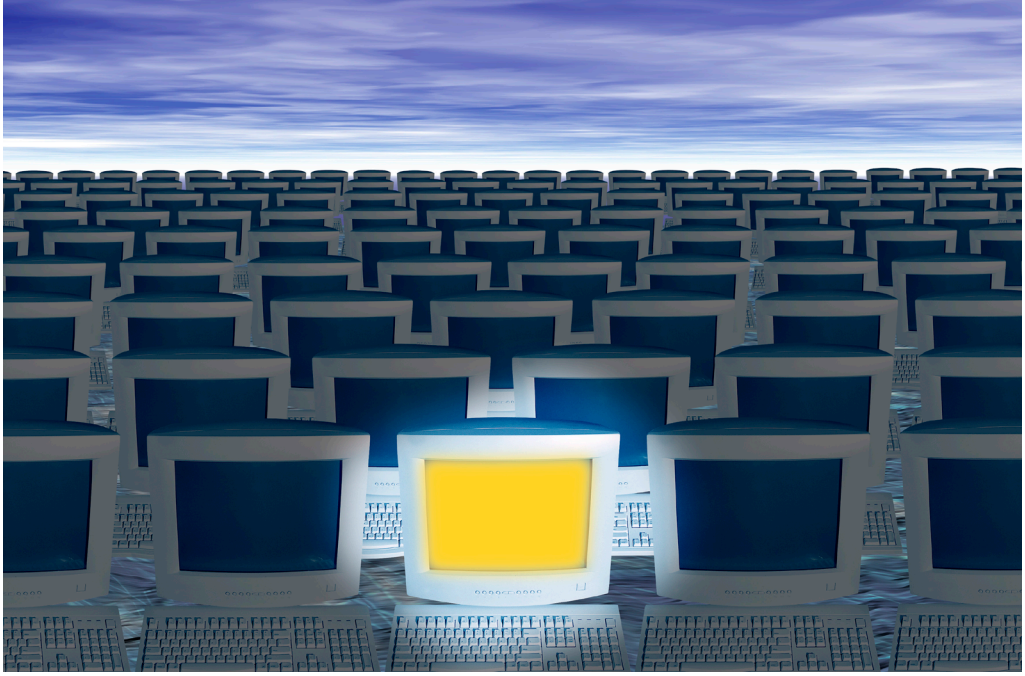

Which Rule of Statutory Interpretation Applies to the Computer Fraud and Abuse Act?

Ambrose V. McCall

Several critical provisions of the Computer Fraud and Abuse Act (CFAA) bar unauthorized access to computers and exceeding authorized access of computers. The Seventh Circuit contends that agency law provides authority as to whether or not access is authorized. The Ninth Circuit disagrees and applies a plain reading of the statute. Which method of statutory analysis is a routing loop for practitioners? [1]

Overview of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act is a statutory provision Congress inserted into the Comprehensive Crime Control Act of 1984.[2] The civil remedy provision in the CFAA permits any person who has sustained recoverable damage or a loss by reason of a violation of the CFAA to obtain compensatory damages and injunctive or other equitable relief.[3] Employers or businesses covered by the CFAA often allege violations based on a person intentionally accessing a computer without authorization, or exceeding authorized access, and obtaining information from a protected computer with the intent to defraud and, by means of such conduct, further an intended fraud and obtain anything of value as defined by the CFAA.[4] Unlike the Electronic Communications Privacy Act, 18 U.S.C. § 2510, which is a potential arrow in an employee's quiver, the 1994 amendments to the CFAA created a civil remedy, where applicable, for employers or businesses to use against unscrupulous agents, consultants, employees, or officers.[5] Within a civil law context, the CFAA can apply to departing personnel who improperly obtain and use employers' computerized data. A primary issue that counsel must first address when evaluating whether the CFAA applies is whether or not the typically departing or terminated agent, consultant, employee, or officer had authorized access to the employer's CFAA-covered computer software or data. Another of many related issues is whether or not the individual leaving the business exercised any unauthorized use of the employer's computer software or CFAA-covered data for any destructive purpose.

