12-1-2010

Civil Liability under the Computer Fraud and Abuse Act (CFAA)

Warren Thomas
Georgia State University College of Law

Georgia State University | COLLEGE OF LAW

Research Guides

Civil Liability under the Computer Fraud and Abuse Act (CFAA)

Guide Information

Last Updated:	Aug 16, 2011
Guide URL:	http://libguides.law.gsu.edu/content.php?pid=164361
Description:	A bibliography created for Nancy Johnson's Advanced Legal Research Class.
Tags:	cfaa, computer fraud, labor_and_employment_law
RSS:	Subscribe to Updates via RSS

Guide Index

Home

Overview

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, is the primary weapon in the federal prosecutors' toolbox to combat computer-based crimes. Since its enactment in its original form in 1984, many computer "hackers" have been prosecuted and punished under the statute. As the nature and extent of nefarious activities and by computers increased, Congress expanded the coverage of conduct under the CFAA.

Particularly relevant to this bibliography, in 1994 Congress added a civil cause of action for any person who suffered damage or loss because of a violation of the act. In recent years, employers have increasingly used the CFAA to sue ex-employees who take company data with them when they leave.

Many of the CFAA offenses require a prosecutor or plaintiff to show that a defendant “accesses a protected computer without authorization, or exceeds authorized access” to create liability for such conduct. Congress defined *exceeds authorized access* as follows: “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.” However, definitions of *access* and *authorization* are notably absent. A split of authority has developed regarding the property interpretation of these terms and the proper scope of the CFAA to cover employee abuse of access to company data. Accordingly, until the split is resolved by Congress or the Supreme Court, both plaintiffs and defendants in an action involving § 1030 must understand the local circuit's interpretation and/or the reasoning of the various decisions if there is none to successfully litigate their case.

Disclaimer

This research guide is a starting point for a law student or an attorney to research the Computer Fraud and Abuse Act, courts' interpretation of it, and its application in civil cases. This is a very active area of federal law, and it is imperative to Shepardize or KeyCite all cases and statutes before relying on them. This guide should not be considered as legal advice or as a legal opinion on any specific facts or circumstances. If you need further assistance in researching this topic or have specific legal questions, please contact a reference librarian in the Georgia State University College of Law library or consult an attorney.

Scope

This guide provides an overview of the Computer Fraud and Abuse Act and its various interpretations, particularly in the "unauthorized access" cases in the civil context. The resources provided in this guide include helpful laws, secondary materials, and Internet resources on the CFAA. However, to provide context to this specific terms of the statute, some of the materials relate to the broad subject of general statutory interpretation. This research guide is intended to assist attorneys with little or no familiarity with this subject matter in gaining a better understanding of the relevant law. At the end of the guide you will find Internet resources that may be used to locate many of the sources contained in the guide.

About the Author

Warren Thomas will graduate from the Georgia State University College of Law in May, 2011. While in law school, Mr. Thomas served as an associate editor for the Georgia State University Law Review and was a finalist in the 2010 Georgia Intrastate Moot Court Competition. He will compete in the Giles Sutherland Rich Memorial Moot Court Competition in the spring of 2011. Before attending law school, Mr. Thomas graduated from the University of Georgia with a Bachelor of Science in Mathematics and Computer Science. After

graduation, he will serve as a law clerk for the Honorable Judge Charles A. Pannell, Jr. in the Northern District of Georgia for two years. For more information, please contact Professor Nancy Johnson via e-mail at njohnson@gsu.edu.

Back to Top

Primary Sources

U.S. Code

The Computer Fraud and Abuse Act is contained, in its entirety, in one section of the United Stated Code. The United States Code can be found, free of charge, online from the Cornell Legal Information Institute.

