TRADE SECRET LAW AND THE
COMPUTER FRAUD AND ABUSE ACT:
TWO PROBLEMS AND TWO SOLUTIONS

Kyle W. Brenton†

I. INTRODUCTION

The recent federal criminal prosecution of a Missouri woman for allegedly causing the suicide of a teenager through fraudulent use of MySpace.com has focused national attention on the Computer Fraud and Abuse Act ("CFAA"). The Act was originally passed in order to give the FBI a weapon for prosecuting computer hackers, but the statute has grown far beyond its roots. The presence of a private right of action in the statute has led to the development of a body of civil precedents interpreting the Act broadly, and the prosecution in the Drew case was able to point to those cases in urging the jury to find criminal liability for Drew’s violation of MySpace.com’s Terms of Service. Academics predicted that the statute might be thus misused in the criminal context as early as 2003. The judge in the Drew case eventually dismissed the case on vagueness grounds. But the harm

† Law Clerk to the Honorable David M. Ebel, U.S. Court of Appeals for the Tenth Circuit; J.D., University of Minnesota Law School; M.F.A., American Repertory Theatre/Moscow Art Theatre School Institute for Advanced Theatre Training at Harvard University; B.A., Vanderbilt University. The author thanks William McGeveran, Orin Kerr, Mark Lemley, Jeff Justman, Randall Kahnke, Kerry Bundy, and, as always, Amy Brenton. © Kyle W. Brenton, 2009.

1. See United States v. Drew, No. 08-cr-00582, Dkt. 1, *6–8, (C.D. Cal. May 15, 2008); Jennifer Steinhauer, Woman Found Guilty in Web Fraud Tied to Suicide, N.Y. TIMES, Nov. 27, 2008, at A25 ("A federal jury here issued what legal experts said was the country’s first cyberbullying verdict Wednesday, convicting a Missouri woman of three misdemeanor charges of computer fraud for her involvement in creating a phony account on MySpace to trick a teenager, who later committed suicide.").

2. 18 U.S.C. § 1030 (2006). This Article will refer to the Computer Fraud and Abuse Act throughout as either “the CFAA” or “the Act.”


4. 18 U.S.C. § 1030(g) (2006) (“any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator”).


that may result from broad interpretations of the Act’s terms is not limited to the criminal arena.

As the American workplace has become more computerized, a broader range of what occurs in that workplace becomes potentially subject to laws regulating computer use. This phenomenon may have a major and hitherto unnoticed impact on trade secret law. As trade secrets become stored on computers with increasing frequency, they gain the protection not only of common-law and statutory trade secret principles, but also potentially of computer misuse statutes. At first glance this may seem like an unalloyed benefit. America’s robust protection of intellectual property has frequently been cited as one of the great driving forces of our information economy. At least one federal agency has valued America’s intellectual property at over $5 trillion. If some protection for trade secrets is a good thing, the argument runs, more protection should be a great thing.

But this viewpoint overlooks some of the fundamental policies underlying trade secret law, and as more and more plaintiffs argue that the CFAA protects their trade secrets, the relevance of those policies is undercut. The CFAA in the civil context creates two major problems for trade secret law. The first is substantive. The Act provides a means of redress to potential trade secret plaintiffs that lacks virtually all of the policy and procedural safeguards built into trade secret law. A plaintiff in a CFAA case need not prove that the information taken was not generally available, that it gained value from secrecy, or that reasonable steps had been taken to protect it. She need not prove that the defendant used improper means to obtain it. She need prove only that the information was on a computer, that the defendant obtained that information through unauthorized access or access exceeding existing


10. See id. at 2 (quoting Margaret J.A. Peterlin, Deputy Under Secretary of Commerce for Intellectual Property and Deputy Director of the USPTO).

11. See infra Part II.A.


13. Id.
authorization, and that she has lost at least $5,000 as a result.\textsuperscript{14} After this minimal showing (and under broad “authorization” precedents, the showing required is minimal indeed)\textsuperscript{15} she can obtain relief. Thus, in many trade secret misappropriation cases, the CFAA provides a means of recovery that is not circumscribed by the policy-based protections of substantive trade secret law. Because those protections are designed to maintain a balance between employers and employees, the CFAA threatens to disrupt that important equilibrium as well.

The second problem is jurisdictional. In those cases where the plaintiff cannot obtain full redress for the information theft purely through the CFAA—for instance, cases in which the plaintiff seeks relief from the misappropriator’s new employer—the Act provides a back door into federal court. As long as the plaintiff can make out the barebones showing, as articulated above, against the misappropriator, the supplemental jurisdiction statute\textsuperscript{16} provides authority for a federal court to adjudicate any and all state law claims that are part of the same “case or controversy” as the plaintiff’s federal claim. The problems created by the private right of action in the CFAA—either in trade secret law specifically or more generally—have gone almost entirely unnoticed by the academy.\textsuperscript{17} Practitioner publications\textsuperscript{18} and blogs,\textsuperscript{19} however, have taken note of these new developments, and have generally espoused a positive view of them.\textsuperscript{20} But no matter how useful the CFAA may seem to be to attorneys

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{14} 18 U.S.C. §§ 1030(a)(2)(C), (g) (2006) (providing the basis for federal jurisdiction and establishing the prima facie elements of a claim); see infra Part II (discussing fraudulent access to information on a computer as a substantive claim under the CFAA).
\item \textsuperscript{15} See infra Part II.B (explaining the simplicity of the four elements needed to establish federal subject-matter jurisdiction over a plaintiff’s civil CFAA claim).
\item \textsuperscript{18} See, e.g., Michael R. Levinson & Christopher E. Paetsch, The Computer Fraud and Abuse Act: A Powerful New Way to Protect Information, 20 No. 3 IPL NEWSL. 24, 28 (2002) (“The CFAA has already been applied broadly enough to suggest that it will become a mainstay of civil litigation over information misuse. . . . [It] may have started as a defense against hackers, but it will end up being used much more broadly.”).
\item \textsuperscript{19} CFAA Provides Federal Jurisdiction in Employment Matters Involving Theft of Computerized Data, FULCRUM INQUIRY, (May 2006), available at http://www.fulcrum inquiry.com/Theft_of_Computer_Data.htm (“Because CFAA’s focus is not on the information or type of data stolen but instead on abuse of a computer system to obtain that information, employers can bring CFAA claims without proving the information wrongfully accessed was a trade secret, constituted confidential or proprietary information, or breached an employment, confidentiality, or noncompete agreement.”). See, e.g., Posting of John Cavicchi to The Trade Secrets Vault, http://www.tradesecretsblog.info/2008/04/trade_secrets_litigation_in_th.html (Apr. 29, 2008, 23:49 EST) (noting “the increasingly common practice of litigating trade secret disputes in the U.S. federal courts in conjunction with claims under the U.S. Computer Fraud and Abuse Act”).
\item \textsuperscript{20} See, e.g., Levinson & Paetsch, supra note 19 at 28 (discussing that the CFAA has already been applied broadly enough to suggest that it will become a mainstay of civil litigation).
\end{itemize}
\end{footnotesize}
representing corporations, this cannot change the fact that using the Act as a civil remedy for trade secret theft in federal court both undermines the fundamental policies underlying trade secret law and contravenes Congress’ intent in leaving trade secret protection to the states. This Article thus argues that the costs of employing the CFAA in the trade secret arena dramatically outweigh the benefits. Congress should take action to remove the CFAA provision most relevant to trade secret cases from the ambit of the statute’s private right of action, or in the alternative enact a statutory definition of one of the Act’s key terms: authorization. In the absence of congressional action, federal judges presiding over cases in which federal jurisdiction is premised entirely upon the CFAA should closely scrutinize the facts and arguments of the parties, and if state law trade secret claims substantially predominate over a barebones CFAA violation, should decline to hear the state claims under the discretion granted in the supplemental jurisdiction statute.

This Article proceeds in four parts. Part II charts the framework of the Computer Fraud and Abuse Act, then explores the substantial judicial disagreement regarding three of the Act’s key terms: authorization, damage, and loss. Part III delves into substantive trade secret law to explore the elements of a misappropriation cause of action and the policies underlying those elements, and compares the substantive components of trade secret law with the elements and policies of the CFAA. In Part IV, the Article points out the difficulties that arise when state trade secret cases appended to CFAA claims make their way into federal court. It analyzes the legislative history of the Act to determine whether Congress intended it to apply to trade secret misappropriation, and addresses the harms to fundamental notions of federalism that this kind of use of the CFAA can create. Finally, Part V proposes two sets of solutions to the two problems created by the CFAA, one legislative and the other judicial. Both Congress and the federal courts should take action to protect state trade secret law and to prevent opportunistic litigants from forum-shopping their way into federal court via the Computer Fraud and Abuse Act.

II. A CFAA PRIMER

The Computer Fraud and Abuse Act establishes seven computer misuse-related activities as substantive crimes. One of those crimes—that laid out in section 1030(a)(2)(C)—parallels trade secret misappropriation and creates the problems that this Article addresses. To make out a civil CFAA claim, the plaintiff must allege both a violation of one of the Act’s criminal prohibitions and damage or loss exceeding $5,000. The real story is somewhat more complex, however, first because the statute is very poorly drafted, and second

22. See infra Part III.B.1.
23. 18 U.S.C. § 1030(a)(2)(C) (2006) (establishing liability for obtaining information through unauthorized access of a computer); See infra Part II.A.
24. 28 U.S.C. § 1367(c) (2006); see infra Part IV.B.
because substantial judicial disagreement exists as to the scope of many of the Act’s key terms. This Part first looks to the Act’s substantive crimes, then to the private right of action and the contested terms therein.

A. Information Theft Under CFAA Section (a)(2)(C)

The common thread woven through almost all of the Act’s substantive crimes is the notion of unauthorized access. The specific contours of that notion will be explored below, but in the broadest possible terms, Congress designed the Act to criminalize computer misuse—that is to say, either wrongful conduct harmful to a computer (such as a denial-of-service attack damaging a computer network), or use of a computer as an instrument of wrongful conduct (such as hacking into a system to steal information). To trigger the Act, the unauthorized access must be of a “protected computer,” which the statute defines as either a computer used by a financial institution or the United States government or a computer “used in or affecting interstate or foreign commerce or communication . . .”. Therefore, the Act applies to the full extent of Congress’ powers under the Commerce Clause, and given the decentralized nature of computer networks and the Internet, it is difficult to imagine a functioning, networked computer that does not fit the Act’s definition.

The Act contains seven substantive criminal prohibitions listed in section (a) of the statute. Two of the crimes apply specifically to activity aimed at the United States government. A second class of crimes address fraud and extortion using computers. The statute then criminalizes damaging a
computer through unauthorized access. But the real action, from a trade secret point of view, lies in subsection (a)(2), which creates three crimes related to the theft of information. Subsections (a)(2)(A) and (B) address information stolen from a financial institution and from the United States government, respectively. But the third is not so limited: subsection (a)(2)(C) is violated whenever anyone “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains...information from any protected computer.” This subsection puts no qualification on the nature or character of the information taken—it focuses squarely and solely on the actions of the defendant in obtaining it.