The appellate courts have not sung in unison or harmony when deciding what constitutes unauthorized access of computers or even which test to apply under the CFAA. For example, the Seventh Circuit strongly contends that common law agency principles apply when determining whether a person is authorized to access a protected computer.[6] In contrast, the Ninth Circuit dismisses the use of common law agency principles and relies on a plain reading of the CFAA. In doing so, the Ninth Circuit calls for a factual analysis that evaluates whether or not the employer specifically or objectively expressed an intent to allow or bar a departing employee to access its computers.[7] Outside of these two circuits, the current tally indicates that the First Circuit may interpret the CFAA in a way that is parallel to the Seventh Circuit's interpretation by citing state law duties when distinguishing authorized access from unauthorized access under the CFAA.[8] The Second and Fifth Circuits appear to adopt a "third way" that seeks to abide by the legislative history, statutory provisions, and intent of the CFAA, while also examining the relations between the owner and user of the computer data at issue.[9] The Second and Fifth Circuits employ what they describe as the "intended use" analysis.[10] Until resolved by Congress or the Supreme Court, counsel must determine which interpretation applies in the jurisdiction in which they practice while keeping in mind that the plain meaning and intended use analyses voiced by the Second, Fifth and Ninth Circuits may prevail—and not just because of the Constitution's Supremacy Clause.[11] If common law principles apply, the interstate nature of the activities covered by the CFAA would arguably support the application of federal common law over sifting through state law issued from 50 state capitals. The doctrine creating federal common law, however, might acknowledge that the CFAA and its legislative history undermine any such argument.

The Seventh Circuit's *Citrin* Opinion

In *International Airport Centers LLC v. Citrin,* the Seventh Circuit held that a plaintiff sufficiently pled a cause of action under the Computer Fraud and Abuse Act by, in part, finding that an employee lost the authority to

access a laptop computer provided to him by his employer upon allegedly breaching his duty of loyalty owed to the employer.[12] The CFAA[13] contains a provision that imposes liability on a person who "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct intentionally causes damage without authorization, to a protected computer," which also includes the laptop computer use by the defendant.[14] The alleged facts in *Citrin* are unique to the extent that the departing employee did not simply download, remove, or transfer data from a computer provided by his employer to the employee's own computer, hard drive, SD memory card, SIM card, or USB flash drive. Upon deciding to become self-employed, the defendant allegedly decided to use a secure-erasure software program. This program not only removed files but also wrote over them so as to bar later efforts to uncover the deleted files. Presumably, the deleted files would have contained any data that the former employee had assembled, including data showing his activities before he chose to quit his job.[15]

Whether the defendant installed the secure-erasure program by inserting a floppy disk, CD-ROM, or hard drive, or by downloading the offensive program from the Internet, the *Citrin* court found that the mode of transmission was irrelevant. All such methods of transferring the secure-erasure program data satisfied the statutory definition of "transmission."[16] As a result, the *Citrin* court did not provide an analysis of how certain other provisions of the CFAA would apply that do not require a transmission but compel a CFAA plaintiff to prove that an adverse party intentionally accessed a protected computer without authority, and as a consequence, recklessly caused damage or, without recklessness, caused damage as well as loss.[17] The CFAA categorizes damage to include not only impairment to the availability or integrity of programs or systems but also data and information.[18] In contrast to the broadly drafted term "damage," the term used in the CFAA—"loss"—requires the plaintiff to show what "reasonable" costs were incurred in responding to the complained offense. Such costs must arise from response activities; damage assessments; restoration efforts aimed at retrieving data, programs, systems, or information and returning them to their pre-offense condition; lost revenue; incurred costs; and other consequential damages flowing from the interrupted service.[19] Because the departing employee had destroyed the employer's computer files, the *Citrin* court did not have to decide if the plaintiff pled sufficient facts to satisfy the statutory element of "loss."

What Test Applies to Determine If Computer Users Have Exceeded Their Authorized Access?