18 U.S.C. § 1030

Relevant subsections for this research guide:

- Subsection (a) sets out the conduct and activities that lead to a criminal or civil violation of the statute. In general terms, include:
    1. Obtaining national security information
    2. Compromising the confidentiality of a computer
    3. Trespassing in a government computer
    4. Accessing a computer to defraud and obtain value
    5. Causing damage to a protected computer
    6. Trafficking in passwords
    7. Extortion involving threats to damage a protected computer
- Subsection (e) contains definitions specific to the CFAA and its terms. Some of the most frequently litigated include
    1. (e)(6) *exceeds authorized access* = "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"
    2. (e)(8) *damage* = "any impairment to the integrity or availability of data, a program, a system, or information"
    3. (e)(11) *loss* = "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 interruption of service"
- Section (g) provides the civil cause of action for any person who "damage or loss by reason of a violation of" § 1030, provided that one of the factors listed in subsection (c)(4)(a)(i) is present.

Legislative History

The following sources shed light on Congress's intent in passing the various incarnations of the statute or its most important amendments:

- H.R. Rep. No. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689
    - Congress made clear that the impetus behind initial creation of § 1030 was to target hacking activities. The House Report accompanying the statute stressed both governments' and businesses' growing reliance on computers and the threat that increased networking would make society more vulnerable to hacking incidents.
- Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (1986) and accompanying S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479
    - The 1986 amendment inserted the phrase *exceeds authorized access* in place of "or having accessed a computer with authorization, uses the opportunity . . . for purposes to which such authorization does not extend." This change is often cited by courts supporting the narrow interpretation. The Senate Report accompanying the 1986 amendments stated that the purpose of the change was to "remov[e] from the sweep of the statute one of the murkier grounds of liability" where conduct could be criminal at one time and not criminal at another.
- Computer Abuse Amendments Act of 1994, Pub. L. No. 103 322, tit. XXIX, § 290001, 108 Stat. 2097
    - This was the act where the civil action for violation of the CFAA was created.
- S. Rep. No. 104-357 (1996), *available at* 1996 WL 492169 (Leg. Hist.)
    - In the Senate Report accompanying the 1996 Amendments, the Senate stated that "The crux of the offense under subsection 1030(a)(2)(C) [intentional access to a computer

without, or in excess of, authorization to obtain government information and, where appropriate, information held on private computers] is the *abuse* of a computer to obtain the information." (emphasis added). Further, the report highlighted that improper *use* of a computer and "abuse [of] authority" would subject the defendant to (misdemeanor) liability. Thus, courts adopting the broad agency view of *without authorization* often cite this legislative history as persuasive of Congress's intent to cover improper use as well as access.

- Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110 326, tit. II, § 204, 122 Stat. 3560, 3561–63
  - This amendment re-organized several of the subsections of the CFAA. Lawyers must be careful when reading cases applying the CFAA from before enactment of this amendment to ensure they understand which sections or violations the courts are referring to.

Case Law

The following are notable cases in the history and development in the split of authority over the meaning of *without authorization* in the CFAA.

Circuit Courts of Appeals

United States v. Nosal, — F.3d —, 2011 WL 1585600, 2011 U.S. App. LEXIS 8660 (9th Cir. Apr. 28, 2011).

The Ninth Circuit "clarif[ied]" an earlier panel's holding in *Brekka* (see below) by holding that "under the CFAA, an employee accesses a computer in excess of his or her authorization when that access violates the employer's access restrictions, which may include restrictions on the employee's use of the computer or of the information contained in that computer." Thus, the court reversed the district court, which had relied on *Brekka* to dismiss five counts of an indictment. The Ninth Circuit panel distinguished *Brekka* on the basis that there the employer in *Brekka* had no employment agreement or guidelines that would prohibit the defendant's use of data. In contrast, in *Nosal* the employees were "subject to a computer use policy that placed clear and conspicuous restrictions on the employees' access" to the computer systems, and—like in *Rodriguez* and *John*, below—the employee could not therefore claim he did not know his use was unauthorized.