Congress recently enlarged the scope of subsection (a)(2)(C). Until September 2008, the subsection read “information from any protected computer if the conduct involved an interstate or foreign communication.” The final clause was dropped as part of the Identity Theft Enforcement and Restitution Act, which also added criminal forfeiture provisions and restitution requirements to the sentencing portions of the Act. The purpose of the amendments was to facilitate prosecution of identity theft, as well as to make it easier for victims to obtain restitution after the successful prosecution of identity thieves. Section 203 of the amendment was entitled “Ensuring Jurisdiction Over the Theft of Sensitive Identity Information,” and while the amendment certainly did that, it likely “ensured jurisdiction” over a whole lot more. According to a press release from sponsor Senator Patrick Leahy’s office, the amendments will “[e]nable prosecution of those who steal personal information from a computer even when the victim’s computer is located in the same state as the thief’s computer. Under current law, federal courts only have jurisdiction if the thief uses an interstate communication to access the victim’s computer.” Not surprisingly, neither the House nor the Senate debated the civil dimensions of this amendment, but removing the interstate communication requirement broadened the CFAA’s scope in the civil arena just as much as (or more than) in the criminal. The impact of this recent

to defraud and the value of the computer use, while (a)(2)(C) imposes no such burden—this Article will focus on the latter. The remaining fraud-like provisions are (a)(6), which bans trafficking in passwords “though which a computer may be accessed without authorization,” and (a)(7), which criminalizes the extortion of money via threats to damage or steal information from a computer.

32. 18 U.S.C. § 1030(a)(5)(A) prohibits the transmission of “a program, information, code, or command” that intentionally causes damage to a protected computer. Subsection (a)(5)(B) penalizes intentional unauthorized access that recklessly causes damage to the computer, and subsection (a)(5)(C) prohibits intentional unauthorized access that—regardless of the accessor’s intent—causes damage and loss, as defined by the statute.


34. Id. (emphasis added).

35. Identity Theft and Restitution Act of 2008, Pub. L. 110–326, § 203, 112 Stat. 3560, 3561 (2008). The full provision was entitled the Former Vice President Protection Act, as the identity theft provisions that had been passed by the Senate were added to a bill that the House had already approved.

36. See 18 U.S.C. § 1030(i)–(j) (describing rights subject to forfeiture).


38. § 203, 112 Stat. at 3561.

amendment remains to be seen.

B. The Private Right of Action

Although the CFAA’s substantive crimes define the kinds of behavior prohibited in both the civil and criminal arenas, civil liability under the statute requires an additional showing. The Act’s private right of action appears in subsection (g), and reads, in its entirety:

Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.40

Therefore, a violation of any of subsection (a)’s criminal offenses can give rise to civil liability under subsection (g),41 and any person harmed—a category not confined to the owner of the accessed computer42—can sue the violator, but only if the plaintiff can also prove one of the sentencing provisions in subsection (c)(4)(A)(i). Of those six factors, the most relevant one in civil litigation is (c)(4)(A)(i)(I), which applies to conduct that causes “loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value.”43 Thus, in addition to the violation of a section (a) criminal prohibition, a CFAA plaintiff must have suffered $5,000 in damages—a kind of amount-in-controversy requirement for the Act.44

Surveying all the various subsections together, the elements of the civil CFAA claim most closely paralleling trade secret misappropriation are: (1) intentional, unauthorized access or access which exceeds authorization; (2) of a protected computer; (3) through which the violator obtains information; (4) causing $5,000 in loss to one or more persons in a one-year period. Pleading those four simple elements establishes federal subject-matter jurisdiction over

41. See Theofel v. Farey-Jones, 359 F.3d 1066, 1078 n.5 (9th Cir. 2004) (“Defendants argue that subsection (a)(5)(A) prescribes the Act’s only civil offenses. But subsection (g) applies to any violation of ‘this section’ and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).”) (referring to numbering in a prior version).
42. See id. at 1078 (“Individuals other than the computer’s owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.”).
43. 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2006). The remaining factors apply to impairment of medical diagnosis and treatment (subclause II), physical injury to a person (subclause III), public health or safety threats (subclause IV), damage to U.S. government computers (subclause V), and conduct that damages 10 or more computers during a 1-year period (subclause VI). Id. at (II)–(VI).
44. Cf. 28 U.S.C. § 1332(a) (setting out the requirements to establish diversity jurisdiction, including command that the amount in controversy equal or exceed $75,000).
the plaintiff’s claim. Proving them by the preponderance of the evidence\(^{45}\) gives the plaintiff a right to “compensatory damages and injunctive relief or other equitable relief.”\(^{46}\)

C. Defining Terms: Authorization, Damage, and Loss

Knowing those elements does not end the inquiry, however, because some of the key terms at issue are either not defined by the statute, or they are defined in a manner that leaves enough ambiguity for courts to disagree substantially as to their scope. A full exegesis of the nuances of the terms “authorization,” “damage,” and “loss” in the statute is beyond the scope of this Article.\(^{47}\) But a quick sketch of the judicial disagreement regarding them will give a sense of the CFAA’s potential reach in the civil arena.

I. Authorization

Key to almost every substantive crime in the CFAA is the notion of authorization. All but one of the seven crimes are triggered by “unauthorized access” or use that “exceeds authorized access.”\(^{48}\) The Act defines the latter term as “to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter,”\(^{49}\) but by simply incorporating the undefined term “authorization,” that provision sheds little light on the scope of the statute. Two schools of thought have arisen on the meaning of the term “authorization.” One defines the term by looking to its legal meaning, and the other by looking to its technological meaning.

The two leading cases on the legalistic side of the equation are *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*\(^{50}\) and *International Airport Centers, L.L.C. v. Citrin.*\(^{51}\) Both cases involved the classic “faithless employee” trade secret misappropriation scenario. In *Shurgard*, after receiving an employment offer from a competitor, the employee emailed confidential information to that competitor while still working for Shurgard.\(^{52}\) In *Citrin*, an

\(^{45}\) See *Diamond Power Int’l, Inc. v. Davidson*, 540 F. Supp. 2d 1322, 1341 n.17 (N.D. Ga. 2007) (“[T]he plaintiff would have to prove, by a preponderance of the evidence, the same elements required to prove a criminal violation of the CFAA to recover in a civil action.”).

\(^{46}\) 18 U.S.C. § 1030(g). It is worth pointing out that the Act’s private right of action limits damages in (c)(4)(A)(i)(I) cases—i.e. $5,000 loss cases—to economic damages. On the face of the subsection, however, that limitation does not limit injunctive or equitable relief, since it limits only damages, and not all remedies. One could perhaps argue that (c)(4)(A)(i)(I) actions do not allow for injunctive or other equitable relief, but if that argument has been made in court, it has not made it to any reported case, and the plain statutory language weighs against it.

\(^{47}\) Indeed, an entire article has been written about some of these terms. See *Kerr, supra* note 7, at 1617–24 (discussing the definitions of the terms “access” and “authorization”).

\(^{48}\) See *supra* Part II.A.


\(^{50}\) 119 F. Supp. 2d 1121, 1125 (W.D. Wa. 2000).

\(^{51}\) 440 F.3d 418, 420 (7th Cir. 2006).

\(^{52}\) *Shurgard*, 119 F. Supp. 2d at 1123.
employee removed sensitive information from his employer-provided laptop in order to start his own company, and then used a secure-erasure program to cover his tracks. Both cases revolved around the question of whether the employees’ use of their employers’ computers was “unauthorized,” even when the offenders still had both physical and technological access to those computers as a part of the employment relationship.

Both District Judge Zilly and Circuit Judge Posner answered that question in the affirmative. Rather than consider whether the employees’ access of their computers was “unauthorized” in a technological sense, both cases looked to a legal notion of authorization as defined by agency law. According to the Restatement (Second) of Agency § 112, “the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.” So, as soon as any agent or employee violates her legal duty of loyalty to her employer, her authorization to access her employer’s computer terminates, and any subsequent access can give rise to CFAA liability. Thus, in Shurgard, subsequent access to employer’s computer system gave rise to CFAA liability when the employee accepted an offer of employment from a rival; in Citrin, subsequent access to employer’s computer system gave rise to CFAA liability when the employee decided to leave his employer’s company and start his own business.

This conception of authorization is quite broad, and in the years since Shurgard and Citrin a number of district courts have questioned it. In International Ass’n of Machinists & Aerospace Workers v. Werner-Masuda, for example, the court rejected both the agency law notion of authorization and the argument that an employee’s illegitimate use of information obtained from a computer could render the access unauthorized. This court looked to the CFAA’s legislative history and found that Congress intended the statute to apply primarily to outside computer hackers, rather than faithless employees. Thus the court held that, despite the fact that Werner-Masuda had accessed her

53. Citrin, 440 F.3d at 419. Citrin’s installation and use of this program, according to Judge Posner, constituted damage to the computer, and so IAC also brought a claim under the CFAA’s computer-damage crimes, in subsection (a)(5). See id.
54. See id. at 420 (describing how the plaintiff alleged that the defendant employee did not have authority to access IAC’s computer because he engaged in misconduct and decided to quit IAC); Shurgard, 119 F. Supp. 2d at 1125 (noting how a plaintiffs pleading a 18 U.S.C. § 1030(a)(2)(C) claim must establish the employee’s use of the computer was unauthorized).
55. See Citrin, 440 F.3d at 420 (finding agency law controls the meaning of “authorization”); Shurgard, 119 F. Supp. 2d at 1125 (same).
57. Citrin, 440 F.3d at 420.
59. Citrin, 440 F.3d at 420.
60. 390 F. Supp. 2d 479 (D. Md. 2005).
61. Id. at 498–99.
employer’s computers on behalf of a competitor, her employer had not yet revoked her access and therefore could not state a claim of a claim for relief under the CFAA. 63

The CFAA, according to the Werner-Masuda court, does not “prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do [its] terms proscribe authorized access for unauthorized or illegitimate purposes.” 64 This latter interpretive camp—call it the “technological school”—would therefore find access to be unauthorized only if the accesser did not have physical and/or technological access to the computer; for example, a valid user ID and password. 65 Several other federal district courts have sided with the Werner-Masuda court on this question,66 and the Ninth Circuit recently cast its lot with the courts adopting the technological reading as well. 67 Other district courts, though—particularly those within the Seventh Circuit—continue to toe the Shurgard/Citrin line.68

As long as this split in authority over the scope of the term authorization in the CFAA remains unresolved, the statute may enable claims arising out of a broad range of employee misconduct. As long as a plaintiff in a trade secret case can prove that the employee’s motives in accessing her work-provided computer were less than pure, there remains a colorable argument under Shurgard and Citrin that that access was unauthorized, and thus in violation of federal law.

