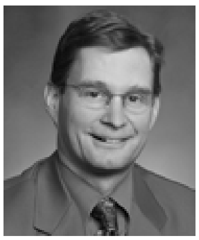
Bloomberg BNA

The United States
Law Week

Case Alert & Legal News™

The Computer Fraud and Abuse Act: 'Authorization' in Flux and the Ninth Circuit Dilemma



BY BRUCE SAMUELS AND CINDY VILLANUEVA

The Computer Fraud and Abuse Act (''CFAA'') was passed by Congress in 1984 to address the unauthorized access and use of computers and computer networks.[1] Although the CFAA is primarily a criminal statute, the 1994 amendment to the CFAA allowed individuals and companies to bring a private civil suit against a person who accessed a protected computer ''without authorization'' or while ''exceed[ing] authorized access.''[2] Increasingly, employers have used the CFAA to bring suit against former employees or agents (''insiders'') who have absconded with company data.[3] Within this context, there is currently a widening split among circuit and district courts over whether insiders can be held liable under the CFAA for accessing data without or in excess of authorization.[4] This diversity of viewpoints is currently playing out in the Ninth Circuit, where an en banc panel is considering whether to affirm a definition of authorization that will allow employers a remedy against insiders who exceed their authorized access, or whether to define to term narrowly.

There is a widening split among circuit and district courts over whether corporate insiders can be held liable under the CFAA for accessing data without or in excess of authorization.

BRUCE SAMUELS AND CINDY VILLANUEVA

Courts have generally applied one of two theories to determine what constitutes unauthorized access within the context of the CFAA: (1) agency theory, or (2) the plain language of the statute. Under the agency theory, or expansive view, an insider can be held liable under the CFAA for lacking authorized access by either acting disloyally to the employer or with an interest adverse to the employer's.[5] Under the plain language interpretation of the statute, or narrow view, an insider lacks authorized access only when the insider was never given

Bruce Samuels is a litigation partner at Lewis and Roca in Phoenix, Arizona, and previously served as president of the State Bar of Arizona's Intellectual Property Section. He can be contacted at bsamuels@lrlaw.com

Cindy Villanueva is an associate in the Commercial Litigation and Intellectual Property Groups at Lewis and Roca in Phoenix, Arizona. She can be reached at cvillanueva@lrlaw.com

[1] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, ch. 21, 98 Stat. 2190 (1984) (codified as amended at 18 U.S.C. § 1030 (2008))

[2] Computer Fraud and Abuse Act of 1994, Pub. L. No. 103-322, tit. XXIX, § 290001, 108 Stat. 2097.

[3] *See* Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B.J. 144, 144-45 (2008) (discussing the increasing use of the CFAA by employers against employees).

[4] Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 12 (noting evolution of litigation under the CFAA and the circuit split created with the U.S. Court of Appeals for the Ninth Circuit decision of *LVRV Holdings LLC v. Brekka*, 581 F.3d 1127, 1131, 78 U.S.L.W. 1174, (9th Cir. 2009)); Thomas Warren, *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. 2, Article 14 (2010) (stating that there has been a changing judicial interpretation of authorization under the CFAA from a broader interpretation to the narrow interpretation seen in Brekka).*

[5] *See International Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

permission to access particular information or when the insider's authority was affirmatively rescinded by the employer.[6]

For the past few years, employers within the Ninth Circuit have had to navigate an ever changing legal landscape to determine whether they could bring a claim under the CFAA against an insider who left the employer to join a competitor and took with them the employer's valuable company data. Before the appellate court waded into the debate, district courts within the Ninth Circuit had experienced an intra-circuit split. The district court decisions in *Shurgard*[7] and *Shamrock*[8] had provided some of the most cited interpretations of both the agency and plain language theories of authorization.[9] Now, with its decisions in *LVRC Holdings LLC v. Brekka*[10] and *United States v. Nosal*,[11] the Ninth Circuit has provided another twist to its history with the CFAA. The discussion below tracks the development of insider liability, or lack thereof, within Ninth Circuit case law.

Birth of the Agency Theory of Authorization And the Ninth Circuit's Intra-Circuit Split

In *Shurgard*, the U.S. District Court for the Western District of Washington adopted what is now know as the agency theory of authorization.[12] This case involved a dispute between two business competitors in the self-storage business.[13] The defendant hired the plaintiff's Regional Development Manager, Eric Leland, who had access to the plaintiff's confidential business plans, expansion plans, and other trade secrets.[14] While still an employee of the plaintiff, Leland e-mailed several of the plaintiff's trade secrets and other proprietary information to the defendant.[15] The plaintiff sued the defendant under the CFAA, on the theory that Leland intentionally accessed the plaintiff's computer without authorization, or in excess of authorization.[16] Finding guidance in the Restatement (Second) of Agency, the court held that "the authorization for [Shurgard's] . . . employees ended when the employees began acting as agents for the defendant."[17] The court concluded that the employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail."[18] Therefore, according to the district court, Leland "lost" his authorization and was thus without authorization under the CFAA when he accepted the job offer and chose to e-mail the proprietary information to the defendant.[19]

Shurgard's agency theory of authorization was given further credence when it was adopted by the Seventh Circuit in *International Airport Centers LLC. v. Citrin*.[20] In *Citrin*, an employee for a real estate agency decided to end his employment and go into business on his own.[21] Prior to leaving his job, he accessed the computer that was given to him by his employer and deleted all the information and data that he had been gathering in the course of his employment. He also loaded a secure-erasure program to prevent the recovery of the files.[22] Relying on agency law and on the *Shurgard* decision, the court held that Citrin's authorization to access the laptop "terminated when, having already engaged in misconduct and decided to quit [his job] in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer, in violation of the duty of loyalty that agency law imposes."[23] The court stated that by breaching his duty of loyalty, Citrin terminated his agency relationship and, with it, his authority to access the laptop.[24]

By breaching his duty of loyalty, the employee terminated his agency relationship and, with it, his authority to access his employer-supplied laptop.

