Bloomberg BNA

BNA's
Patent, Trademark & Copyright Journal®

TRADE SECRETS

Attorneys from Morgan, Lewis & Bockius, in the fifth installment in a series of articles examining trade secrets issues in the U.S., argue that the confusion over when a defendant ''exceeds authorized access'' under the Computer Fraud and Abuse Act begs for congressional resolution.

Stealing Trade Secrets and Confidential Information With Computers: Time to Resolve the Lingering Circuit Split

MARK L. KROTOSKI AND BROCK DAHL

When a trusted employee steals company trade secrets and confidential business information using the company's computer, does this conduct violate federal computer crime laws? Surprisingly, the answer currently depends on where the theft occurred. Whether the employee has ''exceeded'' his ''authorized access,'' a critical determination in whether the employee violated the Computer Fraud and Abuse Act (''CFAA'') (the primary federal computer crime statute) turns on how the courts construe key terms in the statute. For more than five years, the courts have been divided on whether this stealing of information violates the CFAA.[1]

Given increasing concerns over the theft of trade secrets and confidential information by insiders and others, it is important that the discrepancies in applying the law be addressed. This article reviews some of the judicial and legislative options to resolve this lingering, recurring issue.

Mark L. Krotoski is a Litigation Partner in the Privacy and Cybersecurity and Antitrust practices of Morgan, Lewis & Bockius. He previously served as the National Coordinator of the Computer Hacking and Intellectual Property Program in the Criminal Division of the U.S. Department of Justice.

Brock Dahl is an Associate in the Litigation and Privacy and Cybersecurity Groups of Morgan, Lewis & Bockius, resident in the Washington, D.C. office. He formerly worked at the Silicon Valley office of an international law firm and at the Department of the Treasury.

CFAA Background: Key Statutory Language

The CFAA, originally enacted in 1984,[2] and amended through the years,[3] has both criminal penalties and civil

[1] *See, e.g., LVRC Holdings LLC, v. Brekka*, 581 F.3d 1127, 1134-35 (9th Cir. 2009) (noting disagreement with Seventh Circuit construction); *see also United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010) (noting disagreement with Ninth Circuit construction of the CFAA); *Orbit One Communications, Inc. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385 & nn. 65-66 (S.D.N.Y. 2010) (noting the division among federal circuit and district court cases construing the CFAA).

[2] 18 U.S.C. § 1030. Section 1030 was originally enacted in 1984. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified at 18 U.S.C. § 1030 *et seq.*).

[3] After its original enactment, the statute was amended two years later under the Computer Fraud and Abuse Act of 1986.

remedies including a private right of action, injunctive or other equitable relief.[4] The CFAA focuses on whether the computer access was either ''without authorization'' or ''exceeds authorized access.''[5] As the Seventh Circuit has observed, ''The difference between 'without authorization' and 'exceeding authorized access' is paper thin, but not quite invisible.''[6]

To provide a more specific example, Section 1030(a)(2) prohibits obtaining protected information by accessing a computer ''without authorization'' or where one ''exceeds authorized access.''[7] There is no definition in the statute for the terms ''without authorization.'' The phrase ''exceeds authorized access,'' was added in 1986.[8] These terms are defined to mean ''to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.''[9]

Interpretative questions about the CFAA frequently arise in trade secret theft cases because the employee or insider was given ''authorized access'' to valuable information with company computers, but then abused that access in inappropriate ways. For example, in 2012, a district court in the Southern District of New York found that a Goldman Sachs employee did not violate the CFAA when he misappropriated computer source code used in a high-frequency trading system since he did not unlawfully ''access'' the computer.[10] On his last day of employment, the employee ''copied, compressed, encrypted, and transferred'' the source code ''to an outside server in Germany,''[11] but the district court found that the phrases ''without authorization'' and ''exceeds authorized access'' do not encompass an employee's misuse or misappropriation of information since the employee had authorized access. The CFAA count was dismissed while the trade secret theft count proceeded to trial and subsequent appeal. But as will be seen below, other courts would disagree with this application of the statutory language.

In considering options to resolve the dispute between the courts, it helps to review how the division arose. In general, the circuits adhere to either a broad or narrow interpretation of the statute's reach.

The Broad Interpretation

So far, most of the circuits considering this issue have adopted a broad interpretation of the statutory language.