United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010)

TBD

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

The Fifth Circuit was the first Circuit Court of Appeals to cite the *Brekka* decision. In *John*, an account manager at Citigroup used her system access to take customer account data, intending to use the data to incur fraudulent charges on the accounts. The Fifth Circuit distinguished *Brekka* by reasoning that it was neither improper nor unexpected to interpret *exceeds authorized access* to encompass a limit on use, where a criminal defendant *knows* the purpose for the access is both in violation of employer policy and part of an illegal scheme.

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

The Ninth Circuit created a full court of appeals level “split” when it explicitly rejected *Citrin* and similar authority. The court stated that the criminal nature of the CFAA was “most important” to justify its reasoning that the statute should be narrowly interpreted, according to the rule of lenity. Thus, it held that because Brekka had *permission* to use his computer to access company data by his employer, his use was *authorized*, notwithstanding any intent he had to take the data to compete with his firm. The court reasoned that a defendant would have no reason to know a state law breach of duty to loyalty would expose him to criminal liability, that the act therefore could not be interpreted to do so, and that, necessarily, a civil action could not lie either.

International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006)

The Seventh Circuit was the first Circuit Court to address the interpretation of *without authorization* in the CFAA. In *Citrin*, the defendant employee installed a “secure-erasure” program on his company-issued laptop before quitting to form his own, competing business. When he quit, he used the program to erase all of the company’s data off the laptop. The Court held that the plaintiff could held that the plaintiff could state a claim under the “intentionally causes damage without authorization.” Judge Posner, writing for the court, stated that agency law imposed a duty of loyalty on Citrin, and Citrin breached that duty and thus terminated his authorization to access the laptop when he deleted the files. Until recently, Posner’s opinion in *Citrin* was adopted by a large number of district courts whose circuits had not squarely addressed the issue.

P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504 (3d Cir. 2005)

The Third Circuit in 2005 explicitly expanded the scope of violations for which plaintiffs could bring a civil action under the CFAA. The court clarified that the § 1030(g) civil claim was *not* limited to the conduct factors that at the time were listed as subsections “defraud and obtain value” conduct violation. By clarifying that plaintiffs could allege other violations and obtain relief, the Third Circuit added to employers’ opportunities to allege CFAA violations in federal court

EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001)

In this early decision regarding the exceeds authorized access element, the defendant used an automated “scraper” program to scan prices from plaintiff tour company's website. The court avoided interpreting *without authorization* because it affirmed the district court on the basis of the *exceeds authorized access* prong of the CFAA. Here, the court noted that one of the defendants, Gormley, had signed a "broad" confidentiality agreement prohibiting him from revealing or using to benefit any third party any proprietary or confidential information of EF. It therefore held that Gormley likely exceeded whatever level of authorization he may have had to navigate the website by using his know-how to help the other defendants develop the scraper program.

District Courts

1st Cir.

Guest-Tek Interactive Entm't, Inc. v. Pullen, 665 F. Supp. 2d 42 (D. Mass. 2009)

This district court order cites *Brekka* as an example of the trend toward the narrow interpretation of authorization, but interpreted First Circuit Court of Appeals authority as favoring a broad interpretation. Citing *EF Cultural Travel BV v. Explorica*, *supra*, the court stated that the First Circuits prior, "broader reading" of the CFAA "undercut" the defendant's argument for the narrow interpretation of *without authorization* (*Explorica* was not mandatory authority because it interpreted *exceeds authorized access*).

4th Cir.

Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479 (D. Md. 2005)

Wener-Masuda was an officer in a local branch of the IAM union and thus was authorized to access IAM's confidential member list, maintained on IAM's secure, proprietary website. Werner-Masuda signed a "Registration Agreement" where she "agree[d] *not to use the information* provided through [the website] for any purpose that would be contrary" to IAM. At a later point, she did, and IAM sued claiming Wener-Masuda's *authorization* was limited by the Registration Agreement. The district court disagreed and dismissed the claim, stating the CFAA "does not prohibit the unauthorized disclosure or use of information, but rather unauthorized access. Nor do their terms proscribe authorized access for unauthorized or illegitimate purposes."