The Seventh Circuit Uses Common Law Agency Principles to Determine "Authorization"

The amendments to the CFAA, as enacted in 2001, have not changed the meaning of the statutory phrase, "exceeds authorized access," which the statute defined 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."[20]

A plain reading of the statute seems to support any judicial finding that a person accessing a computer must first have authority to access the "computer," also defined in the CFAA,[21] before using such authorized access to obtain or alter information for which the accesser lacks authority.[22] The CFAA, however, does not specify how a person obtains, maintains, or loses the authority to access a computer. In *Citrin*, the Seventh Circuit described the ex-employee's actions as falling within the statutory descriptive term "exceeds authorized access."[23] In the court's view, the difference between accessing a computer "without authorization" and "exceeding authorized access" was "paper thin."[24]

At the center of its rationale, the Seventh Circuit cited agency law principles when finding that, in terminating his agency relationship with his employer, the employee lost any rights he otherwise would have retained as an agent, including accessing his employer's laptop computer.[25] The *Citrin* court noted that the defendant employee argued that his employment contract authorized him to "return or destroy" the data stored in the laptop computer when he left his employment.[26] However, the court did not read the contractual provision as authorization for the employee to destroy data that he knew his employer had no other copies of or might otherwise have wished to retain.[27] Instead, the Seventh Circuit read the cited contractual language as probably notifying the employee that he was prohibited from distributing confidential data upon leaving his employment.[28]

The Ninth Circuit Employs the Plain Meaning Rule to Decide if "Authorization" Exists

In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the Ninth Circuit formulated its own interpretation of the same statutory phrase in the CFAA regarding whether persons have exceeded their authorized access to an employer's computer. In light of the absence of a statutory definition of the term "without authorization" in the CFAA, the *LVRC* court cited the plain meaning statutory rule of construction, which compels the understanding of words in an act to equate with their ordinary, contemporary, or common meaning.[29] Consequently, because the CFAA lacks a specific definition of the word "authorization," the Ninth Circuit referred to dictionary definitions, not agency law, when concluding that when an employer gives an employee permission to use a computer, that employee is authorized to access the computer.[30] As a result, the employee who had use of the computer provided by the employer in *LVRC* did not act "without authorization."[31]

The Ninth Circuit stressed that a substantial distinction exists between an employee who exceeded his or her otherwise authorized access from an employee who has no authority to access a computer. For example, an individual who received authority to use a computer for specified purposes, but exceeded those limitations, was covered by the CFAA provision describing someone who "exceeds authorized access."[32] In contrast, a person who lacked authorization possessed no rights, with or without

conditions or limitations, to access the computer at issue.[33] Therefore, from the perspective of the *LVRC* court, one must look through the factual prism to determine whether or not the employer communicated or took other action that would exhibit an intent to permit an employee to access a computer or, conversely, to stop or prevent such access. According to the Ninth Circuit, that factual determination will determine whether or not the employee acted with or without the necessary authorization under the CFAA.[34] The *LVRC* court underscored its analysis by noting the different provisions that covered persons who had some authority from those who had none as set forth in §§ 1030(a)(2) and (4) of the CFAA.[35] The cited reasoning leads one to consider the query that, with such different provisions in the CFAA, does the Ninth Circuit construe and apply congressional intent correctly? Or, as the Seventh Circuit indicates, did Congress grant the federal courts freedom to apply common law agency principles?

In *LVRC*, the employee had to access his employer's computer to perform his various marketing and other business functions on behalf of the employer. At the same time, the employee allegedly used his authorized access to e-mail the employer's company documents to users of various personal computers outside the workplace—all in the absence of any written employment agreement or employee policies barring him from e-mailing company documents to users of personal computers not owned or controlled by the employer.[36] The *LVRC* court acknowledged that the Seventh Circuit relied on common law agency principles when holding that the employee's breach of the duty of loyalty to his employer terminated the agency relationship that provided him with the authority to access his employer's computer.[37] Indeed, the Ninth Circuit conceded that, if it applied the logic and rationale of *Citrin*, it would have to find that the employee breached his duty of loyalty to the employer when he allegedly decided to transfer key company documents and information to his personal computer in order to enhance his own competing business, because such actions would terminate his authority to access the employer's computer.[38]

The critical element that compelled the Ninth Circuit to reject the use of common law agency principles is the primary status of the CFAA as a criminal statute. As such, the Ninth Circuit decided that the CFAA should not be interpreted in surprising ways and stressed that any ambiguities must be construed against the government.[39] Consequently, the Ninth Circuit declined to read the CFAA as conditioning "authorized access" of a computer based on common law agency principles.[40] The court reformulated the analysis to the following: if the employer did not terminate the employee's right to use the computer, then the employee would lack any reason to know that personally using the company computer in breach of a fiduciary duty under state law would result in a criminal violation of the CFAA.[41] In this context, the Ninth Circuit encapsulated its analysis as not imposing on the employee an interpretation of a criminal statute "in such an unexpected manner."[42]