Seventh Circuit: Breaching a Duty of Loyalty. The Seventh Circuit considered the scope of the CFAA in a civil case where an employee decided to quit a company and destroy files on his company laptop implicating him in wrongdoing before he returned the laptop.[12] Judge Richard Posner, writing for the court, concluded that the employee's ''breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship.''[13] Consequently, his further access to the computer was *without authorization* and violated the CFAA.[14]

First Circuit: Contrary to Non-Disclosure and Use Terms. The First Circuit shares this broader view.[15] In a civil case, the vice president of a company called Explorica, who had formerly been a vice president at a different company named EF Cultural Travel BF, determined to use a scraper to remove pricing information from EF's website for his own competitive pricing purposes.[16] Notably, the employee violated the non-disclosure and use terms of a confidentiality agreement by providing the party he hired to apply the scraper ''proprietary information about the structure of the website and tour codes'' which ''might reasonably be construed to be contrary to the interests of EF.''[17]

Fifth Circuit: Limited Purpose Access. In a criminal case before the Fifth Circuit, a Citigroup employee accessed and printed information to at least seventy-six corporate customer accounts to which she had access as part of her job, providing it to others who incurred fraudulent charges using the information.[18] Though the defendant argued that the statute did not prohibit the unauthorized *use* of material she was authorized to access, the Fifth Circuit held that ''authorized access'' can encompass use limits, ''at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime.''[19] In this case, the defendant's ''access to Citigroup's data was confined'' as she ''was not authorized to access that information for any and all purposes but for limited purposes.''[20]

Eleventh Circuit: Non-Business Purpose. In another criminal case, an employee of the Social Security Administration accessed the personal records (including social security numbers) of individuals without a busi-

---

See Pub. L. No. 99-474, 100 Stat. 1213 (1986). The statute has been amended several times, including in 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008.

[4] 18 U.S.C. § 1030(g) (civil private right of action). The private right of action was added in 1994. *See* Pub. L. 103–322, title XXIX, § 290001(b)–(f), Sept. 13, 1994, 108 Stat. 2097–2099.

[5] For the terms ''exceed authorized access,'' *see* 18 U.S.C. § § 1030(a)(1), (a)(2), (a)(4). For the terms ''without authorization,'' *see* 18 U.S.C. § 1030(a)(1)-(7).

[6] *International Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418, 420 (7th Cir. 2006) (citations omitted).

[7] 18 U.S.C. § 1030(a)(2).

[8] Pub. L. No. 99-474, 100 Stat. 1213, 1215 (1986); *see also* H. Rep. No. 99-612, 99th Cong., 2d Sess. 11 (1986) (noting change).

[9] 18 U.S.C. § 1030(e)(6).

[10] *United States v. Aleynikov*, 737 F. Supp. 2d 173 (S.D.N.Y. 2010), rev'd on other grounds, 676 F.3d 71 (2nd Cir. 2012), superseded by statute, as stated in *United States v. Yihao Pu,* 15 F. Supp. 3d 846 (N.D. Ill. 2014) (noting the amendments to the Economic Espionage Act, not related to the CFAA).

[11] *Aleynikov*, 737 F. Supp. 2d at 175.

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

[13] *Id.* at 420-21.

[14] *Id.*

[15] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st 2001).

[16] *Id*. at 579.

[17] *Id*. at 581-83. Because of the existence of this broad confidentiality agreement, the court found it unnecessary to consider the general meaning of the CFAA or whether using a scraper alone constitutes unauthorized access. *Id*. at 581-82.

[18] *United States v. John*, 597 F.3d 263, 269 (5th Cir. 2010).

[19] *Id*. at 271.

[20] *Id*. at 272.

  PTCJ ISSN 0148-7965

ness reason in violation of the Administration's policy.[21] The Eleventh Circuit found the employee had violated the CFAA because he had been put on notice by the Administration that he was not authorized to obtain personal information for non-business reasons.[22] The court found that his ''use'' of the information was ''irrelevant'' insofar as it determined that he exceeded authorized access when he obtained the information for a non-business reason.[23]

The Narrow Interpretation

Two circuits are in the narrow interpretation camp. The Ninth Circuit was the first to adopt this view followed by the Fourth Circuit.

