that the terms “without authorization” and “exceeds authorized access” only apply when a person accesses a computer without permission or obtains or alters information on a computer beyond what he is authorized to access.\textsuperscript{43} In adopting these definitions, the court rejected the proposition that an employee who uses his computer access for a purpose that diverges from his employer’s interest could be held liable under the CFAA based on a cessation-of agency theory.\textsuperscript{44}

\textsuperscript{34} Id. at 859.
\textsuperscript{35} Id. at 860.
\textsuperscript{36} Id.
\textsuperscript{37} Id.
\textsuperscript{38} Id. at 863.
\textsuperscript{39} 687 F.3d 199, 202 (4th Cir. 2012).
\textsuperscript{40} Id.
\textsuperscript{41} Id.
\textsuperscript{42} Id.
\textsuperscript{43} Id. at 206.
\textsuperscript{44} Id. (The court specifically rejected a rule that revokes authorization when an employee uses his access for a purpose contrary to the employer’s interest because such a rule could impose liability on an employee who posted a Facebook status or checked the score of a sporting event in violation of his employer’s use policy. Under this interpretation, the employee’s agency relationship would cease and he would be left without authorization to access his computer).
D. Broad Approach

While the Fourth Circuit explicitly rejected the argument that an employee can access computer information without authorization or exceed authorized access by breaching a duty to an employer under the law of agency, the Seventh Circuit has concluded that such a breach is grounds for liability under the CFAA. In direct opposition to the Ninth Circuit’s position, the Fifth Circuit has held that an employee’s violation of an employer’s policy can form a basis for liability under the CFAA. These broader approaches are discussed below.

1. Agency Interpretation

Courts adopting the agency-based approach determine whether computer access was authorized under the CFAA through the use of agency principles. The Seventh Circuit adopted this approach in International Airport Centers v. Citrin. In Citrin, International Airport Centers (IAC) lent Citrin a laptop to use in the scope of his employment at IAC. Citrin later decided to quit his job at IAC to start his own business, in breach of his employment contract. Before returning the laptop to IAC, he deleted data he had collected related to his work at IAC, and data that would have revealed to IAC that he had engaged in improper conduct before he decided to quit. Citrin also used a secure-erasure program to prevent IAC from recovering these files. The court considered whether Citrin had accessed his computer without authorization when he deleted the files and held that Citrin’s authorization to access his laptop ended when he violated the duty of loyalty imposed on employees by agency law.

2. Employer-Policy Approach

Courts adopting this approach have determined that an employee can exceed authorized access or act without authorization by using computers in ways that violate an employer’s policy. The Fifth Circuit adopted this approach in United States v. John. In John, Eva Lavon John worked at Citigroup as an account manager and had access to Citigroup’s internal computer system and the customer account information it contained. John later provided this information to her half-brother and others who used the infor-

45. Id.
46. Int’l Airport Centers v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).
47. United States v. Nosal, 676 F.3d. 854, 860 (9th Cir. 2012).
48. United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).
50. Citrin, 440 F.3d at 419.
51. Id.
52. Id.
53. Id.
54. Id. at 420.
55. 597 F.3d 263 (5th Cir. 2010).
56. Id. at 269.
mation to incur fraudulent charges on Citigroup customer accounts. John found John guilty of exceeding authorized access to a protected computer in violation of 1030(a)(2)(A) and (C). John challenged these convictions on the ground that the statute does not prohibit the unlawful use of material that she was authorized to access through the authorized use of the computer. The court held that “authorized access” and “authorization” can place limits on the use of information obtained by permitted access to a computer system and data available on that system “when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.” Although the court’s holding seems to be limited to when an employee misuses information to further a crime, the court emphasized that John’s use of Citigroup’s computer system to perpetrate the fraud violated Citigroup employment policies. Moreover, the court noted that the First Circuit has held that “an employment agreement can establish the parameters of authorized access.”