2. Damage and Loss

Unlike “authorization,” the Act defines both “damage” and “loss,” although it has not always done so. 69 Damage is “any impairment to the

64. Id.
65. See Kerr, supra note 7, at 1648–60 (outlining different ways of defining the scope of authorization). This interpretation of the statute also arguably better accommodates the second kind of prohibited access: access exceeding authorization. Id. According to the technology-focused view, when a company segments the data on its computers and gives an employee legitimate access to some, but not all of that information, and the employee uses their account to gain information not cleared for their account, that access “exceeds authorization.” See Diamond Power Int’, Inc v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007).
67. See LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (“[F]or purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations.”).
integrity or availability of data, a program, a system, or information,” and thus encompasses injury to the computer itself, its software, or the information stored on it. Loss is “any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of disruption of service.” While the destruction or deletion of data would almost certainly constitute damage under the Act, two major questions about the scope of damage and loss arise in the trade secret context. First, does the loss of secrecy constitute an “impairment to the integrity . . . of data” such that it counts as damage? And second, does economic damage due to trade secret misappropriation—for example, lost profits—count as loss?

On the damage question, there is some authority that supports the argument that loss of trade secret status could constitute damage under the Act. In the context of copyright infringement, one district court has held that “[w]e see no principled reason . . . why infringement of copyrighted material taken from a computer system would not qualify as impairment of the integrity of the copyrighted information.” In theory, this argument could apply to information protected by trade secret law as well as copyright law—an argument that is particularly attractive if one is thinking in the Citrin legalistic mode. But later cases have called this line of argument strongly into question, and have held that damage, as defined by the statute, is to be looked at from a technological, rather than a legalistic, point of view.

Loss, however, is defined a bit more broadly in the statute than is damage, and thus might accommodate a more functional construction. In Nexans Wires S.A. v. Sark-USA, Inc., the District Court for the Southern District of New York found that the cost of flying two executives from Germany to New York to investigate an allegation of unauthorized computer access did not constitute “loss,” because the trip was unrelated to the allegedly accessed computers themselves. The court noted that had the record contained evidence that the executives had actually examined one of the

---

72. See, e.g., B&B Microscopes v. Armogida, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) (finding that deletions that make data unavailable to the plaintiff are damage within the statutory definition).
73. Of course, as noted above, a subsection (a)(2)(C) violation does not require statutory damage, and the private right of action requires only “damage or loss,” so this question is not essential in the (a)(2)(C) context. If, however, loss of trade secret status is considered statutory damage, then misappropriators could also face liability under the (a)(5) damage-based offenses, and therefore, the question merits some discussion here.
74. George S. May Int’l Co. v. Hostetler, No. 04 C 1606, 2004 WL 1197395, at *4 (N.D. Ill. May 28, 2004). See also Therapeutic Research Facility v. NBTY, Inc., 488 F. Supp. 2d 991, 996 (E.D. Cal. 2007) (holding that unauthorized access plus disclosure “may constitute an impairment to the integrity of data or information even though no data was physically changed or erased”) (internal quotation marks omitted).
75. See, e.g., Garrelli Wong & Assoc., Inc. v. Nichols, 551 F. Supp. 2d 704, 710 (N.D. Ill. 2008) (“Though Garrelli Wong would like us to believe that [the CFAA applies] to cases where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show ‘impairment to the integrity or availability of data, a program, a system, or information.’”).
77. Id.
computers while in New York, the cost of the trip might have constituted loss, but that the record actually tended to prove that the purpose of the visit was to discuss the information stolen by the faithless employee, rather than the potential harm to the computer system. Further, the aggrieved company argued that because it had lost two business opportunities due to the faithless employee’s information theft, that lost revenue should be considered loss for the purposes of the jurisdictional requirement. The court, however, held that to constitute loss, any lost revenue must be due to an interruption of service in the computer network, according to the statutory definition. Therefore, while the cost of responding to andremedying a violation of computer security does constitute loss, such actions must be directly connected to the wrongfully accessed computers, and lost profits due to lost information do not count toward the $5,000 jurisdictional threshold.

Judicial constructions of the CFAA, thus, appear inconsistent with one another, with courts interpreting terms in a legalistic fashion and others in a technology-centric manner. It seems that the more clearly Congress ties a term to its technological definition, the more likely a court will follow that dictate; the less clearly the statute ties a term to technology, however, the more likely a court is to expand its meaning to its fullest legal extent. The upshot of all of this, however, is a statute that applies to employee theft of information from computers in an uncertain fashion. In that ambiguity lurk two major problems for trade secret law.

III. THE SUBSTANTIVE PROBLEM: VIRTUAL REDUNDANCY

The Computer Fraud and Abuse Act creates two significant problems for trade secret law—one substantive and one jurisdictional. This Part examines the first. Many, if not most, units of information that fit the common law or statutory definition of a trade secret today are stored on computers. Because the CFAA provides a civil cause of action when someone obtains information through unauthorized access to a computer, the Act may apply to a broad range of situations previously covered only by trade secret law. Since the evidentiary requirements and elements of proof of a CFAA (a)(2)(C) claim are far lower than in a traditional trade secret misappropriation claim, there exists a danger that the substantive law of trade secrets will be eclipsed by CFAA litigation.

It will, however, rarely if ever be the case in litigation that a plaintiff will be presented with an either/or choice between a state-law trade secret claim and a CFAA claim. In fact, much of the danger inherent in the CFAA arises from the fact that the two claims will generally be pled together, and thus the plaintiff can get into federal court with what is substantially an exclusively

78. Id.
79. Id. at 477.
80. Id.
81. That such expenditures do not count toward the jurisdictional threshold, however, does not answer the question of whether they might nonetheless be compensable under the Act. See infra Part II.A.3.
82. See generally supra note 8 (noting the increased prevalence of computers in the modern workplace).
state-law claim, a problem addressed by Part IV. The substantive problem treated in this Part arises not because litigants will choose one body of law over the other; rather, the problem comes to light when the CFAA is enlisted to protect information that trade secret law would hold unprotected. As addressed below, this undermines the policy goals of trade secret law and threatens the equilibrium between employer and employee. To lay bare that threat, this Part will first examine the requirements of trade secret protection and compare them to the elements of a CFAA (a)(2)(C) claim, thus putting into stark contrast the policy goals served by each.

A. Substantive Trade Secret Law vs. CFAA (a)(2)(C) Claims

Because trade secret law is entirely a creature of state law, the particular requirements of proving a misappropriation claim will vary from jurisdiction to jurisdiction. But due to the efforts of the American Law Institute and the Uniform Law Commissioners embodied in the Restatements and the Uniform Trade Secret Act (“UTSA”), there is more similarity from state to state than in other areas of the law. At the broadest level, both the UTSA and the common law first focus attention on the character of the information alleged to be a trade secret, and then on the actions of the individual alleged to have misappropriated that secret. This dual focus reflects the policy compromise at the heart of trade secret law: a balance between a property-based conception of trade secret protection and a misconduct/commercial morality-focused approach.

1. Definition of a Trade Secret

The first question in any trade secret litigation is whether the information taken fulfills the common law or statutory definition of a trade secret. The UTSA defines a trade secret as:

83. Misappropriation of trade secrets was included in the original Restatement of Torts. Restatement of Torts §§ 757–59 (1939). When the ALI began work on the second Restatement of Torts, the decision was made to abandon trade secrets, because it had become a species of law separate from pure tort law. See James Pooley, Trade Secrets § 2.02[1] (1998). In 1995, the reporters of the unfair competition Restatement added a section addressing trade secret law. Restatement (Third) of Unfair Competition §§ 39–45 (1995).

84. Forty-five states, the District of Columbia, and the U.S. Virgin Islands have adopted some version of the UTSA. See National Conference of Commissioners on Uniform State Laws, A Few Facts About the Uniform Trade Secrets Act, http://www.nccusl.org/Update/uniformacT_factsheets/uniformacts-fs-utsa.asp (last visited Dec. 16, 2008) (listing which states have adopted the UTSA). There are two versions of the Act: the original 1979 version and the 1985 amended version. Id. Both versions are still in use in various states, but the differences between them are not material to this Article. Id.


86. See supra notes 83–85 and accompanying text.

87. See Pooley, supra note 86, at § 1.02[8].

88. See, e.g., Electro-Craft Corp. v. Controlled Motion, Inc., 332 N.W.2d 890, 897 (Minn. 1983) (“Without a proven trade secret there can be no action for misappropriation, even if defendants’ actions were wrongful.”).
information, including a formula, pattern, compilation, program, device, method, technique, or process that: (i) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.89

The Restatement (Third) of Unfair Competition definition is similar.90 This definition builds three important safeguards into the law from the outset. First, the alleged trade secret must derive economic value from the fact that it is secret.91 This requirement is applied strictly—if an alleged trade secret is valuable only for reasons other than its secrecy it is not protectable on the basis of that value alone.92 Thus trade secret law protects only information that gives its holder a competitive advantage based upon its secrecy.93 Second, the definition excludes information that is ―readily ascertainable by proper means‖ by others.94 Thus, the UTSA permits ―reverse engineering‖ of a trade secret from an end product, as long as the allegedly protected information can be ascertained readily and legitimately.95 Finally, the definition imposes a positive duty on the holders of supposed trade secrets to undertake reasonable precautions to keep their proprietary information secret.96 The holder of the information need not take every conceivable step to keep it secret, but must do that which—taking into account the value of the information and other circumstances—a reasonable person would do to preserve secrecy.97

From the outset, then, a cardinal difference between a UTSA-based trade secret claim and a CFAA-based information theft claim reveals itself. While trade secret law is very much concerned with the character of the information for which protection is sought, under the CFAA as long as what was stolen was information stored on a computer, no further inquiry is necessary.98 This is even more apparent following the 2008 amendments to the Act, which

89. UNIF. TRADE SECRETS ACT § 1(4) (1979) (amended 1985).
90. See POOLEY, supra note 86, at § 2.04[2].
91. UNIF. TRADE SECRETS ACT § 1(4)(i); see also RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 39 (1995) (defining a trade secret as ―any information . . . that is sufficiently valuable and secret to afford an actual or potential economic advantage over others.‖).
92. See, e.g., Buffets, Inc. v. Kline, 73 F.3d 965, 968–69 (9th Cir. 1996) (affirming summary judgment where plaintiff failed to prove, inter alia, that their recipes gained any economic value from their secrecy).
93. See POOLEY, supra note 86, at § 4.05 (discussing elements that establish a secret as providing a competitive advantage).
94. UNIF. TRADE SECRETS ACT § 1(4)(i).
96. UNIF. TRADE SECRETS ACT § 1(4)(i).
97. See E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012, 1016 (5th Cir. 1970) (―[W]e need not require the discoverer of a trade secret to guard against the unanticipated, the undetectable, or the unpreventable methods of espionage now available . . . .‖).
98. See William Lynch Schaller, Jumping Ship: Legal Issues Related to Employee Mobility in High Technology Industries, 17 LAB. LAW. 25, 85–86 (2001) (―[The CFAA] could prove especially potent, as the federal statute at issue in Shurgard Storage Centers appears to apply to any information, not just trade secrets.‖).
removed even the minimal requirement that the wrongfully-accessed computer be engaged in “interstate or foreign communication.” While the utter absence of proof requirements related to the information taken has disturbing policy implications, it also has a dramatic practical effect—proving a CFAA claim becomes far easier than establishing a prima facie case of trade secret status. This disparity in the respective hurdles a plaintiff must clear, therefore, creates an incentive bias toward a CFAA claim and against a trade secret misappropriation claim.