Ninth Circuit: Access But Not Use Restrictions. An en banc panel of the Ninth Circuit, in *United States v. Nosal*, determined that the CFAA is not meant to cover the misuse or misappropriation of information, but rather its ''unauthorized procurement or alteration.''[24] In *Nosal*, a former employee of the company coaxed current employees to use their log-in credentials ''to download source lists, names and contact information from a confidential database on the company's computer,'' and then sent the information to the former employee.[25] The court confronted the question of whether this conduct fell under the CFAA, and held that the statute was ''limited to violations of restrictions on access to information, and not restrictions on its use.''[26] In particular, the court said the purpose of the CFAA was to punish hacking, but not the misappropriation of trade secrets.[27]

Prior to *Nosal*, in *Brekka*, the Ninth Circuit had rejected the Seventh Circuit's breach of duty theory and found that an employee who was still employed could not have accessed his computer ''without authorization.''[28] There, an employee emailed a number of company files to himself while still working for the company.[29] The Ninth Circuit disavowed any notion that authorization for an employee to use a company computer ceases when an employee resolves to use the computer contrary to the employer's interest, saying that the very existence of the phrase ''exceeds authorized access'' belies such a claim.[30] The court ultimately held that ''a person uses a computer 'without authorization' . . . when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.''[31]

Fourth Circuit: No Remedy without Rescission. Finally, the Fourth Circuit was confronted with a case where a former employee of WEC allegedly downloaded company confidential materials, resigned, and then provided those materials to a competitor.[32] The court determined that the CFAA does not ''provide a remedy for misappropriation of trade secrets or violation of a use policy where authorization has not been rescinded.''[33] The Fourth Circuit was persuaded by the Ninth Circuit analysis.

Two Paths For Resolving the Deepening Court Split

Given the division among the courts, this important issue has two paths for resolution. First, the Supreme Court could resolve this issue. However, there are some tradeoffs under this option. Second, Congress could amend the CFAA to clarify this issue. Both of these avenues are considered next.

First Avenue: Supreme Court Resolution

When significant disagreement over the construction of a statute arises, normally the Supreme Court can resolve the division and decide the matter once and for all. The Rules of the Supreme Court of the United States provide that the Court may consider whether a ''United States court of appeals has entered a decision in conflict with the decision of another United States court of appeals on the same important matter'' as one key consideration for exercising discretionary review.[34]

Given the importance of this issue, and the divergence in case law, the Supreme Court would be fully justified in granting review to resolve this statutory construction issue under the CFAA. Criminal enforcement of the CFAA and civil remedies result in disparate application based on the same or similar facts. Employers lack clarity on the application of the law.

In 2013, the Supreme Court dismissed the petition for certiorari review of the Fourth Circuit case in *WEC Carolina Energy Solutions LLC v. Miller*, after the parties stipulated to dismiss the petition.[35] In the *Nosal* case, the Solicitor General's Office elected not to seek Supreme Court review.[36]

Even if an ideal case were identified to present this issue, there are constraints to Supreme Court resolution. The Court is obviously limited to interpreting the same ambiguous language in the statute with which lower courts have been wrestling for the last several years. Any decision leaning towards either a broad or narrow interpretation may still not provide the necessary clarity in this area given the language constraints.

Second Avenue: Legislative Amendment Resolution

The most prudent course of action is for Congress to enact legislative amendments to clarify its intent with

[21] *United States v. Rodriguez*, 628 F.3d 1258, 1260 (11th Cir. 2010).
[22] *Id*. at 1263.
[23] *Id*. at 1263.
[24] 676 F.3d 854, 863 (9th Cir. 2012) (en banc).
[25] *Id.* at 856.
[26] *Id.* at 856, 863-64.
[27] *Id.* at 863-864.
[28] *Brekka*, 581 F.3d at 1134-35.
[29] *Id.* at 1129-30. He also conducted some post-employment activities not addressed here.
[30] *Id.* at 1133.
[31] *Id.* at 1135.
[32] *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 202 (4th Cir. 2012).
[33] *Id.* at 203.
[34] Sup. Ct. R. 10(a).
[35] *WEC Carolina Energy Solutions LLC v. Miller*, 133 S.Ct. 831 (2013) (No. 12-518).
[36] Motion for Issuance of the Mandate, *United States v. Nosal*, No. 10-10038 (9th Cir. Aug. 2, 2012) (ECF No. 83).

respect to Section 1030. The vigorous public debate around these issues signals the value of a negotiated (legislative) solution to the matter. To advance debate on this avenue, four alternatives are highlighted among others that may be considered.