II. BROADER MISUSE THEORY IS FLAWED

Although the Fifth and Seventh Circuits’ approaches may appeal to many courts because they punished employees in Citrin and John who undoubtedly wronged their employers, these courts’ definitions of what constitutes authorization and exceeding authorized access consider only the specific facts presented in those cases without considering the implications that these broader views will have on future litigants. Moreover, these approaches fail to consider Congress’s original intent in passing the CFAA. I contend that the broader view these circuits adopted is flawed for three reasons. First, the fact that Congress passed the CFAA to criminalize computer hacking and made subsequent amendments to the Act suggests that Congress has remained concerned with computer hacking and with developing new ways to combat it. Second, the broader view is inconsistent with basic tenets of federalism because it permits employers to use the CFAA to bring employment law and trade secret claims traditionally governed by state law into federal courts. Third, this interpretation permits employers to use the CFAA’s broad language to bring claims likened to trade secret misappropriation claims against their employees under a substantially lower burden of proof than what is required by state and federal trade secret statutes.

57. Id.
58. Id. at 270. (These provisions make it a crime to intentionally access a computer without authorization or exceed authorized access and thereby obtain: “information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),” or “information from any protected computer,” respectively. 18 U.S.C. § 1030(a)(2)(A), (C) (2012).)
59. John, 597 F.3d at 271.
60. Id. at 271–72.
61. Id. at 272.
A. Legislative History

The CFAA’s legislative history suggests that Congress passed the Act specifically to address computer hacking. Before Congress passed the CFAA, there was no federal legislation that addressed computer crimes. With the evolution of computer technology progressing faster than Congress could act, charges for computer crimes could only be brought under statutes that were designed for other offenses, such as mail fraud or wire fraud statutes. What would later become the CFAA was passed in 1984 in response to the publication of a number of computer crime studies and an increase in the number of media reports of juvenile computer hacking. In a 1984 House Report, Congress specifically addressed this concern:

Compounding this is the advent of activities of so-called ‘hackers’ who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results. The relative ease of access by a hacker is due to a corresponding proliferation of computer networking which began during the 1970’s.

The fact that Congress equated “access” to “trespass” further suggests that it did not intend for rogue employees who were initially given permission to access an employer’s data to be considered “without authorization” under the Act. To trespass is to “enter unlawfully upon the land of another” and the act of “hacking” into a computer is more analogous to unlawful entry than misuse of computer information. In 1986, the Act was substantially amended and Congress introduced the phrase “exceeds authorized access” to replace the phrase “or having accessed a computer with authorization, uses the opportunity such access provides for purposes which such authorization does not extend.” Before this amendment, the Act’s plain meaning would likely have extended liability to an employee who misuses his employer’s data he was authorized to access because in doing so he used it “for purposes which such authorization does not extend.” While it is plausible that Congress amended the Act simply to provide a more condensed version of the Act’s language with the intent of retaining its original meaning, it is more probable that Congress amended the Act with the express purpose of preventing employers from bringing misuse of information claims under the CFAA. One of the purposes for this amendment was to shield federal employees from “murkier grounds of liability” based on their access to computer data. Specifically, the Committee on the Judiciary expressed that it did not want the statute to criminalize employee misuse of information:

63. Id.
65. MERRIAM WEBSTER’S COLLEGIATE DICTIONARY 1334 (11th ed. 2006).
66. Id. at 2494–95.
The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct.\footnote{Id. at 2485 (emphasis added).}

Congress undoubtedly realized that a government employee’s misuse of government data was “wrong,” but it did not intend to make this act a crime. Currently the CFAA has four provisions that specifically protect government computer data.\footnote{18 U.S.C. §§ 1030(a)(1), (2), (3) and (6) (2012).} Given this emphasis on protecting government information, the broader view is inconsistent with congressional intent because Congress unlikely intended to criminalize employee misuse of information in the private sector if it did not want to do so in the public sector.