2. Misappropriation Through Improper Means

Once a plaintiff establishes trade secret status, the focus then shifts to the behavior of the defendant. In order to establish liability, the plaintiff must prove that the defendant misappropriated the trade secret at issue. The UTSA defines misappropriation as:

(i) acquisition of a trade secret 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 had 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 [or her] 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.

Therefore, misappropriation occurs either when one acquires a trade secret by improper means, or when one discloses or uses a trade secret either acquired by improper means or acquired innocently but with knowledge that it should have been protected. “Improper means” include “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain

99. See supra notes 35–43 and accompanying text (discussing the 2008 amendments).
100. See infra Part II.B.
102. See POOLEY, supra note 86, at § 2.03(3).
103. UNIF. TRADE SECRETS ACT § 1(2) (brackets in original).
104. Id.
secrecy, or espionage through electronic or other means.” The comments to the UTSA add that the definition is not a “complete catalogue” of the kinds of behavior that constitute improper means, but that such behavior need not necessarily even be unlawful—merely “improper under the circumstances.” The comments to the Restatement add to the definition the notion that means “inconsistent with accepted principles of public policy” may also be improper.

A CFAA subsection (a)(2)(C) claim also focuses on the character of the defendant’s actions. The CFAA’s analogue to the improper means inquiry is the determination of whether the defendant’s access to the computer was unauthorized or exceeded existing authorization. It is not immediately apparent, however, whether the UTSA’s “improper means” is broader or narrower in scope than the CFAA’s “unauthorized access.” The answer will depend on which of the two schools of thought on authorization wins the day. If authorization is viewed in a purely technological sense, then the scope of proscribed conduct under the CFAA seems narrower than that proscribed by the UTSA; in order to trigger liability, the defendant must either be an outsider to the computer system and hack into it, or bypass a code-based limitation on their authorized access to obtain information exceeding their authorized access. A putative defendant could thus engage in a wide range of behavior that a court might consider “improper under the circumstances,” and yet not violate any technological limits on their access, and thus escape CFAA liability.

If, on the other hand, the Shurgard/Citrin legalistic interpretation of authorization prevails, the breadth of prohibited conduct under the CFAA may approach that of the improper means requirement of the UTSA. If any breach of an employee’s legal duty of loyalty to his or her employer terminates the agency relationship and makes any subsequent computer access unauthorized, more conduct is swept in than just that which, as proscribed in the UTSA, breaches a narrower duty to maintain secrecy. The UTSA definition of “improper means” certainly reaches a great deal of conduct that is entirely unrelated to the principal/agent relationship—such as theft, electronic espionage, or bribery—but in the context of the employment relationship, the Shurgard/Citrin notion of authorization is at least arguably as broad as or broader than the UTSA’s improper means test.

There remains, however, one type of misappropriation in the UTSA that the CFAA does not encompass: third-party liability. In its definition of misappropriation, the UTSA includes actions by third parties who use or disclose a trade secret, even if they did not acquire it through improper means.

105. Id. at § 1(1).
106. Id. at cmt. 1 (citing E.I. DuPont deNemours & Co. v. Christopher, 431 F.2d 1012 (5th Cir. 1970)).
108. See supra Part II.C.1 (explaining the notion of authorization in CFAA crimes).
109. See supra notes 52-69 and accompanying text (discussing the split in authority over the scope of the term “authorization”).
110. See supra Part II.C.1 (discussing the “faithless employees” problem).
means. The CFAA’s private right of action, in contrast, provides only for “a civil action against the violator,” and so third-party liability of a user of trade secrets stolen from a computer by another is not available. So if a plaintiff wants to sue anyone other than the party that stole the information from her computer, the UTSA (or state common law misappropriation) provides her only recourse.

3. Remedies

The final area of contrast between UTSA and CFAA § 1030(a)(2)(C) claims lies in the remedies available. The UTSA provides both for money damages—compensatory, punitive, and attorney’s fees—and injunctive relief to prevent “threatened or actual misappropriation.” Compensatory damages under the UTSA include both the actual loss to the plaintiff and the amount the defendant is unjustly enriched by use of the trade secret that is not captured in the amount of the plaintiff’s actual loss. An injunction may also include the award of so-called “reasonable royalty” damages, which require the defendant to pay the plaintiff an amount that the court determines would have been a reasonable royalty for access to the protected information.

Unsurprisingly, given its criminal purpose and roots, the CFAA does not adequately specify the types of remedies available to civil plaintiffs. As noted above, subsection (g) authorizes civil actions “to obtain compensatory damages and injunctive relief or other equitable relief.” The only express limitation on CFAA damages is the mandate that damages in (c)(4)(A)(I) actions—i.e. $5,000 loss actions—are limited to economic damages. As noted above, this limitation does not on its face rule out injunctions or equitable relief for these actions. Caselaw on this topic offers limited clarity—most reported CFAA cases dealing with damage address whether the plaintiff has adequately pleaded statutory damage and/or loss exceeding the jurisdictional

111. See Unif. Trade Secrets Act § 1(2)(ii).
115. Punitive damages are limited to double the amount of compensatory damages. Id. at § 3(b).
116. Id. at § 4.
117. Id. at § 2(a).
118. Id. at § 3(a).
119. Id. at § 2(b).
121. See supra note 48.
amount, but few cases address the propriety of damage awards post-trial.

The question of whether damages for lost profits or loss of business advantage or goodwill are available in civil CFAA actions has generated disagreement in the courts. Both the statute’s text and the thrust of the opinions construing the jurisdictional amount question argue that only costs incurred in responding to a computer security breach should be compensable under the Act. Subsection (g) applies to “[a]ny person who suffers damage or loss by reason of a violation” of the Act, and there seems no reason not to apply the statutory definition of those terms to the question of compensable losses. As explored above, loss is broader than damage, but both require the expenditures at issue to be related to the computer security breach that gave rise to CFAA liability. Therefore, it might be reasonable to assume that only those costs incurred in investigating and responding to a computer security breach are compensable under the CFAA.

However, the statute could be read differently. At least one court, relying on a textualist reading of the statute, has held that lost revenue should be compensable under the CFAA. Because “compensatory damages” are not defined in the statute, the court assumed that Congress intended to adopt the usual legal meaning of that term, which encompasses all compensation necessary to make the plaintiff whole. Further, the lack of a definition for “economic damages” led the court to conclude that use of that term excluded only damages for things like emotional distress or pain and suffering. The court finally held that Congress’ use of the terms “damage” and “loss” in the private right of action (and their associated statutory definitions) applied only to the jurisdictional threshold, and did not limit the types of loss recoverable upon a favorable verdict. “When a defendant copies unauthorized data to gain a competitive advantage,” in the court’s view, “it makes no sense to limit the plaintiff’s recovery when the lost revenue is a direct result of the defendant’s misconduct.”

Therefore, it is impossible to say with certainty what categories of damages will be available in a CFAA case. But even if a court adopts the more restrictive interpretation covering only costs incurred in responding to a breach in information theft cases, injunctive relief may well be of much greater benefit to the plaintiff than any amount of monetary damages. If a company’s trade

123. Compare Nexans Wires S.A. v. Sark-USA, Inc., 166 F. App’x 559, 562–63 (2d Cir. 2006) (requiring economic loss to stem directly from an interruption in service to be compensable under the CFAA), with Creative Computing v. GetLoaded.com LLC, 386 F.3d 930, 935 (9th Cir. 2004) (holding that damages for loss of business and business goodwill are compensable as “economic damages” under the statute).
125. Supra Part I.C.2.
126. See Frees, Inc. v. McMillan, No. 05-1979, 2007 WL 2264457, at *4–6 (W.D. La. Aug. 6, 2007) (holding lost revenue to be compensable under the CFAA by interpreting “compensatory damages” as a legal term of art).
127. Id. at *5. The court further noted that by using the term “compensatory damages,” Congress excluded exemplary or punitive damages from the scope of the statute. Id.
128. Id. at *5.
129. Id. at *6.
130. Id. at *5.
secrets have been stolen and it has incurred sufficient costs in responding to the breach, an injunction requiring the defendant to return or destroy the stolen information may be all the remedy that the company needs. Therefore, while the CFAA’s damages provisions may not be as expansive as the UTSA’s, the remedies that the CFAA does provide will likely be sufficient for plaintiffs in most cases.

In sum, UTSA trade secret misappropriation and CFAA information theft do not align precisely. They do, however, overlap in their core areas to a great enough extent that, when potentially protectable information is taken from a computer, a plaintiff might plead either or both in court. The relative ease of establishing a CFAA violation, however, creates a bias against relying upon a traditional trade secret claim. Even if that is the case, though, it remains to be shown why that matters.

B. Trade Secret Law Policy Goals and the CFAA

The pleading and proof requirements of traditional trade secret law are there for a reason. Trade secret law does not exist to impose strict liability for the theft of information. As a matter of policy, trade secret law has two major purposes: to enforce a baseline level of commercial morality by punishing wrongful business conduct and to encourage investment in research by guaranteeing businesses that their confidential information will be protected. Each of the pleading requirements relates in some way to one of those two goals, or both. For instance, the requirement that the plaintiff prove that the information taken fit the definition of a trade secret ensures that defendants are not penalized for using easily ascertainable information that happens to have been discovered first by another party. And requiring only reasonable efforts to maintain secrecy—rather than demanding absolute confidentiality—reduces the costs that companies must spend on security, leaving more funds available for pure research and development.