6th Cir.

ES & H, Inc. v. Allied Safety Consultants, Inc., No. 3:08-CV-323, 2009 WL 2996340 (E.D. Tenn. Sept. 16, 2009)

This case illustrates another troublesome term in the CFAA: the proper pleading and interpretation of "loss". After discussing the thorny issues of the interpretation of *without authorization*, the court held the plaintiff did not plead the type of loss contemplated by the statute. Plaintiff alleged it sustained "damages" as a result of the defendant's misappropriation of information (of course, allegedly obtained *without authorization*); the court noted the inference was that the damages were in the nature of lost profits. But the court held that the term loss as defined in § 1030(e)(11) only includes lost profits if they were incurred due to an "interruption in service."

8th Cir.

Condux Int'l, Inc. v. Haugum, No. 08 4824 ADM/JSM, 2008 WL 5244818 (D. Minn. Dec. 15, 2008) ("[T]he Lockheed line of cases reflects a more correct interpretation.")

Condux is partially valuable as a resource simply because it collects a large number of cases on either side of the *without authorization* debate (including several not included in this guide). Ultimately, the court agreed with the narrow interpretation of the term and dismissed the claims. Agreeing with the analysis in several of the cases it cited, the court stated that the *broad* interpretation cases "incorrectly focuses on what a defendant did with the information after he accessed it (use of information), rather than on the appropriate question of whether he was permitted to access the information in the first place (use of access)." It also found the 1984 and 1986 House and Senate Reports, respectively, supported a narrow reading due to the apparent intent to remove liability from "murkier" kinds of conduct where in some instances a defendant's access would create liability while in others it would not. Thus, to the court, the agency theory and its dependence on the defendant's use of information is incorrect.

NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042 (S.D. Iowa 2009) ("The legislative history of § 1030(e)(6) supports the broad view.")

The court in *NCMIC* adopted the broad, agency interpretation of *without authorization*. First, it noted that courts in various cases had used agency law to give meaning to the the term *authority* in statutes. Next, it broadly quoted Judge Posner in the 7th Circuit *Citrin* case and agreed that the broad view best distinguishes between the two terms *without authorization* and *exceeds authorized access*. In contrast to cases like ES & H, supra, the court stated that "the broad view does not focus on an employee's later misuse of information but rather focuses on an employee's initial *access* of the employer's computer with the intent" to defraud.

9th Cir.

Between 2000 and 2009, the Ninth Circuit developed an *intra*-circuit split over the proper interpretation of the CFAA. Both bookends of this period have been highly influential for decisions following them: *Shurgard Storage Centers* below and *Brekka*, above.

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

This was the first case to interpret *without authorization* to encompass a breach of duty of loyalty. For a number of years, its holding was followed by a majority of other courts in the United States. The court first imported agency principles into the discussion by citing a previous Ninth Circuit decision, *United States v. Galindo*, 871 F.2d 99 (9th Cir. 1989), where a jewlery store employee was held to have lost her authority to act as an agent for the store when she used fraud to carry out her actions. It also cited the Restatement of Agency for the proposition that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." The *Shurgard* court thus held that the plaintiff's former employee lost his authority when he became an agent of the defendant competitor, and therefore he accessed the company data *without authorization*.

Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962 (D. Ariz. 2008)

The court in *Shamrock* rejected *Shurgard* and similar authority by stating the plain meaning of "authorization" is commonly understood as "conferring authority; permission." It argued that *Citrin* and *Shurgard* "conflate[]" the meaning of the separate terms *access without authorization* and *exceeds authorized access* because Congress explicitly contemplated the situation where a person initially accesses a system *with* authority but then later goes beyond it by *exceeding* that authority. The court also examined the legislative history and read it to support the idea that "the CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information." It thus held *access without authorization* occurs only where the initial access was not *permitted*.