[Insiders, who are authorized to access a computer, face liability only if they intend to cause damage to a computer, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for intentional, reckless, or other damage they cause by their trespass.\footnote{Id.}]

Thus, Congress likely intended to impute liability on rogue employees only if they intentionally damaged their employer’s computer. The CFAA defines “damage” as “any impairment to the integrity or availability of data, a program, a system or information.”\footnote{18 U.S.C. §1030(e)(8) (2012).} Simply misusing an employer’s information does not satisfy this definition.

The narrow approach has also been supported by other recent congressional research. In 2012, Charles Doyle released a Congressional Research Report that provides an overview of the CFAA and the meaning of each of its provisions.\footnote{Charles Doyle, CONG. RESEARCH SERV., RS20830, CYBERCRIME: AN OVERVIEW OF THE FEDERAL COMPUTER FRAUD AND ABUSE STATUTE AND RELATED FEDERAL CRIMINAL LAWS (2012).} He noted that some courts have adopted the broader approach.\footnote{Id. at 15–16.}
but maintains that the CFAA is a cybersecurity law that protects federal computers, bank computers, and computers connected to the Internet from hacking.\(^78\)

**B. The Broader Approach Violates Basic Tenants of Federalism**

The American court system relies on a division of power between state and federal courts. Federal court jurisdiction is limited to cases that raise a federal question\(^79\) or present diversity of citizenship.\(^80\) While federal courts have jurisdiction over some employment disputes,\(^81\) many labor and employment cases are heard by state courts. For example, each state has its own laws concerning employment compensation, hours and other work conditions.\(^82\) Because there are also federal employment laws, courts must acknowledge the role of judicial federalism, which is concerned with the sharing of judicial power by federal and state court systems over the same land and people.\(^83\) Michael E. Solimine and James L. Walker, professors at University of Cincinnati College of Law and Wright State University, respectively, contend, “judicial federalism is essential to the health, and even to the existence of a successful system of power sharing, and it has been consistently undervalued in that role.”\(^84\)

Because the CFAA is a federal statute, litigants can pursue their claims in federal court. However, the CFAA should not be used as a catalyst for employers to get into federal court to pursue claims that should otherwise be heard by state courts. Under 28 USC § 1367(a), plaintiffs who present a claim that raises a federal question may ask a federal court to exercise subject-matter jurisdiction over a state law claim that forms “part of the same case or controversy” as the plaintiff’s federal claim.\(^85\) There is evidence that employers are taking advantage of the CFAA to pursue their state claims in federal court. For example, in *WEC Carolina Energy Solutions*, the employer pursued nine state-law causes of action, including conversion, tortious interference with contractual relations, civil conspiracy, and misappropriation of trade secrets against the defendant.\(^86\) Because there was no diversity jurisdiction, the employer’s CFAA claim served as the sole basis for federal jurisdiction.

The division of power between federal and state courts is unnecessarily blurred when employers use the CFAA to pursue claims that fall within the subject matter jurisdiction traditionally allocated to state courts. When em-

---

78. *Id.* at 2.
84. *Id.* at 6.
86. Miller, 687 F.3d at 202, 207 n.4.
Employers bring causes of action against their employees under the CFAA, they are often related to the employee’s breach of a fiduciary duty after they misuse information they were authorized to access. For example, the defendant in Citrin undoubtedly was authorized to access his employer’s laptop; it was given to him to perform his job. While his company may not have authorized him to “misuse” the data on the laptop, this lack of authorization is outside the scope of employer protections afforded by the CFAA because the defendant was given proper access to the data. As noted previously, at the heart of the Seventh Circuit’s analysis in this case is that Citrin violated a duty of loyalty to his employer. Employees in positions of trust owe a common law fiduciary duty of loyalty to their employers while they are employed.87 This duty usually arises under state law. While a breach of a duty of loyalty claim is certainly one that employers should feel empowered to pursue in state court, there is no reason that this claim and other related state employment law claims should be brought into federal court under the CFAA absent proof that the employee hacked his employer’s computer data.