The Ninth Circuit also stressed that the interpretation found in the *Citrin* ruling conflicted with the plain meaning of the CFAA's statutory language in a way that rendered the statutory term "without authorization," as used in §§ 130(a)(2) and (4), to mean something other than the fact that a person did not have permission to employ the computer for any purpose, or to mean something different from when an employer has withdrawn or revoked the previously granted permission to access the computer and the employee uses it anyway.[43] Applying this reading, the Ninth Circuit found that the undisputed permission that the employer gave to the employee to access documents or information by computer during the course of his employment undermined any attempt to apply the statutory term "without authorization" as used in the CFAA. The Ninth Circuit affirmed the summary judgment ruling that the employee did not violate § 1030(a) during the course of his employment.[44] The Ninth Circuit's analysis compels considering whether an inherent ambiguity exists in the CFAA because of its use of the term "authorization," to the extent of calling for also applying the rule of lenity to civil actions based on the CFAA.

What Is the Legal Landscape Beyond the Ninth Circuit's Split With the Seventh Circuit?

Other circuit courts have revealed some of their own thinking on the topic of whether common law or statutory interpretation controls the disposition of whether individuals have exceeded their authority in accessing the computers of their employer, a business competitor, or a school or other institution lacking any principal-agent relationship with the person accessing the computer. For example, like the Seventh Circuit, the First Circuit cited Massachusetts law when explaining that, if the allegations were proven, a business competitor who had entered into a confidentiality agreement had probably exceeded its authority to use website tour codes to find a competitor's pricing data.[45] The Fifth Circuit, however, refers to the legislative history of the CFAA and stresses that Congress established two categories of computer users: "insiders," who have the authority to access the computers in question, and "outsiders," who hack into a computer.[46] The Fifth Circuit, therefore, generally concurs with the Ninth Circuit that, where analysis is required as to whether or not access to a computer was authorized, one must refer to the CFAA itself, rather than agency law principles.[47] In the wake of the *Citrin* ruling, Illinois federal district courts have seemed to categorize the issue as one involving whether or not "damage" or "loss" occurred under CFAA in order not to premise decisions on whether a defending party possessed authority to access the computer at issue.[48] Yet, in the majority of potential civil cases under the CFAA—specifically those involving departing employees or corporate officers, or businesses accessing each other's computers or networks under a confidentiality or noncompete agreement— the core question of whether or not such access is authorized remains.

Moreover, given the disparity and variety of various federal or state common law doctrines that have a potential impact on a determination of whether authorized access exists, it seems likely that the Ninth Circuit, along with the

The legislative history of the CFAA reflects an intent to either clarify or narrow its scope since Congress enacted the legislation.

Fifth Circuit, interprets the CFAA in a manner that is most consistent with congressional intent. The legislative history of the CFAA suggests that courts use a nationally consistent tool for measuring whether or not computer access is authorized.[49] Nevertheless, until either Congress or the Supreme Court conclusively resolves the issue of whether common law agency principles or a more strict or narrow interpretation of the CFAA applies to departing personnel, based on a plain reading of the statute or legislative history, practitioners might consider using both agency common law principles and the CFAA's statutory provisions and legislative history when evaluating whether unauthorized access occurred. Still, one might also ponder whether arguing that the application of the rule of lenity could lead to a judicial finding of ambiguity in the CFAA that would support employing the more restrictive interpretation of authorized computer access than would possibly occur when using common law agency principles. This divide in the law creates a challenge for all lawyers dealing with these issues under the CFAA.

Does the CFAA Permit Application of Federal Common Law?