10th Cir.

US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189 (D. Kan. 2009)

Here, the court specifically adopted the arguments and analysis of *Shamrock*. Thus, the court dismissed plaintiff's claims premised on access *without authorization* where the defendants had initial permission. However, it allowed the claims for *exceeds authorized access* to survive because the plaintiffs alleged their former employees had "limited access" to some of the confidential information they allegedly accessed & took, including some data which was outside the geographic scope of the the employee's duties. Thus, the court held the explicit limitation was enough to state a claim for exceeding their authority.

11th Cir.

Lockheed Martin Corp. v. Speed, No. 6:05 CV 1580 ORL 31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006)

The Florida court rejected outright *Citrin* and *Shurgard*'s use of "extrinsic materials" like the Restatement of Agency where the plain language of the CFAA is sufficient to interpret the disputed term. Again, the court looked to a dictionary definition of *authorization* to equate the term with *permission*. It also noted that Congress had "targeted actions other than access, such as 'communication' or 'delivery' of confidential information" (actions the court apparently felt were closer to the improper "use" other courts held actionable) elsewhere in the statute. The court then provided a lengthy analysis of its disagreement with *Citrin* and *Shurgard*, an analysis which has been cited by many other courts despite the case's unreported status.

Back to Top

Secondary Sources

Law Journal Articles

Below are notable law review and other periodic sources that contain relevant information to shed light on this topic. Those sources are organized by author and can be found on LexisNexis, Westlaw, or HeinOnline for a fee.

Nick Akerman, ***When Workers Steal Data to Use at New Jobs: Despite Some Negative Case Law, The Computer Fraud and Abuse Act is an Effective Tool for Employers***, Nat'l L. J., July 6, 2009, at 18

This pre-*Brekka* article outlines some of the contours of the caselaw interpreting *without authorization* in the CFAA. Akerman argues that the district court opinions adopting the narrow interpretation are incorrect and should not withstand appellate review because many of them cite a M.D. Fla. case (*Lockheed*) that, according to him, was "effectively overruled" in a subsequent 11th Circuit case, *United States v. Salum*, 257 Fed. Appx. 225 (11th Cir. 2007). [Guide author's Note: According to a KeyCite search, as of Nov. 2010 no federal court decision has cited *Salum*.] Akerman also points to the Supreme Court's use of Restatement of Agency to affirm a conviction under the mail and wire fraud statute to argue that agency principles should be equally applicable to limit the scope of an employee's authority to access his computer.

Patricia L. Bellia, ***Defending Cyberproperty***, 79 N.Y.U. L. Rev. 2164 (2004)

This article discusses the application of traditional property-law doctrines (e.g., trespass) to computer and network resources. Although the weight of scholarship and court authority has thus far rejected application of these traditional rules in such a different medium, Professor Bellia argues that in some circumstances property-rule protection *is* appropriate. Bellia analyzes the evolution of computer trespass laws, using the CFAA as an example of one of those, and discusses the policy considerations that these laws express. Ultimately (at least with regard to the CFAA), she argues that the unauthorized access in the CFAA should be limited to *technical* breaches of access, thus excluding use-based theories (e.g., *Shurgard* & *Citrin*).

Victoria A. Cundiff, ***Reasonable Measures to Protect Trade Secrets in a Digital Environment***, 49 IDEA 359 (2009)

A central tenant of this article is that "[t]he digital world is no friend to trade secrets." The article explores the difficulty trade secret owners have in protecting their "secrets" in an increasingly digitized society where walking away with a company's data can be as easy as downloading onto a USB drive or iPod (R). Then, the article provides practical advice to trade secret owners on their options and what exactly constitutes the "reasonable" measures they must take to keep their trade secret status under trade secret laws. Ms. Cundiff explains how the CFAA is one tool (albeit an imperfect one) an owner can use to punish misappropriation of trade secrets. Specifically, Section I.D.3 discusses the circuit split in the case of former employees taking data; section D.4 provides advice on how companies can draft contracts with their employees in order to increase likelihood that a subsequent theft of data would be held to be *unauthorized access* or *exceeding authorized access* under the statute; and section D.5 summarizes other pleading and jurisdictional issues to consider.