State courts have a legitimate interest in overseeing employment disputes between state citizens. Permitting states to make decisions on matters over which they have general jurisdiction preserves the ability of local governments to act independently.88 This is key because state courts serve the important purpose of making law and policy and serving as “legal entrepreneurs and as teachers to the community.”89 There is no evidence that state courts are incapable of adequately resolving disputes concerning employee misuse of information when there is no diversity of citizenship. In fact, state courts are better suited to resolve such disputes. If one accepts the basic principle of federalism, it follows that a federal official should not be permitted to interpret federal law in a way that infringes on a state’s power to regulate in areas traditionally reserved to the state.90

Additionally, federal courts have an interest in using their resources to hear cases that truly raise a federal question. In 1995, the Judicial Conference of the United States met to discuss a long-range plan for the federal courts.91 It made the following observation:

If federal courts were to begin exercising, in the normal course, the broad range of subject-matter jurisdiction traditionally allocated to the states, they would lose both their distinctive nature and, due to burgeoning dockets, their ability to resolve fairly and efficiently those cases of clear national import and interest that properly fall within the scope of federal concern.92

88. SOLIMINE & WALKER, supra note 83, at 139.
89. Id.
92. Id. at 21–22.
If federal courts continue to permit employers to litigate disputes over employee misuse of information under the CFAA, they will be less able to dedicate their resources to hearing cases that truly should be resolved by federal courts. Federal courts should be left to deal with cases that concern diverse litigants and interstate activity. The narrow approach is more consistent with the principles espoused in judicial federalism and with Congress’s motive for passing the CFAA. When the Committee on the Judiciary first recommended that the CFAA should be amended in 1986, it explained:

Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead 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. The Committee is convinced that this approach strikes the appropriate balance between the Federal Government’s interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.  

This balance between the federal and state governments is best achieved by adopting the narrow approach taken by the Ninth and Fourth circuits because it effectively keeps state employment claims out of federal court while allowing litigants to use the CFAA to pursue computer hacking claims. Conversely, the broader views adopted by the Seventh and Fifth Circuits permit employers to use the CFAA simply to get state employment law claims into federal court. This approach violates basic tenets of federalism by disturbing the traditional balance of power between state and federal courts.

C. This Interpretation Would Lower an Employer’s Burden of Proof for Claims Against Employees

The broadest provision of the CFAA makes guilty of a crime “whoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer.” The Act defines a protected computer 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.” Arguably, any computer connected to the Internet satisfies this definition.

An interpretation that an employee who misuses employer information violates the CFAA permits employers to bring trade secret theft and misappropriation claims against rogue employees without having to satisfy the elements

---

Anderson

outlined in state statutes that specifically address these claims. Unless Congress has expressly indicated an intent to federalize and displace these kinds of claims by establishing less stringent standards, one should assume that Congress intended to leave the state regulations where they were at the time the legislation was adopted.

1. Trade Secret & Misappropriation Elements

Including employee misuse of information within the scope of activities in which an employee acts without authorization or exceeds authorized access under the CFAA allows employers to pursue potential trade secret claims that lack “virtually all of the policy and procedural safeguards built into trade secret law.”

Because the evidentiary requirements and elements of proof set forth in a § 1030(a)(2)(C) claim, which only requires proof an individual (1) accessed a computer without authorization or exceeded authorized access and (2) obtained information from any protected computer, are substantially lower than a trade secret misappropriation claim, employers can use the CFAA to enhance their chances of recovering against rogue employees. An employee’s duty to not share trade secrets arises from the common law and from state statutes. Most states have enacted statutes that provide civil remedies for the misappropriation of trade secrets. Many of these statutes are based on the Uniform Trade Secrets Act (UTSA).