By enacting the CFAA, Congress has spoken to the issue of the commission of fraud and abuse through the use of computers. As noted by some of the courts cited above, Congress has not provided any statutory definitions that specify what it may arguably mean by the use of the terms "without authorization" or "exceeds authorization" in 18 U.S.C. § 1030(a)(2)(C) and § 1030(a)(5)(A). The Supreme Court, however, has stated that, unlike state courts, federal courts do not retain the general power to create, help evolve, and apply their own rules of decision.[50] Moreover, the context for allowing federal courts to apply federal common law requires finding that Congress has not spoken to a specific issue and that a significant conflict also exists between applying state law and a federal interest or policy.[51] Only in such rare, limited, and restricted circumstances are federal courts allowed to develop federal common law.[52] Moreover, when Congress addresses a specific question or issue that previously was determined by federal common law, the need for federal courts to use federal common law evaporates.[53] The limited availability of federal common law pursuant to Supreme Court precedent would suggest that the plain meaning interpretation of the CFAA is arguably the best alternative for a federal district court to adopt.[54] As a result, under the common and ordinary reading of the CFAA, not only would references to technical definitions prove unnecessary, so would references to duties of loyalty or confidentiality under state law or any arguments that a national federal common law standard should apply because of an otherwise claimed statutory gap of the CFAA to define what is "authorized" access to a computer system and what "exceeds authorized" access to a computer system.

What Should District Courts and Private Counsel Do?

How have the district courts responded to the split among the circuits on this issue? One might think that the district courts would readily use the "plain meaning" of words when interpreting the CFAA's use of "with authorization" and "without authorization" and would define the terms in a nontechnical manner consistent with congressional intent. Indeed, the legislative history of the CFAA reflects an intent to either clarify or narrow its scope since Congress enacted the legislation.[55] The split among the circuits, however, appears to have had the opposite effect on the district courts. Rather than wade into the fray to resolve the philosophical and semantic differences in the *Citrin* and *LVRC* interpretations, or citing the combined "plain meaning" and legislative history interpretation of the Second and Fifth Circuits, the district courts have arguably and largely opted for undue caution. Such caution has resulted in interpretations of the CFAA that appear to reflect a judicial effort to narrow the scope of the statute.[56] Indeed, one district court has supported its proposed narrow reading of the term "without authorization" under the CFAA based on a correspondingly narrow reading of the Stored Wire and Electronic Communications Act, 18 U.S.C. § 2701.[57] Other district courts might sidestep the issue by closely evaluating the evidence proffered by the plaintiff seeking injunctive relief under the CFAA.[58] Furthermore, district courts may even avoid such issues at the pleading stage by noting the specificity, or lack thereof, of the allegations related to authorization made against defendants along with the existence of any contractual duties otherwise owed by defendants.[59]

As counsel, however, it is likely that we will continue to address this issue until there is a resolution of the larger issue of what tools to use to measure computer access and determine whether it is authorized or not under the CFAA. Given the uncertainties regarding what practices are authorized or exceed authorized use when accessing an employer's computers, all counsel should consider suggesting to their clients that a review of their company's computer usage policies is in order. **TFL**

Ambrose V. McCall is a partner in the firm of Hinshaw & Culbertson in Peoria, Ill., and is a member of the Federal Civil Practice Section Council of the Illinois State Bar Association.

Endnotes

[1]A routing loop is a type of network failure in which

packets (the fundamental unit of information transport in all modern computer networks) continue to be routed in an endless circle instead of arriving at their intended destinations. (Definitions of Routing Loop and Packet, the Linux Information Project, 2005-2006).

[2]18 U.S.C. § 1030(g).

[3]*Id*.

[4]*Continental Group Inc. v. K.W. Property Management LLC*, 622 F. Supp. 2d 1357, 1369–1371 (S.D. Fla. 2009), citing 18 U.S.C. § 1030(a)(2)(C) and § 1030(a)(4)(explaining that the object of fraud must consist of more than use of computer and the value of such use must exceed $5,000 in any one-year period); *see also Ill. Corp. v. A-1 Tool Corp.*, 714 F. Supp. 2d 863, 876 (N.D. Ill. 2010)(citing *Continental Group* with approval and its explanation that loss requires interruption of service or damage to the computer or computer system).

[5]*See* 18 U.S.C. § 1030(g); *see also P.C. Yonkers v. Celebrations Superstore*, 428 F.3d 504, 510 (3d Cir. 2005)(citing *Pacific Aerospace & Elecs. Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003))("Employers … are increasingly taking advantage of the CFAA civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."); *Shurgard Storage Centers Inc. v. Safeguard Self Storage*, 119 F. Supp. 2d 1121, 1124 & n.3 (W.D. Wash. 2000) (explaining that 1994 amendment Congress made to the CFAA created a private cause of action under § 1030(g)).