Orin S. Kerr, ***Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes***, 78 N.Y.U. L. Rev. 1596 (2003)

In this seminal article (cited by many of the courts adopting the narrow interpretation of *unauthorized access*), Professor Kerr argues for a constrained interpretation of authorization in the context of computer crime laws. He first reviews the history of unauthorized access statutes (their origin being attempts to apply burglary, trespass, and theft to computers), and then discusses his view that broad interpretations of these statutes in civil cases (where courts may be more likely to want to punish "bad" behavior) may unintentionally create *criminal* liability for a broad swath of society. He proposes that courts reject agency and contract interpretations of *authorization* and, like Bellia above, limit the application of the CFAA to breaking technical measures of protection.

Stacy Nowicki, Ph.D., ***No Free Lunch (or Wi-fi): Michigan's Unconstitutional Computer Crime Statute***, 13 UCLA J.L. & Tech. 1, 33–41 (2009), http://www.lawtechjournal.com/articles/2009/01_091026_nowicki.pdf.

This article argues that Michigan's computer crime statute is unconstitutional under the void for vagueness doctrine (a suggestion Kerr made in his article as well). In the proposal

section of the article, Dr. Nowicki provides a draft definition of "authorization" (as the MI statute refers to it) that would potentially make disloyal employee conduct unauthorized. She would include limitations on use as part of the definition and include a "reasonable person" standard ("An actor has authorization if a reasonable person would believe that the act was authorized.").

Katherine Mesenbring Field, Note, ***Agency, Code, or Contract: Determining Employers' Authorization Under the Computer Fraud and Abuse Act***, 107 Mich. L. Rev. 819 (2009)

This student note explains the three theories of limiting authorization under the CFAA, with particular attention and citations to the legislative histories of the statute. Ms. Field concludes that code-based authorization provides an ideal "default" rule with contract-based limitations on authorization being permissible when the contract clearly and specifically applies to the employee's conduct.

Graham M. Liccardi, Note, ***The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court***, 8 J. Marshall Rev. Intell. Prop. L. 155 (2008)

This student primarily discussed the CFAA as an alternative to state-law trade secret actions. Liccardi argues that existing trade secret law does not adequately protect businesses' needs in increasingly complex technical and business situations—there are too many "hurdles" to overcome. But the CFAA, at least under the broad interpretation of *unauthorized access*, provides a means for businesses to protect *all* valuable computer data, it allows access to federal courts without the need to show diversity jurisdiction, and he argues that the CFAA should (at least until Congress acts) in effect serve as a federal trade secret statute.

Linda K. Stevens & Jesi J. Carlson, ***The CFAA: New Remedies for Employee Computer Abuse***, 96 Ill. B.J. 144 (2008)

This articles reviews several of the frequently cited cases in the *without authorization* debate. In particular, highlights a case that distinguished itself from the *Lockheed* line of cases because the defendants had signed an agreement to refrain from "sending or accessing messages on HP's computer systems for personal gain." Like Ms. Field, above, the authors suggest that this method of drafting employment contracts presents a way of avoiding the harsh-to-employers, narrow interpretation.

Warren Thomas, Note, ***Lenity On Me:*** LVRC Holdings LLC v. Brekka ***Points The Way Toward Defining Authorization And Solving The Split Over The Computer Fraud And Abuse Act***, 27 Ga. St. U. L. Rev. 379 (2011)

This Note—also by the author of this research guide—analyzes the the development of the split in authority over the meaning of *unauthorized access* through the 2009 *Brekka* case. The Note proposes that the rule of lenity should inform courts' interpretation of the CFAA, even in civil contexts. However, in cases decided since the Note's publication, a trend has developed where courts have held the fair notice is provided to defendants where their conduct is expressly prohibited by employee policies or criminal conduct. This Note remains useful for a background on the circuit split and how the rule of lenity informs these courts' analyses.