The UTSA defines a trade secret as:

Information, including a formula, pattern, compilation, program, device, method or technique that: 1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and 2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Interpreting the CFAA as a federal trade secret statute permits employers to sidestep obstacles and limitations imposed by state trade secret statutes. For example, an employer in Illinois suing a former employee for trade secret misappropriation under the CFAA could evade three obstacles presented by the Illinois Trade Secret Act (ITSA) for the same claim. Under the ITSA, the employer would be required to prove that the employee stole information that constitutes a legally protected trade secret. Under the CFAA, the same employer is only required to prove that the information was housed on a

96. Brenton, supra note 64, at 430.
97. Id. at 440.
98. ROTHSTEIN ET AL., supra note 87, at 807.
100. ROTHSTEIN ET AL., supra note 87, at 807.
101. Id.
103. Id. at 6–7.
The Computer Fraud and Abuse Act

protected computer. Second, the ITSA requires an employer to prove that he took reasonable steps to protect the secrecy of the information at issue while the CFAA only requires the employer to prove that the employee accessed the information without authorization or by exceeding his authorization. Like other states that have codified provisions of the UTSA, Illinois defines misappropriation as:

(i) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or (ii) disclosure or use of a trade secret of another without express or implied consent by a person who

(A) used improper means to acquire knowledge of the trade secret; or
(B) at the time of disclosure or use knew or had reason to know that his knowledge of the trade secret was

(I) derived from or through a person who has utilized improper means to acquire it;
(II) acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or
(III) derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use; or
(C) before a material change of his position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.

The CFAA does not require proof of misappropriation and an employer must only show that his employee accessed the information and that the access caused damage, which the Act defines as “any impairment to the integrity or availability of data, a program, a system or information.”

If the Fifth and Seventh Circuits’ approaches are adopted, employers will be able to sue employees under the CFAA for claims likened to state trade secret theft claims without being required to prove that an employee actually misappropriated information. For example, if access is determined by an employee’s agency with the employer and is terminated when an employee violates a duty of loyalty, as suggested by the Seventh Circuit, an employer will be able to prevail on a claim under 18 USC § 1030(a)(2)(C) simply by proving that the employee obtained the employer’s information after he violated his duty of loyalty. This burden of proof is substantially lower than the requirement to prove a breach of a duty to maintain secrecy under the UTSA, ILCS and other state trade secret laws, and provides an unfair advantage to employ-

104. Id.
105. Id. at 7.
106. ILL. COMP. STAT. 1065/2(a) (2012).
107. Winters & Costello, supra note 102, at 7.
108. 18 U.S.C. §1030(e)(8) (2012). Even if an employer successfully brings a claim into federal court under the CFAA without being able to prove that he suffered damages as a result of his employee’s access to his computer data, there are policy reasons for not permitting these claims to be brought into federal court. The additional costs imposed by using the federal court system will likely put additional pressure of defendants to settle disputes that could otherwise be litigated in state courts at a substantially lower cost.
ers when pursuing claims against their employees or at the very least changes the balance drawn by the states in these disputes between employers and employees.

III. SOLUTIONS

Because courts have already mistakenly applied the broader approach to resolve CFAA disputes, it is imperative for Congress to intervene. Congress should amend the CFAA so that courts know that the statute is an anti-hacking statute and was not intended to impute criminal or civil liability on an employee who misuses his employer’s information. Specifically, Congress should provide a definition of “authorization” and amend the current definition of “exceeds authorized access.” Alternatively, Congress should amend the statute to specifically note that the CFAA cannot be used to pursue misappropriation claims. In the event that Congress does not amend the CFAA, the judiciary should uniformly adopt the narrow approach.