[6]*Int'l Airport Centers LLC v. Citrin*, 440 F.3d 418, 420–421 (7th Cir. 2006) ("Citrin's breach of his duty terminated his agency relationship (more precisely, terminated any rights he might have claimed as IAC's agent—he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship.").

[7]*LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) ("The plain language of the statute therefore indicates that 'authorization' depends on actions taken by the employer. Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer."); *see also, U.S. v. Nosal*, ____ F.3d_____, 2011 WL 1585600 at **4–7 (9th Cir. April 28, 2011) (distinguishing *Brekka* on grounds that the defendant was subject to computer use policy restrictions) ("Therefore, as long as the employee has knowledge of the employer's limitations on that authorization, the employee 'exceeds authorized access' when the employee violates those limitations. It is as simple as that.").

[8]*E.F. Cultural Travel v. Explorica Inc.*, 274 F.3d 577, 583 (1st Cir. 2001)(citing the individual defendant's entry into a broad confidentiality agreement and Massachusetts state law imposing duty of good faith and fair dealing on all contracts governed by state law, as grounds for affirming the finding that defendant entity exceeded authorization by supplying proprietary data and related technical knowledge to retained Internet consultant).

[9]*U.S. v. Morris*, 928 F.2d 504, 509–11 (2d Cir. 1991) (citing and discussing the legislative history of the CFAA when explaining that the common understanding of the statutory term "authorization" applies and formulating intended use analysis); *U.S. v. John*, 597 F.3d 263, 271–273 (5th Cir. 2010)(applying "intended use" test to determine if the defendant exceeded authorized use); *U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007)("Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user.").

[10]*Id*.

[11]U.S. Const., Article VI, Clause 2.

[12]*Citrin, supra* note 6, at 419–421, *on subsequent appeal,* 455 F.3d 749 (7th Cir. 2006).

[13]18 U.S.C. § 1030 et seq.; *see also* Nick Ackerman and Patricia Finnegan, *Computer Law: Civil Relief Under CFAA*, Nat'l L. J. at A19 (Dec. 24-31, 2001) ("Enacted in 1984, the CFAA began as an exclusively criminal statute, designed to protect classified information on government computers and financial records or credit information on financial institution computers.").

[14]*Citrin, supra* note 6, at 419, citing 18 U.S.C. § 1030(a)(5)(A) and referencing CFAA's definition of protected computer as including an employee's laptop computer, found at 18 U.S.C. § 1030(e)(2)(B), defining "protected computer" to include a computer "which is used in or affecting interstate or foreign commerce or communication ... ."

[15]*Citrin, supra* note 6, at 419.

[16]*Id.* at 419–420

[17]18 U.S.C. § 1030 (a)(5)(B),(C).

[18]18 U.S.C. § 1030 (e)(8).

[19]18 U.S.C. § 1030(e)(11).

[20]18 U.S.C. § 1030(e)(6).

[21]18 U.S.C. § 1030(3)(1), *see also Register.com Inc. v. Verio Inc.*, 356 F.3d 393, 439 (2d Cir. 2004) ("Both §§ 1030(a)(2)(C) and (a)(5)(C) require that the plaintiff prove that the defendant's access to its computer system was unauthorized, or in the case of § 1030(a)(2)(C), that it was unauthorized or exceeded authorized access.").

[22]18 U.S.C. § 1030(e)(6).

[23]*Citrin*, *supra* note 6, at 420, citing 18 U.S.C. §§ 1030(a)(1), (2), (4); § 1030(e)(6); *EF Cultural Travel BV v. Explorica Inc.*, *supra* note 8, at 583–584; *Pacific Aerospace & Electronics Inc. v. Taylor*, *supra* note 5, at 1196–1197.

[24]*Id.*

[25]*Citrin*, *supra* note 6, at 420–421, *citing, in part, U.S. v. Galindo*, 871 F.2d 99, 101 (9th Cir. 1989); *Safeguard Self Storage supra* note 5, at 1123–1125; *Phansalkar v. Andersen Weinroth & Co. LLP*, 344 F.3d 184, 201–202 (2nd Cir. 2003) (per curiam); *State v. DiGiulio*, 172 Ariz. 156, 835 P.2d 488, 492 (App. 1992); Restatement (Second) of Agency, §§ 112, 387, 409(1) and comment b and illustration 2 (1958).