Trade secret law as it currently exists represents a compromise between two possible ways of protecting confidential business information: protecting information as property or punishing the betrayal of confidence. The latter school conceives of trade secret law as primarily about the enforcement of confidential relationships—if the defendant was in a position of confidence vis-à-vis the plaintiff (such as an employment relationship) and abused that confidence, the defendant should be liable no matter what shape that abuse took. The former school, on the other hand, conceives of the trade secret

131. And in most companies, the bill to clean up a security breach will very likely surpass $5,000 quickly. See Chan & Rubiner, supra note 101 (noting that the cost of remediation will almost always be greater than the jurisdictional amount).
132. See POOLEY, supra note 86, at § 1.02 (discussing the policies behind the development of trade secret law).
133. See generally id. at § 1.02[8] (discussing the debate between those who characterize a trade secret holder’s rights as property and those who characterize them as a breach of confidentiality).
134. See, e.g., Servo Corp. v. Gen. Electric Corp., 393 F.2d 551, 555 (4th Cir. 1968) ("The gravamen in a trade secrets case is a breach of confidence, rather than an infringement of a property right . . . .").
right as propertarian in nature, and the owner of the protected property is entitled to redress for any kind of trespass by another party. The requirements of proving misappropriation serve both of these interests: The necessity of proving trade secret status ensures that there is a legally-recognized property right in the thing being protected, and the improper means inquiry demands that the defendant violate some social norm of confidence.

The CFAA serves none of these policy goals. At first blush, it might appear that the CFAA falls on the property-rights side of the debate. After all, the Act imposes liability for the theft of information in an almost strict manner—as long as the right is interfered with in the proscribed fashion, liability follows. This hearkens back in a sense to the law of trespass, which imposes strict liability for any interference with a possessory right. The application of real property law concepts in cyberspace has a long and somewhat sordid history, and using trespass law to punish online wrongdoing in particular is fraught with difficulty. But a closer examination suggests that the CFAA approach does not truly represent the propertarian view of trade secrets, because even from that perspective, trade secret law’s focus is on proving that the information taken was in fact a trade secret, and thus property. The CFAA, on the other hand, merely assumes that any information on a computer is protectable property, and moves immediately to the character of the defendant’s actions in accessing it.

The key difference between the two bodies of law on a policy level boils down to the requirement of secrecy: a trade secret must have been secret to gain protection, while any information may be protected under the CFAA. Some might see this as a good thing. One could see trade secrets as a cumbersome, archaic body of law with difficult pleading requirements that is best supplanted by a simpler, surer regime of federal information protection, which is precisely what the CFAA’s (a)(2)(C) information-theft crime seems to do. Mark Lemley has argued that the requirement of secrecy, however, constitutes the essential core of trade secret law. In his view, the secrecy requirement serves two policy goals: encouraging controlled disclosure of confidential information to spur innovation and resolve Arrow’s disclosure

---

135. See, e.g., Van Products Co. v. Gen. Welding & Fabricating Co., 213 A.2d 769, 780 (Pa. 1965) (“The starting point in every case of this sort is not whether there was a confidential relationship, but whether, in fact, there was a trade secret to be misappropriated.”).
136. See supra Part III.A.1.
137. See RESTATEMENT (SECOND) OF TORTS § 158 (1965).
139. See generally Dan L. Burk, The Trouble with Trespass, 4 J. SMALL & EMERGING BUS. L. 27 (2000) (discussing the difficulties courts experience when applying the “anachronistic” trespass to chattels cause of action to disputes involving computer network access).
140. See, e.g., Van Prods. Co., 213 A.2d at 780.
141. See supra text accompanying notes 93–100.
143. Id. at 342–48.
paradox between negotiating companies  
and directing “inventors to the form of IP protection that best achieves the goal of society” by channeling inventors between patent law and trade secrecy.  

But Lemley’s argument is a justification for the existence of trade secrets as opposed to no protection at all; it gives little help in choosing between the current level of trade secret protection and the more absolute information protection offered by the CFAA. Moreover, generalized defenses of trade secret law are of less utility in the CFAA context, because CFAA claims parallel only the “faithless employee” type of traditional misappropriation claim, and so any defense must be similarly limited.  

From a normative viewpoint, the crux of why trade secret law is better than the CFAA lies in a second compromise embodied in trade secret law: in addition to accommodating both propertarian and morality-based approaches, it also strikes a balance between safeguarding business information and guaranteeing employee mobility.  

According to the *Restatement (Third) of Unfair Competition*, “[t]here is a strong public interest in preserving the freedom of employees to market their talent and experience in order to earn a livelihood.” Too little protection of business information could create the problem of “employee hold-up,” whereby an employee’s assertion of rights in information drastically raises the cost of a business using it. Too much protection, however, might force an employee leaving a firm out of an entire line of business at great personal cost, for fear of liability for using what he or she knows. 

Dan Burk and Brett McDonnell have characterized IP law generally—and trade secret law specifically—as helping to resolve a second variant of Arrow’s disclosure paradox, this one between the firm and the employee.  

---

144. It does so by, for example, assuring companies that they may share sensitive information while negotiating with other firms without that information losing its protected character. This use of trade secret law resolves Kenneth Arrow’s disclosure paradox, whereby the seller of secret information can never obtain its full value, because the buyer cannot be assured of the information’s value without disclosure, and disclosure destroys that value. See id. at 336–37.  
145. Id. at 341.  
146. See supra notes 52–69 and accompanying text.  
147. See POOLEY, supra note 86 at § 1.02 [6].  
148. Id.  
151. See Katherine V.W. Stone, Knowledge at Work: Disputes Over the Ownership of Human Capital in the Changing Workplace, 34 CONN. L. REV. 721, 742 (2002) (noting that an at-will employee subject to a noncompete clause who has been unfairly dismissed can be enjoined from accepting all subsequent employment in the type of work he or she is best able to perform).  
employees cannot be sure when they leave a firm which information is theirs and which belongs to the employer, they will never be able to compete in the labor market with 100% efficiency. Burk and McDonnell posit that the protections of IP law serve to put employees on notice as to what information cannot be taken with them when they leave a firm. The formal procedures of patent, copyright, and trademark law—alongside the “reasonable means to preserve secrecy” requirement of trade secret law—police the boundary between protected and unprotected information, and allow employees to effectively and efficiently compete in the labor market when they leave a firm without engaging in unfair competition against their former employer.

Concededly, Burk and McDonnell argue that trade secret law, with its less formalistic procedures and extremely wide subject-matter coverage, does not achieve this goal as well as the harder forms of IP. Even if that is the case, however, how much less well would the CFAA police the boundary between employer and employee? At first blush, the statute’s requirement of unauthorized access might provide a rough-and-ready way to differentiate between the two types of information: if access to the information requires authorization, it is protected; if not, it is not. But this argument proves too much: a firm may choose to put a list of the members of its board of directors on a password-protected server, but this does not make that list proprietary information that an employee may not use after leaving the company. And since the CFAA has no analogue to the UTSA’s ready ascertainability defense, a departing employee could indeed eventually be held liable for accessing such information, despite its public character.

But even this marginal value of the unauthorized access requirement as a method of putting employees on notice of what information is protected withers under the Shurgard/Citrin interpretation of the statute. If “access” can be rendered “unauthorized” long after the fact merely by use of the information that a court finds objectionable in the context of a lawsuit, the goal of achieving predictability for either employers or employees is hopelessly lost. The CFAA fails utterly at resolving the disclosure paradox between the firm and the employer; under the Shurgard/Citrin interpretation it precludes the problem of employee hold-up by giving the employer the equivalent of a nuclear weapon.

In sum, while the CFAA covers much of the same territory as the UTSA, it does so in a manner that disserves the fundamental policy goals of trade secret protection. It resolves any conflict between the employer and employee in a ham-fisted manner that breaks all ties in favor of property rights and against employee mobility. The CFAA’s information-theft crime thus makes trade secret law virtually redundant.

153. Id.
154. Id.
155. See Burk, supra note 152, at 9–11; Burk & McDonnell, supra note 154, at 592–93.
IV. THE JURISDICTIONAL PROBLEM: DIGITAL BOOTSTRAPPING

The second major problem with the CFAA in the trade secret context arises out of the first. Because the two bodies of law overlap, and a CFAA violation is so easy to make out in the context of a trade secret theft, those litigants who still plead a UTSA violation will be able to do so in federal court, even when the parties are not diverse. Under the supplemental jurisdiction statute, a plaintiff who can make out a claim that gives rise to federal question jurisdiction can ask the federal court to exercise subject-matter jurisdiction over state law claims that form “part of the same case or controversy” as the plaintiff’s federal claim. Because the same allegedly wrongful act will frequently give rise to both CFAA and UTSA liability, the plaintiff’s state-law trade secret claims will probably satisfy the initial supplemental jurisdiction requirements. Virtually all of the federal cases analyzed in this Article involved both a CFAA claim and a trade secret misappropriation claim, and many of them arose in the posture of a defendant’s motion to dismiss the federal claim and to force the plaintiff to bring the pendant trade secret claim in state court.

There is nothing per se wrong with a litigation strategy that brings a pendant trade secret law claim into federal court on the back of a meritorious CFAA violation. The purpose of supplemental jurisdiction is to promote judicial economy by bringing all claims that form part of the same case or controversy before a single court for resolution. If a CFAA claim is substantial enough to support federal question jurisdiction—and the fact that Congress put a private right of action in the statute is strong evidence of that point—why shouldn’t a pendant state-law trade secret claim be heard by the same court? This Part proposes two answers to this question: that such a use of the statute may contravene Congress’ intent, and that it might damage key notions of federalism.

A. Congressional Intent

As the courts that have sided against the Shurgard/Citrin interpretation of the CFAA have pointed out, it is not at all clear that Congress intended the statute to sweep as broadly as it has come to in practice. Legislative history
on the various relevant portions of the Act is sparse at best, but what is there argues that—at the very least—Congress did not intend the “unauthorized access” provisions of the Act to apply to insiders, but rather to outside hackers.\textsuperscript{163} And one piece of evidence arising from the negative implications of the Economic Espionage Act of 1996 strongly argues that Congress did not intend for there to be a federal civil remedy for trade secret theft at all.