A. Congress Should Amend the CFAA

In response to Aaron Swartz’s suicide purportedly linked to his prosecution under the CFAA for downloading millions of academic articles from the JSTOR subscription service, Representative Zoe Lofgren and Senator Ron Wyden have proposed amendments to the CFAA. These amendments, collectively known as Aaron’s Law, exclude breaches of terms of service and user agreements from the scope of the CFAA and also attempt to define unauthorized access “to make a clear distinction between criminal hacking activity” from “acts that exceed authorized access on a minor level.” However, Congress is unlikely to make Aaron’s law a priority because both the House and Senate Judiciary committees are largely focused on issues such as immigration and gun control. Moreover, it’s unclear if the President would support such legislation. The Obama administration tried to expand the scope of the CFAA as part of its 2011 proposal on cybersecurity reform.

However, Aaron’s law is not the only proposed amendment to the CFAA. In wake of the recent circuit split, the Senate Judiciary committee took a crucial step towards narrowing the scope of the CFAA by approving S1551: The Personal Data Privacy and Security Act of 2011. The bill proposes to amend the definition of “exceeding authorized access” as follows:

Section 1030(e)(6) of title 18, United States Code, is amended by striking ‘alter;’ and inserting ‘alter, but does not include access in violation of a contractual obligation or agreement, such as an acceptable use policy or terms of

110. Id.
112. Id.
The Computer Fraud and Abuse Act

service agreement, with an Internet service provider, Internet website, or non-
government employer, if such violation constitutes the sole basis for deter-
mining that access to a protected computer is unauthorized. This amendment would prevent employers from using the CFAA to bring breach of contract suits against an employee in federal court under the guise that the employee exceeded authorized access. It would also prevent courts from adopting the employer-policy approach that the Fifth Circuit advocated in United States v. John. However, it does not address what constitutes authorization under the CFAA and would permit courts to define authorization based on agency law to determine that an employee acts without authorization by violating a duty of loyalty as proposed by the Seventh Circuit in Citrin. Thus, an amendment to the CFAA must include a definition of “authorization” and a clearer definition of “exceeds authorized access” than the one proposed by the Senate Judiciary committee.

Kyle W. Brenton’s proposal for how Congress should define the term “authorization” in the CFAA has merit. In 2009, he proposed that Congress should define authorization as “permitted physical access to a computer or code-based technological permission (such as a username and password) to use a computer, either in person or remotely.” His proposed definition would prevent courts from adopting the view that an employee accesses a computer without authorization as soon as he violates a duty of loyalty to his employer. However, Brenton’s proposal does not completely eliminate the possibility that an employer could use the CFAA to recover for a misappropriation of information claim. For example, an employer could contend that an employee who accesses information with authorization under Brenton’s definition could still exceed authorized access under the current CFAA definition by misusing information in a way that the employee “is not entitled” to do so under an employment agreement. Thus, in addition to adopting Brenton’s proposed amendment, Congress should amend 18 USC §1030(e)(6) to provide:

The term “exceeds authorized access” means to access a computer with authorization and to use such access to obtain or alter information in the computer that the acceser is not entitled so to obtain or alter. A person does not exceed authorized access by misappropriating information he accessed with authorization as defined in this subsection.

Alternatively, Congress could amend the CFAA provision that addresses the requirements for raising civil actions under the statute to specify that an employer cannot bring civil claims against an employee for misuse of the employer’s information. This would be consistent with the statutory scheme because the CFAA already contains provisions that specify that certain claims

114. Brenton, supra note 64, at 460.
115. Id.
Anderson

cannot be brought under the Act. For example, § 1030(g) provides that “[n]o action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.” Thus, Congress should amend § 1030(g) so that the last sentences provides, “No action may be brought under this subsection for the misappropriation of information that a person accessed with authorization within the meaning of this Act.”

These proposed amendments solve the problems created the broader approach. First, they will prevent employers from bringing state employment law and trade secret claims into federal court and thus, will help reinstate the appropriate division of power between state and federal courts. This will effectively allow state courts to resolve disputes between their citizens and permit federal courts to use their resources to resolve matters that involve interstate computer hacking. As a consequence, these amendments will also prevent employers from using the CFAA to pursue claims against their employees under a substantially lower burden of proof than what is required by state trade secret statutes. Lastly, these amendments will help bring clarity to the courts by giving them clear definitions of what constitutes authorization and exceeding authorized access and what makes the CFAA provisions consistent with the legislature’s original intent to criminalize computer hacking.