Richard Warner, ***The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act***, 12 Emp. Rts. & Emp. Pol'y J. 11 (2008)

Warner's article explains how the CFAA is another "arrow in the quiver" of employers to use against employees taking the business's trade secrets. He explains the expansion of interpretations of both *without authorization* and *damage* under the statute. Warner argues that while the decision in *Shurgard*'s was ultimately correct, the agency analysis is "problematic" because their interpretation would necessarily mean that *all* authorization by the employee was terminated after a breach of loyalty. Where, according to him, authorization should depends on the purpose of the access. He argues that the agency argument eviscerates the distinction between *without authorization* and *exceeds authorized access* in the statute, and he believes the statute should be changed to reflect this result. Warner concludes his article with a discussion of state laws requiring disclosure of unauthorized access to certain computer resources, and these statutes present another important (and potentially expensive) consideration for businesses when analyzing liability issues for a data breach.

Peter A. Winn, ***The Guilty Eye: Unauthorized Access, Trespass and Privacy***, 62 Bus. Law. 1395 (2006–2007)

Winn takes a position in this article almost opposite of Kerr's article: He argues that computer trespass can and should still be based on the common law action. He proposes a test for computer trespass cases so that (1) the access must take place without the (subjective) permission of the rights-holder, and (2) the access objected to must be of a kind that a reasonable person (objectively) would expect to be unauthorized. This "reasonable person" test would allow courts to "balance" the interests in public access to the information with the employer's right to restrict it, and courts can decide cases based on the facts before them without the rigidity that either the broad or narrow interpretations of the CFAA would require.

OTHER SOURCES

Amy E. Bivins, ***Employers Should Revisit Data Misuse Policy In Light of Ninth Circuit*** Brekka ***CFAA Ruling***, 8 Priv. & Sec. L. Rep. (BNA) 1441 (Oct. 5, 2009)

Reviews the Brekka decision, including commentary from practitioners (particularly from the Ninth Circuit), and argues that there is a trend of courts almost uniformly becoming less receptive to the CFAA as a cause of action in trade secret cases.

Books & Treatises

Books and Treatises Discussing the Computer Fraud and Abuse Act

Robert D. Brownstone, ***Privacy Litigation***, ***in*** Kevin P. Cronin and Ronald N. Weikers, Data Security & Privacy Law: Combating Cyberthreats §§ 9.3–16 (West Supp. 2010)

This treatise generally covers various sources of liability for breaches of privacy or information theft. The sections above discuss the Computer Fraud and Abuse Act in detail from a litigation perspective, including prohibited conduct, proper parties to a claim, statute of limitations, proper court, remedies, and a specific section (§ 9:13.50) on the split in authority over whether disloyal employees' access is authorized.

Deborah F. Buckman, ***Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)***, 174 A.L.R. Fed. 101 (2001 & Supp. 2009)

This legal encyclopedia article provides a general overview of the CFAA.

A. Hugh Scott & Kathleen Burdette Shields, Computer and Intellectual Property Crime: Federal and State Law (Cumulative Supp. 2006) (Call Number: KF9350.S29 2001)

This encyclopedic volume provides in-depth descriptions of federal and every state's computer crimes laws. Chapter 4 addresses the CFAA, including its legislative history, elements (and their interpretation) of the various offenses, jury instructions, and civil remedies.

Books Discussing General Statutory Interpretation

The following resources provide an overview of the various interpretive methods courts use to interpret the statutes, including the CFAA. Many of the arguments and analyses cited in the decisions interpreting the CFAA rely on techniques described in these sources.