The Computer Fraud and Abuse Act was originally passed in 1984, primarily in response to the publication of a number of computer crime studies and an upsurge in media reports of juvenile computer hacking.\textsuperscript{164} The Act was substantially amended in 1986, largely in response to criticisms from the Justice Department.\textsuperscript{165} Neither the original statute nor the 1986 amended version contained a private right of action—the focus of the statute was originally on empowering law enforcement to prosecute computer hackers who might otherwise escape punishment.\textsuperscript{166}

The addition of “exceeds authorized access” liability in the 1986 amendments, however, argues against the \textit{Shurgard/Citrin} interpretation of the statute. Congress added the term “exceeds authorized access” as a basis of liability to replace the prior version’s use of the phrase “or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.”\textsuperscript{167} The reason behind this change was to eliminate “one of the murkier grounds of liability, under which a [person’s] access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization.”\textsuperscript{168} This change argues strongly against the \textit{Shurgard/Citrin} interpretation of authorization, because that interpretation of authorization requires a court to look \textit{specifically at the purpose} of the accessor in accessing the information to determine whether that access—as in \textit{Citrin}—legally terminated the agency relationship. If the agent’s purpose in accessing the information at issue was impure, the agency relationship was terminated and the access was unauthorized.\textsuperscript{169} But, in 1986, Congress wanted to eliminate such a “murk[y]” ground of criminal liability from the statute. Therefore, the 1986 amendments counsel against a broad, legalistic interpretation of unauthorized access.\textsuperscript{170}

The incorporation of the private right of action, unfortunately, did not

\begin{itemize}
\item \textsuperscript{163} See, e.g., Int’l Ass’n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495–496 (D. Md. 2005) (describing the distinction the legislative history suggests).
\item \textsuperscript{164} See Griffith, supra note 3, at 459–60 (explaining that several published studies on computer crime, combined with an increase in media coverage on the topic, influenced Congress to quickly pass the 1984 Act).
\item \textsuperscript{165} See id. at 474 (stating that the 1986 amendments clarified several subsections of the 1984 Act).
\item \textsuperscript{166} See id. at 473 (noting that the Justice Department recommended patterning amendment language on the federal mail fraud and wire fraud acts).
\item \textsuperscript{169} See supra notes 50–61 and accompanying text (observing that the agency relationship ends and unauthorized access to a company’s computers arises when an agent’s motives are opposed to the employer’s interests).
\item \textsuperscript{170} See Int’l Assn. of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 499 n.12 (D. Md. 2005) (noting that Congress provided a clear definition for “exceeds authorized access”).
\end{itemize}
come with a clear indication of its intended scope. Subsection (g) was originally added to the Act by the Violent Crime Control and Prevention Act of 1994. 171 Because of the omnibus nature of that legislation (the Public Law itself is over 300 pages long), contemporaneous legislative history is difficult to sift through. 172 But four years earlier, the Senate Judiciary Committee approved the amendments that eventually found their way into the 1994 crime legislation, and published a report. 173 The report stresses the need to balance regulation of computer misuse against the threat of over-legislating in a way that stifles legitimate experimentation in computer use. 174 The amendments made two jurisdictional changes to the statute: they added the private right of action and expanded the statute’s general reach beyond “federal interest computers”—to which it had previously been confined—and to all “protected computers” as defined by the current statute. 175 In support of this broadening of the statute’s reach, the report mentions several high-profile and destructive incidents of hacking, virus writing, and worm transmission, and points to the United States’ scientific and economic reliance upon interstate computer networks. 176

The Senate Report gives short shrift to the addition of the private right of action to the statute. Other than a brief note that the private right of action is not intended to be used against government whistleblowers, the sum total of discussion of subsection (g) is: “the bill creates a new, civil remedy for those harmed by violations of the Computer Fraud and Abuse Act. This would boost the deterrence of the statute by allowing aggrieved individuals to obtain relief.” 177

Obviously, this sheds little light on Congress’ intent in adding a civil cause of action to the statute. But the language in the remainder of the report pointing to malicious computer hacking as the motivating force behind the statute further argues against a broad scope for the legislation.

The addition of the subsection (a)(2)(C) information theft crime in 1996 also argues against broad liability for unauthorized use of information. 178 The Senate Judiciary Committee Report on the amendments strongly hints that Congress’ intent behind the “accesses... without authorization... and thereby obtains... information” crime was to catch outside hackers, rather than faithless employees. 179 When addressing the information theft crime, most of the report simply parrots back the language of the statute itself. But at

---


172.  Id.


174.  Id.

175.  Id. at 7–8.

176.  Id. at 6–6.

177.  Id. at 6–7.


one point, when talking about the sentencing provisions, the report uses some telling language by referring to “individuals who intentionally break into, or abuse their authority to use, a computer and thereby obtain information.”

The language characterizes users “exceed[ing] authorized access” under subsection (a)(2) as those who “abuse their authority to use[] a computer,” but it brands those who would fall under the “access[...]. without authorization” prong as those who “intentionally break into” the computer at issue. This distinction implies that Congress intended the information-theft crime to apply to outsiders, and undercuts the Shurgard/Citrin interpretation of the Act’s authorization requirement.

Perhaps the most telling piece of evidence that Congress did not intend the CFAA to apply to trade secret theft arises by negative implication. In 1996, Congress passed the Economic Espionage Act. That Act makes it a federal crime to steal a trade secret related to a product that enters interstate or foreign commerce. Its definition of “trade secret,” by and large, tracks the UTSA definition. The House Report accompanying its passage notes again and again the great importance of trade secrets to the national economy, going so far as to equate threats to trade secrets with threats to the country’s national security. The Act empowers the Attorney General to initiate a civil proceeding to enjoin behavior that violates the statute, so that the trade secret at issue may be protected in advance of the criminal prosecution. And yet, for all that, the Act contains no private right of action, nor does it support civil federal question jurisdiction. If ever there had been a moment for Congress to extend the protection of federal law to the civil misappropriation of trade secrets, 1996 was it. Nevertheless, Congress chose not to rise to the occasion. This lack of action, in a context directly related to trade secret law, argues against interpretations of the CFAA that force it to do what the drafters of the Economic Espionage Act chose not to do.

Overall, the legislative history of the CFAA does not categorically answer the question of whether Congress intended the Act to bring trade secret misappropriation claims into federal court on the back of CFAA violations. At best, the CFAA is a haphazard statute, which has been patched up again and again without much regard for its cumulative effects and implications. But viewed as a whole, the legislative history at the very least argues against the Shurgard/Citrin interpretation of the statute, and gives the impression that the

180. Id. at 8.
188. Witness, as a case in point, the 2008 amendments. Congress removed the interstate communication requirement from subsection (a)(2)(C) without for a moment considering what effect that might have on civil cases under the Act. See supra notes 35–38 and accompanying text.
Act was intended to be only of modest scope.

B. Federalism Concerns

Allowing trade secret claims into federal court on the back of CFAA claims works one last harm, more theoretical but no less serious. One of the bedrock principles of the United States federal government is that it is one of limited and enumerated powers. The limitations on federal courts laid out in Article III of the Constitution ensure that those courts do not invade the province of state law except when their jurisdictional prerequisites are met. The strictures on federal court subject-matter jurisdiction are so tight that even when a case is patently frivolous on the merits, a federal court may not exercise jurisdiction to dismiss it without first examining its constitutional and statutory power to do so.

The CFAA can provide a valid source of federal question jurisdiction, and when it is invoked by a plaintiff in the manner Congress intended—with sufficient allegations to survive a motion to dismiss—no federalism problem arises. Such a case fits into one of the limited categories in which a federal court may adjudicate a state law claim without offending our notions of federalism. If, on the other hand, a plaintiff pleads a skeleton CFAA claim—perhaps even alleging only Shurgard/Citrin-style unauthorized access—merely for the purpose of getting her trade secret misappropriation claim heard by a federal judge, then the state/federal balance so carefully preserved by the Founders in the Constitution may be threatened.

Implied preemption of state law under the Supremacy Clause of the Constitution implicates similar federalism questions and values. To be clear: this Article does not argue that the CFAA preempts state trade secret law, nor that it should. In passing the CFAA Congress did not explicitly exercise its power under the Supremacy Clause to displace any state law. But the policy issues that arise both in implied preemption and in the nexus between the CFAA and trade secret law counsel courts and legislators to think long and hard about the balance between federal and state power. The basic assumption of courts in implied preemption cases is that “the historic police powers of the States [are] not to be superseded by [a] Federal Act unless that was the clear and manifest purpose of Congress.” The Supreme Court,

189. See Marbury v. Madison, 5 U.S. (1 Cranch) 137, 180 (1803) (holding that all branches of the federal government are constrained by the U.S. Constitution).
190. U.S. CONST. art III, § 2. See also Mansfield, Coldwater & Lake Mich. Ry. Co. v. Swan, 111 U.S. 379, 383–84 (1884) (holding that the case must be remanded to state court when federal courts were not granted jurisdiction by the U.S. Constitution over the matter, even if both parties wish to proceed in federal court).
191. See Steel Co. v. Citizens for a Better Env’t, 523 U.S. 83, 89–90 (1998) (rejecting the position that courts may assume the existence of subject-matter jurisdiction in order to dismiss a case on the merits).
192. U.S. CONST. art. VI, cl. 2.
193. See Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003) (discussing Congress’s reluctance to preempt or interfere with local and state computer crime authorities when it initially passed the CFAA).
demonstrating what some have called an attitude of “New Federalism,”195 has in its most recent implied preemption cases ruled against giving broad preemptive effect to federal statutes in the absence of an explicit preemption provision.196 Congress in passing the CFAA made no “clear and manifest” statement that it intended in any way to affect state trade secret law. Trade secret law—as an exercise of the state police power—deserves the same presumption of validity outside the implied preemption arena, and courts should avoid interpreting the CFAA in a manner that undermines trade secret law’s basic policies.197

The Court, in fact, has recognized a canon of statutory construction that instructs courts to avoid interpreting federal statutes in a manner that treads too heavily upon state sovereignty and areas of state regulation.198 In Gregory v. Ashcroft199 and BFP v. Resolution Trust Corp.,200 the Court, in essence, required that Congress, when it intends for a law to impact areas of state sovereignty or traditional state regulation, make a clear statement to that effect.201 If, as argued above, Congress did not intend for the CFAA to significantly impact state trade secret law, courts could use this canon of statutory construction to police the boundaries between the federal and state spheres.202

As it currently exists, the CFAA poses a threat to the federal-state balance which is every bit as serious as the risk it poses to the balance between the employee and the employer in the substantive area. In order to safeguard federalism in the trade secret context, as well as to serve Congress’ intent, the jurisdictional problems the CFAA creates should be resolved—if not by Congress, then by the courts.