[26]*Citrin*, *supra* note 6, at 421

[27]*Id.*

[28]*Id.*

[29]*Brekka*, *supra* note 7, at 1132, citing *Perrin v. U.S.*, 447

U.S. 37, 42, 100 S.Ct. 311 (1979).

[30]*Brekka*, *supra* note 7, at 1133.

[31]*Id.*

[32]*Brekka*, *supra* note 7, at 1133, citing 18 U.S.C. § 1030(e)(6); *see also U.S. v. Nosal*, *supra* note 7.

[33]*Id.*

[34]*Id.*

[35]*Id.*

[36]*Brekka*, *supra* note 7 at 1129–1130.

[37]*Id.* at 1133–1134.

[38]*Id.* at 1134.

[39]*Id.* at 1134–1134, citing *U.S. v. Santos*, 553 U.S. 507, 128 S. Ct. 2020, 2025, 170 L. Ed. 2nd 912 (2008) (J. Scalia) (plurality opinion). In that case, the plurality opinion did not clarify the question of how to define "proceeds" under the federal money laundering statute, 18 U.S.C. § 1956(a)(1), other than holding that the word "proceeds" was inherently ambiguous because it could mean either "receipts" or "profits." As a result, the *Santos* Court applied the rule of lenity, meaning that where ambiguity exists over a term used in a criminal statute, the benefit of the doubt goes to the defendant, which in *Santos* meant that the term "proceeds" would be construed as "profits" rather than as "receipts." Congress closed the continuing use of the rule of lenity with respect to the money laundering statute by passing an amendment in May 2009.

[40]*Brekka*, *supra* note 7, at 1135.

[41]*Id.*

[42]*Id.*

[43]*Id.*

[44]*Id.* and n. 7 (also explaining that the permission granted to the employee to use the employer's computer nullified any attempt to apply the CFAA definition of exceeding authorized access detailed in 18 U.S.C. § 1030(e)(6)).

[45]*Explorica, supra* note 8, at 577, 583 (citing Massachusetts case law).

[46]*U.S. v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007), *cert. denied,* 552 U.S. 820 (2007)("With regard to his authorization, the CFAA does not define the term, but it does clearly differentiate between unauthorized users and those who exceed [] authorized access." *See* § 1030(e)(f) (defining "exceeding authorized access" as "access[ing] a computer with authorization and … us[ing] such access to obtain or alter information in the computer that the access or is not entitled so to obtain or alter …"); *see also* §§ 1030(a)(1), (a)(2), (a)(4). Several subsections of the CFAA apply exclusively to users who lack access authorization altogether. *see,* for example, §§ 1030(a)(3, (5)(A)(i), (5)(A)(ii), (5)(A)(iii). In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between "insiders, who are authorized to access a computer," and "outside hackers who break into a computer." *See* S. Rep. No. 104-357 at 11 (1996); *see also* S. Rep. No. 99-432 at 10, as printed in 1986 U.S.C.C.A.N. 2479, 2488 (1986) (stating that §§ 1030(a)(3) and (a)(5) "will be aimed at outsiders.").

[47]*Phillips, supra* note 9; *see also John*, *supra* note 9, at 272–273.

[48]*U.S. Gypsum Co. v. Lafarge North America Inc.*, 670 F. Supp. 2d 737, 743–744 (N.D. Ill. 2009); *Del Monte Fresh Produce, N.A. Inc. v. Chiquita Brands Intern. Inc.*, 616 F. Supp. 2d 805, 809–813 (N.D. Ill. 2009)(with discussion of related cases); *compare with A.V. ex rel. Vanderhye v. iParadigms LLC*, 562 F.3d 630, 645 (4th Cir. 2009)(noting that access was unauthorized by finding that the person registered and submitted papers as a student of a university in which he was not enrolled and had never attended, using a password obtained on the Internet).

[49]*See Clarity Services Inc. v. Barney*, 698 F. Supp. 2d 1309, n. 4 (M.D. Fla. 2010)(citing CFAA legislative history as stating an intent to remove from the scope of statute "one of the murkier grounds of liability, under which a [person's] access to computerized data might by legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization." S. Rep. No. 99-432, at 21, U.S.C.C.A.N. 1986, 2479, 2494–2495."); *but see White Buffalo Ventures, LLC v. Univ. of Texas*, 420 F.3d 366, 370 (5th Cir. 2005), *cert. denied,* 546 U.S. 1091 (2006)(finding that CAN-SPAM Act, 15 U.S.C. §§ 7701–7713, did not pre-empt the university's internal anti-spam policy due to textual tension in the act that triggered presumption against pre-emption); *see also Cipollone v. Liggett Group Inc.*, 505 U.S. 504, 517–518 (1992)(discussing presumption against preeemption).