Reed Dickerson, The Interpretation and Application of Statutes (1975) (Call Number: KF425.D5)

Professor Dickerson's scholarly treatise on statutory interpretation is a comprehensive work that presents a coherent theory of interpretation.

Linda D. Jellum & David Charles Hricik, Modern Statutory Interpretation: Problems, Theory, and Lawyering Strategies (1st ed. 2006) (Call Number: KF425.J45 2006)

This is a casebook suitable to a course in drafting or statutory interpretation. Like many casebooks, it teaches the process of interpretation through excerpts of cases where courts wrestled with the boundaries of the core concepts. Likewise, it contains many thought-provoking "problems" with answers. One unique aspect of this reference is an appendix comparing canons of statutory interpretation and demonstrating each canon's "opposite" which can be used to rebut or counter an argument for its use.

William D. Popkin, A Dictionary of Statutory Interpretation (2007) (Call Number: KF425.P669 2006)

This is similar to a "pocket" reference with brief but useful definitions and discussions of interpretive methods and terms. This is a wonderful resource when one wants to understand the basics or needs a concise definition or explanation.

Back to Top

Law Review Articles and other Periodicals

Back to Top

Books and Treatises

Back to Top

Internet & Associations

Interest Groups

Electronic Frontier Foundation (EFF)

The EFF is a policy and legal advocacy organization focused on free speech, privacy, innovation, and consumer rights issues. With respect to the CFAA, the EFF advocates for a narrow reading of the statute, particularly in the cases where plaintiffs (private or government) claim access without authorization based on violation of website terms of service. According to one post on their Deeplinks Blog, "criminalizing terms of service violations has severe ramifications for free speech, innovation, and other digital freedoms." The EFF has filed amicus briefs in several of these CFAA cases, arguing for a narrower interpretation of the act.

The EFF also hosts and Internet Law Treatise wiki with a page devoted to the CFAA. This page contains a description of the statute and lists several criminal and civil cases interpreting the CFAA.

Blogs

Below are a number of legal blogs that have regularly included content addressing liability under the CFAA. These are blogs which generally deal with technology-related legal topics, with the CFAA being a particularly relevant area of privacy and data theft law in this area.

Nick Akerman, Computer Fraud/Data Protection

Attorney Nick Akerman maintains an active practice litigating and advocating for changes to fraud and data privacy law. His blog contains many cases dealing with the CFAA, and one of his articles is cited in the Law Review section of this research guide.

Susan Brenner, CYB3RCRIM3

Professor Brenner's blog is primarily focused on criminal aspects of technology law, including CFAA cases (both civil and criminal). In a post entitled *"Access,"* professor Brenner described some interpretations of the *access* term of the statute, particularly the "usually cited" case of *State v. Allen*, 917 P.2d 848, 852–53 (Kan. 1996) (construing Kansas statute's definition of *access* narrowly).

Evan Brown, Internet Cases

Attorney Evan Brown is an intellectual property and technology law attorney practicing in Chicago, IL. His blog is a good resource for general technology and Internet law updates, and includes several posts relating to CFAA cases (the link above goes to posts with "computer crime" tag).

Orin Kerr, The Volokh Conspiracy

Professer Kerr is a regular contributor to the Volokh Conspiracy, and he has posted several times regarding his pro bono defense of Lori Drew in the first criminal prosecution under the CFAA where violation of a website's terms of service was the predicate *access without authorization*. See http://volokh.com/2009/09/25/government-files-notice-of-appeal-in-lori-drew-case for a representative post.

Proskauer Rose LLP, New Media & Technology Law Blog

Proskauer's blog contains several posts tagged as relating to the CFAA. The blog generally contains updates on recent cases relevant to the firm's technology and media clients (or potential clients). New content is posted approximately once per month. The blog had posts on the *Brekka* and *United States v. Nosal* decisions in the Ninth Circuit dealing with the *without authorization* term of the CFAA.

Back to Top