195. See Allison H. Eid, Preemption and the Federalism Five, 37 Rutgers L.J. 1, 7–8 (2005) (arguing, pre-Altria and Wyeth, that the new federalism had not yet reached the area of preemption).
196. See Wyeth v. Levine, 129 S. Ct. 1187 (2009) (rejecting argument that state-law failure-to-warn tort claims were preempted by FDA labeling requirements); Altria Group, Inc. v. Good, 129 S. Ct. 538 (2008) (denying preemptive effect to the Federal Cigarette Labeling and Advertising Act). It is notable, however, that in both the recent preemption decisions the Justices in the majority were not the “Federalism Five” identified in Eid, supra note 209.
197. See supra notes 151–159 and accompanying text (discussing how trade secret law protects confidential business information in a more policy-positive manner).
198. See Felix Frankfurter, Some Reflections on the Reading of Statutes, 47 Colum. L. Rev. 527, 540 (1947) (“[W]hen the Federal Government . . . radically readjusts the balance of state and national authority, those charged with the duty of legislating [should be] reasonably explicit . . . .”).
201. See Phillip P. Frickey, Revisiting the Revival of Theory in Statutory Interpretation: A Lecture in Honor of Irving Younger, 84 Minn. L. Rev. 199, 211–12 (1999) (discussing the creation and expansion of the “clear statement rule”). Concededly, a core element of Justice O’Connor’s opinion in Gregory was that applying the ADEA to state-court judges would impinge on “the heart of representative government,” an area within which trade secret law does not likely lie. Gregory, 501 U.S. at 463. But Justice Scalia’s extension of the federalism canon in BFP brings it far closer to the realm of ordinary tort law—the Justice argued that “the essential sovereign interest in the security and stability of title to land” sufficed to invoke the canon. BFP, 511 U.S. at 545 n.8. See also Rapanos v. United States, 547 U.S. 715, 738 (2006) (Scalia, J.) (plurality opinion) (citing BFP to reject a broad interpretation of the Clean Water Act).
202. See Jenna Bednar & William N. Eskridge, Jr., Steadyng the Court’s “Unsteady Path”: A Theory of Judicial Enforcement of Federalism, 68 S. Cal. L. Rev. 1447, 1458–60 (1995) (noting that while the Court’s opinions in Gregory and BFP do not necessarily require courts to police the boundary, the cases’ logic implicitly permits them to do so).
V. Two Solutions

The Computer Fraud and Abuse Act, abetted by loose language and overly-broad judicial interpretations, creates two significant problems. On the one hand, it occupies much the same space as trade secret law, but without that body of law’s policy-based protections and balancing mechanisms. On the other hand, it provides an easy way for claims—either entirely based upon the Act or upon a combination of the CFAA and trade secret law—to get into federal court, thus contravening Congress’ intent in passing it and damaging fundamental notions of federalism. This Part proposes two solutions. First, from the legislative side, Congress should amend the CFAA to strip out the information theft crime from the private right of action, or alternatively enact the more restrictive definition of “authorization.” Second, from the judicial end, courts considering CFAA-based complaints should take a hard look at the plaintiff’s allegations to determine whether state trade secret law substantially predominates over the CFAA claim, and if so, these courts should dismiss the state law claims.

A. Fixing the Problems Legislatively

If Congress chooses to act to fix the two problems identified in this Article, it could do so in one of two ways. First, and most comprehensively, it could—and should—amend the CFAA to remove the subsection (a)(2)(C) crime from the ambit of the private right of action. If, however, Congress wishes to take a more modest approach, it could add a statutory definition of the term “authorization” that overturns the Shurgard/Citrin reading of the statute and reins in some of its greatest excesses.

1. Remove Subsection (a)(2)(C) from the Private Right of Action

In order to solve the problems set out thus far in this Article, Congress should amend the private right of action in the CFAA to exclude from its ambit the subsection (a)(2)(C) information theft crime. The amended subsection should thus read:

Any person who suffers damage or loss by reason of a violation of this section, other than a violation of subsection (a)(2)(C), may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in sub-clauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct

203. Before diving in, however, a brief digression may be in order. As the Lori Drew prosecution mentioned at the beginning of this Article reveals, the interaction between the civil justice system and the CFAA has the potential to create many more—and possibly greater—problems than just the two examined in this Article. In a perfect world, the true solution to all of these problems may be to remove the private right of action from the Act altogether. At the very least, a credible argument could be made that the private right of action is more trouble than it is worth. That argument, however, is for another day and another article. This one shall continue with a tight focus on solving the problems that the CFAA creates for trade secret law.
described in (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

The added language removing subsection (a)(2)(C) crimes appears in italics. This simple legislative action would completely prevent both problems this Article addresses. Without a civil cause of action for information theft from computers, companies whose faithless employees steal trade secrets—whether or not in violation of a legal duty of loyalty and whether or not they had technological access to the computer—will have to turn to the UTSA or common law trade secret misappropriation for relief. And with Congress clearly expressing its intent that subsection (a)(2)(C) does not support federal question jurisdiction, those companies will take their claims where they belong: to state court.\footnote{204}

Removing subsection (a)(2)(C) from the private right of action will also help re-focus the CFAA and serve the goals Congress intended in originally passing the statute. Congress initially passed the Act to combat hacking.\footnote{205} Subsequent amendments have increased its scope to encompass fraud, the creation of viruses and worms, and intentionally damaging a computer system.\footnote{206} Employee misappropriation of trade secrets does not cleanly fit into any of those categories, and removing it from the statute’s scope would in no way do violence to Congress’ intent. And as the Drew prosecution illustrates,\footnote{207} having a body of broad civil interpretations of the statute—interpretations adopted in a setting with a lower evidentiary burden and without the rule of lenity—can have worrisome consequences when prosecutors use those cases to further expand the reach of the statute in the criminal realm.\footnote{208}

Finally, this legislative approach is not without precedent in the history of the statute itself. When Congress amended the Act in 1994, it added both the private right of action and subsection (a)(5) computer damage crimes.\footnote{209} But that first version of subsection (g) excepted the subsection (a)(5)(B) crimes—

\footnote{204. That is, of course, assuming that they cannot fulfill the requirements of the diversity jurisdiction statute. See 28 U.S.C. § 1332 (2006) (requiring that the parties be citizens of different states or non-U.S. citizens and that the matter in controversy exceed the sum or value of $75,000). Diversity jurisdiction cases, however, implicate a host of different federalism-based policy concerns, and those issues are beyond the scope of this Article. See, e.g., David Marcus, Erie, the Class Action Fairness Act, and Some Federalism Implications of Diversity Jurisdiction, 48 WM. & MARY L. REV. 1247 (2007) (discussing the impact of judicial preferences on the federalism balance of power).}

\footnote{205. See supra note 169 and accompanying text (discussing the impetus for passage of the CFAA).}

\footnote{206. See supra notes 171–85 and accompanying text (discussing subsequent amendments to the Act and concomitant congressional intent).}

\footnote{207. See supra note 1 and accompanying text (noting the use of civil precedents to find criminal liability in the MySpace cyberbullying verdict against Lori Drew).}

\footnote{208. See Kerr, supra note 7, at 1598–99 (discussing the potential impact of having an uncertain scope of the term “unauthorized access” in the CFAA).}

\footnote{209. See supra note 180 and accompanying text (comparing the original version of the statute to the newer version, which allowed for civil actions against crimes falling under (a)(5)(B)).}
in essence, transmission of code in reckless disregard of a substantial risk that it will damage a computer—from the private right of action.\textsuperscript{210} In fact, the new language this Article proposes for subsection (g) is modeled on that original version of the private right of action. The 1994 amendment also added to the statute subsection (h), which required the Attorney General and the Secretary of the Treasury to report to Congress on the enforcement of subsection (a)(5) crimes each of the first three years the statute was in effect.\textsuperscript{211} At a minimum, this subsection indicates that Congress was unsure of the effect of the new transmission-based crimes, and so included two safety measures—it exempted them from the private right of action and required annual reports on their enforcement.\textsuperscript{212} So an approach that treats some of the substantive crimes differently with respect to civil causes of action is hardly unprecedented.

One consequence of removing subsection (a)(2)(C) crimes from the private right of action, however, is that some plaintiffs harmed by subsection (a)(2)(C) violations will be unable to obtain redress in the civil system. But this is not as serious a possibility as it might first appear. First, when truly valuable secret information is stolen from a company in any way—not just through computer access—redress by way of trade secret law would remain available. If a company cannot prove that the information was a trade secret under the UTSA or common law, then it is simply not information that the law should protect. This is not a problem in trade secret law, so it is difficult to see why it would be a problem from the computer law perspective.

Second, the CFAA’s other computer crimes would remain viable as civil causes of action. So if information was stolen as part of an intentional act of fraud, a company could still sue under subsection (a)(4). If the wrongful access of a company’s computer caused damage—for instance, if a departing employee vandalized the company’s servers—subsection (a)(5) would still provide a civil remedy.\textsuperscript{213} If a company faced extortive threats that involved computer damage, they could still sue the perpetrator under subsection (a)(7).\textsuperscript{214} One thing that all these remaining crimes have in common is that they are all far more firmly tied to the congressional intent behind the Act—deterring hacking and computer misuse—than the information theft crime. Therefore, excepting subsection (a)(2)(C) from the private right of action should not have a great effect on those meritorious CFAA claims that fall within Congress’ intent when the statute was originally passed.

2. Define “Authorization” to Overturn Shurgard/Citrin

If Congress wished to repair some of the problems identified in this Article but did not want to go so far as to remove subsection (a)(2)(C) from the private right of action, it could take a more moderate approach. Many of the

\textsuperscript{210} 18 U.S.C. § 1030(g) (1994).
\textsuperscript{211} 18 U.S.C. § 1030(h) (1994).
\textsuperscript{212} See supra Part II.A (discussing the development of information theft laws under the CFAA).
\textsuperscript{213} Id.
\textsuperscript{214} Id.
The greatest problems with the CFAA in the trade secret context stem from the Shurgard/Citrin line of cases that interpret the term “authorization” broadly to encompass improper use of information or access in violation of a legal duty of loyalty.\textsuperscript{215} The sounder reading of the statute confines “unauthorized” access to that which bypasses a code-based technological or physical barrier to access of a computer system.\textsuperscript{216} By a simple statutory addition, Congress could enshrine this interpretation and bind the courts to it. Such an amendment to subsection (e) of the statute could read:

\begin{quote}
(13) the term “authorization” means 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.
\end{quote}

This amendment would foreclose the Shurgard/Citrin argument that access that is authorized by a username and password becomes unauthorized as soon as the employee has an impure motive and thus violates a legal duty of loyalty to the employer.

In sum, Congress should take action to curtail broad applications of the CFAA that threaten to displace state trade secret law. Either it should remove subsection (a)(2)(C) crimes from the CFAA’s private right of action, or should define authorization to eliminate the Shurgard/Citrin interpretation. By doing so, Congress could help restore the proper balance between state and federal law, between trade secret law and computer misuse statutes.

\textbf{B. Judicial Solutions to the Problems}

If, on the other hand, Congress fails to take action on this issue, it falls to the federal courts to ensure that the CFAA does not overly upset the balance between state and federal law. In order to do so, judges should reject the Shurgard/Citrin interpretation of unauthorized access and carefully examine CFAA-based complaints and exercise discretion to dismiss state-law trade secret claims under the supplemental jurisdiction statute.

\textbf{1. Reject Shurgard/Citrin}

As recounted above, a number of district courts and the Seventh Circuit have embraced a broad, legalistic interpretation of when computer access is unauthorized.\textsuperscript{217} This interpretation broadens the scope of unauthorized access beyond just those users who do not have physical or technological access to the computer at issue and encompasses those whose motives for accessing the computer are somehow impure.\textsuperscript{218} But some courts, including the Ninth Circuit, have begun to reject that interpretation, and hold that access is only unauthorized when the accessing party has not been granted a user account, or

\textsuperscript{215} See supra notes 55–73 and accompanying text (discussing differing opinions on the issue of whether unauthorized access should be interpreted to include unauthorized disclosure).