(1) Redefine the Definition of ''Exceeds Authorized Access.'' Based on the cases, part of the dispute has arisen over the definition of ''exceeds authorized access'' under Section 1030(e)(6). For example, some of the cases have attempted to construe the meaning of the terms ''entitle'' and ''so'' that are used in the definition.[37]

Congress can redefine ''exceeds authorized access'' to provide better guidance on the intended application of the statute. For example, Congress can clarify that ''exceeds authorized access'' applies to situations where permission to access information is later abused such as by the theft of information.

(2) Remove the ''Exceeds Authorized Access'' Standard and Substitute New Language. Another option is to remove the ''exceeds authorized access'' language and substitute language that disallows theft of information for which access was previously given.

As background, the original 1984 version of the CFAA included the following language: ''having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.''[38] Ironically, the legislative reports for the 1986 amendment noted that the ''exceeds authorized access'' language was substituted to clarify the 1984 language.[39]

(3) Distinguish ''Access'' from ''Use'' or ''Purpose.'' Another option would be to distinguish between ''access'' and ''use'' or ''purpose'' to misuse the information. As some courts have suggested, this would cover the situation in which access was originally provided but later abused. For example, the Seventh Circuit concluded that once the employee acted contrary to the interests of his employer, liability attached.[40] Similarly, the Fifth and Eleventh Circuits have focused on the obtaining of the information for a non-business purpose,[41] or unauthorized purpose.[42]

(4) Misappropriation of Information Option. Another related option would be to adopt a misappropriation standard which would not turn on whether access was authorized to the information. Instead, the focus would be on whether the information was misappropriated.

White House Proposal

On January 13, 2015, President Barack Obama proposed a new cybersecurity legislative package including amendments to the CFAA.[43] The amendments are intended in part to ensure that ''insignificant conduct does not fall within the scope of the statute, while making clear that it can be used to prosecute insiders who abuse their ability to access information to use it for their own purposes.''[44]

The White House proposal would amend CFAA Section 1030(a)(2) to modify the ''exceeds authorized access'' language and replace it with a new provision, criminalizing or creating civil liability where a person:

> (B) intentionally exceeds authorized access to a protected computer, and thereby obtains information from such computer, and
>
> (i) the value of the information obtained exceeds $5,000;
>
> (ii) the offense was committed in furtherance of any felony violation of the laws of the United States or of any State, unless such violation would be based solely on obtaining the information without authorization or in excess of authorization; or
>
> (iii) the protected computer is owned or operated by or on behalf of a governmental entity.[45]

This amendment would have the effect of avoiding criminal or civil liability for minor offenses that some courts, such as the Ninth Circuit, have feared the current statutory provisions unduly criminalize. However, the proposal still uses the phrase ''exceeds authorized access.'' The proposal redefines these terms:

> to access a computer with authorization and to use such access to obtain or alter information in such computer—
>
> (A) that the accesser is not entitled to obtain or alter; or
>
> (B) for a purpose that the accesser knows is not authorized by the computer owner.[46]

Subsection (B) appears to encompass those situations where an employee has signed a confidentiality agreement prohibiting the use of information to which the employee has access. This would arguably also apply where the employee had been notified of any policy prohibiting the access of or utilization of company computers for non-work reasons.

Under this approach, with effective company policies in place (permitting access only for specific work functions and prohibiting access for any personal use, etc.), the *Nosal* and *WEC* decisions discussed above could have come out differently. The companies could have argued that relevant company policies put the employee on notice that the extraction of proprietary company data was done ''for a purpose that the accesser [knew was] not authorized.''

---

[37] *See, e.g.*, *Nosal*, 676 F.3d at 857-58 (focusing on the meaning of ''entitled'' and ''so'' as used in Section 1030(e)(6)).

[38] Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92.

[39] H. Rep. No. 99-612, 99th Cong., 2d Sess. 11 (1986) (''The purpose of this change is merely to clarify the language in existing law.''); *see also* S. Rep. No. 432, 99th Cong., 2d Sess. 9 (1986) (''The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in . . . the bill.'').