Those opposed to such amendments might argue that they would prevent employers from recovering against their rogue employees for valid claims. However, employers can still pursue their trade secret claims in state courts. Moreover, employees can also be punished criminally for misappropriating trade secrets in federal court under 18 U.S.C. § 1832. In fact, many of the employees who are sued for misappropriation of information under the CFAA are also charged with an 18 USC §1832 violation. For example, at the time that the Ninth Circuit dismissed the CFAA claims against Nosal, the government had also charged Nosal with violating 18 USC § 1832(a) and the charge was still pending. These proposed amendments do not prevent employers from recovering on valid misappropriation claims; they simply require them to seek recourse under state and federal statutes that specifically address these claims and outline the appropriate burden of proof an employer must carry to prevail.

B. Courts Should Adopt the Narrow Approach

If Congress does not amend the CFAA, the judiciary should adopt the narrow approach when deciding cases under the Act. Although the Fourth

117. Id. at 1030(g).
118. Nosal, 676 F.3d at 867 n.3.
and Ninth Circuits have already adopted this approach, there will continue to be inconsistency in how courts apply provisions of the CFAA to employment disputes if the other circuits do not also adopt the narrow approach. Arguably the best judicial means to resolve a circuit split is for the Supreme Court to issue a ruling on the dispute. However, this issue has not reached the Supreme Court and may not be presented to the Supreme Court in the immediate future because the U.S. Solicitor General chose to not appeal the Ninth Circuit’s decision in United States v. Nosal.\(^{120}\)

If the courts rejected the broader interpretations advocated by the Fifth and Seventh Circuits in favor of the narrow interpretation proposed by both the Fourth and Ninth circuits, the results would be similar to those created by a congressional amendment to the CFAA. First, it would demonstrate the judiciary’s deference to legislative intent by supporting a narrow view that is consistent with the CFAA’s legislative history. Second, it would help restore balance between state and federal courts by preventing employers from using the CFAA to bring state trade secret and employment law claims in federal court. Lastly, it would prevent employers from using the CFAA’s ambiguous language to recover against their employees for misappropriation of information claims under a substantially lower burden of proof than what is required by state and federal statutes.

Although Congress passed the CFAA almost thirty years ago, its provisions continue to be important today. While our reliance on computers has increased since Congress passed the CFAA in 1984, the intent behind the Act should not be misconstrued to permit employers to use the CFAA to bring misappropriation claims against their employees. Because the Act was passed to target computer hacking, a crime increasingly committed today, the Ninth and Fourth Circuits’ narrow interpretation of what constitutes “exceeding authorized access” is substantially more consistent with the Congressional intent than the Fifth and Seventh Circuits’ broader approaches. Moreover, the broader approaches are flawed because they permit employers to use the CFAA to raise state claims against their employees in federal court. This disturbs judicial federalism by upsetting the traditional balance of power between state and federal courts. Additionally, the broader approaches permit employers to bring claims likened to state trade secret claims against employees under a substantially lower burden of proof than what is required by statutes that specifically address such claims.

However, the circuit split will unlikely be resolved without congressional or judicial intervention. Thus, Congress should amend the CFAA to provide a definition of “authorization” and “exceeds authorized access” so that courts will construe these terms in adherence to Congress’ original intent: prose-

Anderson

cutting computer hacking and providing a civil cause of action for those who suffer damage or loss as a consequence of such hacking. Alternatively, the judiciary should adopt the narrow approach to demonstrate its deference to congressional intent, protection of judicial federalism, and unwillingness to permit employers to pursue state claims in federal court by taking advantage of the CFAA’s broad language.