\textsuperscript{216} See Kerr, supra note 6, at 1648–60.

\textsuperscript{217} Supra Part I.C.1.

\textsuperscript{218} Id.
similar code-based permission to use the computer system. 219

Federal courts considering CFAA-based complaints should reject the Shurgard/Citrin interpretation of the statute, and embrace the technology-centric view of authorization. As noted above, the technological interpretation better comports with the available legislative history and other evidence of Congress’ intent in passing the Act. 220 But rejecting Shurgard/Citrin is also sound policy: doing so will route the most common trade secret-like CFAA claims—faithless employee misconduct claims—out of federal court and back into the state courts. 221 It will also put the burden of maintaining data security on the same party with whom trade secret law places it: the employer. 222 The employer is in the best position to determine who should and should not have access to its computer systems, and so the employer should bear the burden of determining who, for the purposes of the statute, has authorized access. If an employer fails to cancel an employee’s user account and that employee uses the account to steal information, the employer should not be afforded a remedy beyond that already given by trade secret law, simply because the employee used a computer. If courts reject the Shurgard/Citrin interpretation of unauthorized access, they will go a long way toward returning the CFAA to the limited role that Congress intended for it. 223

As an added justification for rejecting the legalistic interpretation of authorization, courts might look to the in pari materia canon of statutory interpretation in order to avoid creating a conflict between the CFAA and the Economic Espionage Act. As discussed above, 224 the EEA makes trade secret theft a federal crime, but does not include a private right of action. The in pari materia canon instructs courts to interpret federal statutes in harmony with one another. 225 Thus, if the EEA refuses to provide a federal civil remedy for trade secret misappropriation, courts should not interpret the CFAA—a statute far less on-point to trade secret theft than the EEA—to do so. 226

In short, whether a court chooses to reject the Shurgard/Citrin interpretation outright as a matter of the statute’s text and precedent, or as a consequence of an interpretation that is in harmony with the Economic

219. Supra notes 66–73 and accompanying text.
220. Supra notes 162–188 and accompanying text.
221. Supra Part III.B.
222. See LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (“It is the employer’s decision to allow or to terminate an employee’s authorization to access a computer that determines whether the employee is with or ‘without authorization.’”).
223. Supra notes 161–189 and accompanying text.
224. Supra notes 186–190 and accompanying text.
225. See William N. Eskridge, Public Values in Statutory Interpretation, 137 U. Pa. L. Rev. 1007, 1039–40 (1989) (“Where a federal law is similar to (in pari materia with) another federal law, the Court will presumptively interpret the former law consistently with the other . . . .”).
226. While the in pari materia canon most often applies in circumstances in which statutes incorporate language similar or identical to other statutes, see id., courts have applied its spirit where the objects of two statutes are similar. See, e.g., Dowling v. United States, 473 U.S. 207, 217–18 (1985) (refusing to apply the National Stolen Property Act to copyright infringement because of the difference between tangible property and the intangible rights created by Copyright Act); United States v. LaMacchia, 871 F. Supp. 535, 544–45 (D. Mass. 1994) (dismissing wire fraud indictment for posting copyright-protected software online for download, where the Copyright Act would not have imposed criminal liability).
Espionage Act, courts addressing CFAA violations should hold that access without authorization is only that which bypasses a code-based limitation on access to information in a computer system.

2. Use Supplemental Jurisdiction Discretion to Dismiss Trade Secret Claims

In addition to narrowly interpreting authorization, federal district judges have another tool empowering them to police the federal-state balance: the supplemental jurisdiction statute’s discretionary dismissal provisions. Section 1367(c) reads:

The district courts may decline to exercise supplemental jurisdiction over a claim under subsection (a) if –

(1) the claim raises a novel or complex issue of State law,
(2) the claim substantially predominates over the claim or claims over which the district court has original jurisdiction,
(3) the district court has dismissed all claims over which it has original jurisdiction, or
(4) in exceptional circumstances, there are other compelling reasons for declining jurisdiction.

At the outset, if and when a court does dismiss a CFAA claim that is the sole basis for federal jurisdiction in an action, it should immediately dismiss the remaining trade secret claims under subsection (c)(3). But even prior to dismissal, district courts must bear in mind that “pendent jurisdiction is a doctrine of discretion, and not of plaintiff’s right.”

If the trade secret issue in a case is particularly thorny, courts should decline to exercise jurisdiction over it under § 1367(c)(1). Most garden-variety state law claims—tort claims, contract disputes, etc.—will not raise novel issues of state law. Trade secret law must constantly evolve to keep up with advancements in technology, however, and that evolution should take place in state, rather than federal, courts. So if the factual questions underlying the trade secret issue in a CFAA-based case—or the application of trade secret law itself to those facts—are novel with respect to the state law, the federal court should dismiss the state law claims. Under § 1367, declining jurisdiction due to “exceptional circumstances” is warranted when supported by judicial economy, convenience, and fairness to the parties, as well as whether all the

---

230. See POOLEY, supra note 86, at § 1.02[1] (explaining that advances in technology cause difficulty in surrounding issues of trade secrets). Cf. Kyle W. Brenton, Note, BONGHITS4JESUS.com? Scrutinizing Public School Authority over Student Cyberspeech Through the Lens of Personal Jurisdiction, 92 MINN. L. REV. 1206, 1206 (2008) (providing the example of school administrators censoring speech online as advances in technology have moved this expression to the Internet).
claims would be expected to be tried together.\textsuperscript{231} Such determinations must obviously be made on a case-by-case basis, but a judge should not shy away from declining to rule on complicated issues of trade secret misappropriation merely because the plaintiff has made out a bare-bones CFAA subsection (a)(2)(C) claim for information theft.\textsuperscript{232}

Finally, § 1367(c)(2) gives judges leave to decline jurisdiction when pendant state law claims substantially predominate over federal claims granting subject-matter jurisdiction.\textsuperscript{233} A state-law claim may substantially predominate over a federal one “in terms of proof, of the scope of the issues raised, or of the comprehensiveness of the remedy sought.”\textsuperscript{234} A district court should dismiss under § 1367(c)(2) when “a state claim constitutes the real body of the case, to which the federal claim is only an appendage—only where permitting litigation of all claims in the district court can accurately be described as allowing a federal tail to wag what is in substance a state dog.”\textsuperscript{235} At least one federal court of appeals has found substantial predominance where a complex and important state-law regulatory scheme addresses the same conduct as a simpler, more straightforward federal statute.\textsuperscript{236}

One federal district court, when confronted with a case involving a CFAA claim joined to at least nine state-law claims arising out of an employment relationship removed to federal court, elected to exercise § 1367(c)(2) discretion to return the state claims to state court, but retain the CFAA claim in federal court.\textsuperscript{237} The court first recognized that it had valid supplemental jurisdiction over the state-law claims based on § 1367(a).\textsuperscript{238} It noted, however, that the slim evidence required to prove the CFAA claim was dwarfed by the scope of the issues and proof required for the state claims, which included breach of contract and fiduciary duty, fraud, conversion, and a number of other theories.\textsuperscript{239} Because of this evidentiary predominance, as well as to avoid unnecessarily deciding contested issues of state law,\textsuperscript{240} the court exercised its discretion to remand the state claims to state court, while retaining jurisdiction

\textsuperscript{231} Parker v. Scrap Metal Processors, Inc., 468 F.3d 733, 745 (11th Cir. 2006) (noting what courts consider under the “exceptional circumstances” prong).

\textsuperscript{232} Additionally, if a case is pending in state court involving the same factual situation and issues as a federal CFAA claim, a court may consider dismissing the action based on the abstention doctrine of \textit{Colorado River Water Conservation Dist. v. United States}, 424 U.S. 800 (1976). See, e.g., H&R Block Tax Services, Inc. v. Rivera-Alicea, 570 F. Supp. 2d 255, 265–69 (D.P.R. 2008) (dismissing CFAA claim under \textit{Colorado River} where a parallel claim was pending in the Puerto Rico Commonwealth Court).


\textsuperscript{234} United Mine Workers of Am. v. Gibbs, 383 U.S. 715, 726–27 (1966) (laying out federal common law factors that have been interpreted as applying to later supplemental jurisdiction statute).


\textsuperscript{238} Id. at *3.

\textsuperscript{239} Id. at *3–5.

\textsuperscript{240} Cf. Gibbs, 383 U.S. at 726 (“Needless decisions of state law should be avoided both as a matter of comity and to promote justice between the parties, by procuring for them a surer-footed reading of applicable law.”).
over the federal CFAA claim.\textsuperscript{241}

Section 1367(c)(2) provides a perfect vehicle for judges to smoke out cases in which a CFAA is nothing more than a federal computer-abuse tail wagging a state trade secret dog. As laid out above, the proof required in a CFAA subsection (a)(2)(C) claim will almost always be significantly simpler and more straightforward than in a trade secret claim.\textsuperscript{242} A trade secret law claim raises far more involved public policy issues and questions of commercial morality than does a CFAA information theft claim.\textsuperscript{243} Moreover, the remedies provided for in the UTSA are both more certain and more comprehensive than the underdeveloped remedy provisions in CFAA subsection (g).\textsuperscript{244} Therefore, in many cases, a judge may have—under section 1367(c)(2)—the discretion to sever state law trade secret claims from federal civil suits under the CFAA.

Both Congress and the courts have the power to fix some or all of the problems that arise when trade secret law meets the CFAA. The legislative solutions are cleaner, surer, and will result in substantially less litigation. But Congress moves slowly. In the absence of legislative action, courts must bear the burden of policing the boundaries between computer misuse and trade secret misappropriation, and their discretion under the supplemental jurisdiction statute provides them the perfect tool with which to do so.

VI. CONCLUSION

Over the years, trade secret law has proven both resourceful and flexible as it has been called upon to deal with the ever-increasing pace of technological development in American society. But with the passage of the Computer Fraud and Abuse Act in 1984, the addition of a private right of action in 1994, and the broadening of the information theft crime in 2008, technology may have finally overtaken it.

The CFAA creates two major problems for trade secret law, one substantive and one jurisdictional. Both could be solved either by Congress amending the statute to except the information theft crime from the private right of action, or by federal judges declining to exercise supplemental jurisdiction over state law trade secret claims appended to CFAA claims.

\textsuperscript{241} Contemporary Servs., 2008 WL 3049891, at *5.
\textsuperscript{242} Supra notes 83–86 and accompanying text.
\textsuperscript{243} See supra notes 101–104 and accompanying text (differentiating between the policy issues required by CFAA information theft claim and trade secret law claim).
\textsuperscript{244} See supra notes 117–25 and accompanying text (explaining the remedies available under both UTSA and CFAA).