[40] 440 F.3d at 420-21.

[41] *Rodriguez*, 628 F.3d at 1263 (''Rodriguez exceeded his authorized access and violated the Act when he obtained personal information for a nonbusiness reason.'').

[42] *John*, 597 F.3d at 272 (''Access to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded.'').

[43] Updated Administration Proposal: Law Enforcement Provisions, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.

[44] The White House, Office of the Press Secretary, ''Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts,'' (January 13, 2015), *available at* http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat.s

[45] 18 U.S.C. § 1030 (a)(2)(B) (as proposed).

[46] 18 U.S.C. § 1030 (e)(6)(A)-(B) (as proposed).

  PTCJ ISSN 0148-7965

This formulation does put the onus of adequate notice on companies. Though a bevy of lawsuits challenging whether the ''accesser knows'' certain uses are not authorized are likely to arise, where adequate human resourcing practices are implemented—including requiring employees to *acknowledge* review and receipt of policies in writing—companies would appear to be on strong grounds for establishing such knowledge. The formulation may be burdensome to smaller enterprises without the resources to draft and implement tailored policies, but in such cases boilerplate policies would likely be adequate to cover the most significant risks regarding trade secret theft by insiders.

Initial Reactions to the White House Proposal. Some have already criticized the White House proposal. For example, one commentator contends the new definition of ''exceeds authorized access'' introduces an awkward and redundant mental state.[47] Among other issues, there are questions on whether the formulation is not clear in how it applies to varying types of written restrictions.[48]

Another key concern is whether the amendments may chill the contributions of white hat hackers and security researchers. As written, the statute prohibits intentionally exceeding authorized access and obtaining information given certain conditions. The expanded definition of authorized access includes for a purpose ''the accesser knows is not authorized.'' But this may interrupt the market for security research that has emerged. As some have asked, ''[d]isclosure policies and bug bounties provide a form of safe harbor for researchers.''[49] However, this safe harbor could be disrupted should the statute be construed against such white hat activities.

The amendments expand the scope of prohibited activities in such a way that would arguably encompass security researchers, dissuading their activities and discouraging a robust market for healthy vulnerability identification. In addition, though presumably an employee or contractor hired for the specific purpose of penetration and vulnerability testing would have authorized access, the entire point of such efforts is to venture into areas a company does not want parties to go, and a range of disputes could occur as to what constitutes proper authorization, whether certain assets are so cherished as to never be intended for exposure, and so on.

Others have criticized the proposal for marking the violation of a written restriction on computer use a crime.[50] A related issue concerns the elevation of prior misdemeanors to felonies under the revisions.[51]

While the White House proposal does address a range of considerations upon which commentators have been focusing for some time, therefore, it seems prudent for Congress to take a broader view on the potential amendments that may rectify the CFAA's current weaknesses.

Conclusion

Companies need to allow access to trade secrets and confidential information to trusted insiders. When this trusted access is abused, federal law should be able to redress the misappropriation. Statutory amendment presents the most promising prospect for an effective and complete resolution to the problem.

Congress should resolve the confusion and disparate application of the law under the CFAA. A remedy should not turn on where the theft occurs. The law must be clearly and evenly applied. To advance the debate on this important issue, this article has reviewed a number of options that may be considered. Because of the pervasive risk that the theft of trade secrets and confidential business information will go unpunished, prompt resolution is necessary. Federal law should foster American innovation and ingenuity, not hamper its development, and thoughtful amendments to the CFAA can do just that.

---

[47] Orin Kerr, ''Obama's proposed changes to the computer hacking statute: A deep dive,'' *The Washington Post– The Volokh-Conspiracy* (January 14, 2015), *available at*: http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/.

[48] *Id.*

[49] Ericka Chickowski, ''President's Plan to Crack Down on Hacking Could Hurt Good Hackers,'' *Dark Reading* (Jan. 21, 2015), *available at*: http://www.darkreading.com/risk/presidents-plan-to-crack-down-on-hacking-could-hurt-good-hackers/d/d-id/1318721.

[50] Peter Toren, ''The Administration's Misguided Proposal to Amend the CFAA,'' *Law360* (Jan. 16, 2015), *available at*: http://www.law360.com/articles/612467/the-administration-s-misguided-proposal-to-amend-the-cfaa.

[51] *Id.*