[50]*City of Milwaukee v. Illinois and Michigan,* 451 U.S. 304, 313 (1981).

[51]*Id.*

[52]*Id.*

[53]*Id,* at 314.

[54]*U.S. v. Morris*, *supra* note 9, at 504, 511 ("The District Court decided that it was unnecessary to provide the jury with a definition of 'authorization.' We agree. Since the word is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning.").

[55]*See U.S. v. Middleton*, 231 F.3d 1207, 1211–1213 (9th Cir. 2000)(rejecting the proposed meaning of "individuals" and "person" in the CFAA as examples of technical use requiring reference to the Dictionary Act, 1 U.S.C. § 1 and noting congressional expansion of the CFAA as reflected in the Senate Report on the 1996 amendments) citing S. Rep. No. 104-357, pt. II, pt. IV(1)(E)).

[56]*See Clarity Services Inc., supra* note 49, at 1316 ("Furthermore, if an employee's authorization terminates at the moment the employee acquires an interest adverse to the employer, an employee who checks personal e-mail at work commits a federal crime."); *Orbit 1 Communications Inc. v. Numerx Corp.*, 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010)(holding that a plain language reading of the CFAA supports a narrow reading of the terms "access without authorization" and "exceeds authorized access" of the CFAA so as to exclude an employee's "misuse or misappropriation of information to which the employee freely was given access and which the employee lawfully obtained"); *see also Continental Group, supra* note 4, at 1357, 1372 (distinguishing case law cited by the defendant in light of the employer's right to control and set terms for authorization to access its computer systems

on grounds that the individual defendant downloaded files that were not needed for remaining business purposes at the time the individual defendant and former employee was negotiating to leave for employment by the co-defendant entity); *but see Guest-Tek Interactive Entertainment v. Pullen*, 665 F. Supp. 2d 42, 45–46 (D. Mass. 2009)(adopting a broad interpretation of the CFAA based on the view that amendments to the CFAA broadened its application); *NCMIC Finance Corp. v. Artino*, 638 F. Supp. 2d 1042, 1055–1059 and n.7 (S.D. Iowa 2009)(applying *Citrin*, rejecting narrow reading of CFAA provisions, and adopting a broad view interpretation of "exceeds authorized access" under 18 U.S.C. § 1030(e)(6)).

[57]*Lasco Foods Inc. v. HSSMC,* 600 F. Supp. 2d 1045, 1049–1050, 1053 (E.D. Mo. 2009).

[58]*Maxpower Corp. v. Abraham*, 557 F. Supp. 2d 955, 962–963 (W.D. Wis. 2008)(noting lack of evidence that passwords had been changed or that defendants deleted any electronic data from servers of the plaintiff, and weakness of evidence that defendants accessed computers of plaintiffs to obtain data they did not possess as employees, while also noting that evidence showing deletions of data by defendants were arguably consistent with company policy for clearing unnecessary data from laptops).

[59]*Patrick Patterson Custom Homes Inc. v. Bach*, 586 F. Supp. 2d 1026, 1035 (N.D. Ill. 2008)(discussing *Citrin* while noting that the plaintiffs alleged that the defendant intentionally accessed a protected computer in a way that exceeded her authority and intentionally, recklessly or otherwise resulted in damage consisting of permanently deleting and shredding a significant number of files and that the defendant deleted various files from a laptop computer and was behind the installation of "shredding" software on the laptop computer to destroy computer files and make them nonretrievable); *Modis Inc. v. Bardelli*, 531 F. Supp. 2d 314, 319 (D. Conn. 2008)(noting the split among the circuits over the terms "without authorization" and "exceeding authorization" in the CFAA but noting no need to resolve the conflict because the defendant had signed an employment agreement that limited the defendant's authorization to use the plaintiff's database to furtherance of plaintiff's business, thereby supporting denial of the motion to dismiss).