Seventh Circuit in *Citrin*

The use of agency principles to define authorization within the CFAA has been adopted by other courts within the Ninth Circuit. One such case is *ViChip Corp. v. Lee*.[25] In *ViChip* the defendant, Tsu-Cgang Lee, was a former officer and director of ViChip Corp.[26] As an employee of ViChip, Lee was required to sign, and did in fact sign, an employee agreement that contained both an assignment provision and a confidentiality provision, in which he agreed to keep confidential any proprietary information he possessed and to return all proprietary information to ViChip in the event of termination.[27] While still an employee of ViChip, Lee removed from ViChip's offices and ViChip's patent counsel's office hard copies relating to ViChip's provisional patent

[6] *See Brekka*
[7] *Shurgard Storage Ctrs. Inc. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000)
[8] *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962 (D. Ariz. 2008)
[9] *See* Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 Bus. Law. 1395, 1409 (2006-2007) (stating that "[a]lthough a district court opinion, the analysis in *Shurgard* has been very influential. Its broad reading of the CFAA has been followed by the majority of other courts in the United States.); Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 Emp. Rts. & Emp. Pol'y J. 11, 19 n.36 (2008) (noting the "widespread endorsement of *Shurgard* and citing cases); Amy E. Bivens, *Employers Should Revisit Data Misuse Policy in Light of Ninth Circuit Brekka CFAA Ruling*, 8 Privacy & Sec. L. Rep. (BNA) 1441, 1441 (Oct. 5, 2009) (stating that *Shamrock* has been "widely cited outside the circuit" for its rejection of the *Citrin* line of reasoning).
[10] 581 F.3d 1127 (9th Cir. 2009)
[11] 642 F.3d 781, 79 U.S.L.W. 2475 (9th Cir. 2011).
[12] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1633 (2003).
[13] *Shurgard*, 119 F. Supp 2d at 1123.
[14] *Id.*
[15] *Id.*
[16] *Id.* at 1124.
[17] *Id.* at 1124.
[18] *Id.* at 1125.
[19] *Id.* at 1125.
[20] 440 F.3d 418 (7th Cir. 2006).
[21] *Id.* at 419.
[22] *Id.*
[23] *Id.* at 420.
[24] *Id.* at 420-21.
[25] 438 F. Supp. 2d 1087 (N.D. Cal. 2006).
[26] *Id.* at 1090.
[27] *Id.* at 1090-1091.

  LW ISSN 0148-8139

application; accessed ViChip's file server and deleted the contents of computer files that Lee had generated as an employee; deleted the contents of his ViChip-issued laptop computer; and removed the executed copy of his employee confidentiality agreement.[28] ViChip sued Lee under the CFAA for taking and deleting the electronic files without authorization. [29] Lee argued that he was not liable under the CFAA because his actions were technically authorized, since he deleted the files while still an officer and director of ViChip.[30] The court found that Lee, ''as both employee and officer, had a duty of loyalty that he owed ViChip, and therefore an agency relationship.''[31] The court held that in deciding to delete all the information from ViChip's server, Lee breached his duty of loyalty and terminated his agency relationship which, in turn, terminated his authorization to access the files.[32] Thus, Lee was ''without authorization'' when he took and deleted the electronic files from the server.[33]

The CFAA ''targets the unauthorized procurement or alteration of information, not its misuse or misappropriation.''

U.S. DISTRICT COURT FOR ARIZONA IN *SHAMROCK*

In 2008, the U.S. District Court for the District of Arizona in *Shamrock* broke ranks with *Shurgard* and adopted the plain language, or narrow interpretation of authorization, to conclude that insiders were not liable under the CFAA.[34] In *Shamrock*, an employer, Shamrock Foods Co., brought a complaint under the CFAA against a former employee, Jeff Gast, and a competitor after Gast e-mailed numerous documents containing Shamrock's confidential and proprietary information to his personal email account a few weeks before resigning and starting work with the competitor.[35] The defendants moved to dismiss the CFAA claims for failure to state a claim based on the argument that Gast did not violate the CFAA because he was authorized to access the computer and information at issue.[36] Shamrock argued that Gast was no longer authorized to access its confidential information once he acquired the improper purpose to use this information to benefit himself and the competitor.[37]

Looking first at the language of the CFAA, the court found that the plain language of the CFAA supports a narrow reading of the statute. It stated that the language of the CFAA ''targets the unauthorized procurement or alteration of information, not its misuse or misappropriation.''[38] Second, the court examined the legislative history and concluded that it supports a narrow view of the CFAA.[39] The court found that the committee reports emphasize concerns over hackers and computer trespass, not a concern for the subsequent use and misuse of information.[40] Finally, applying the rule of lenity, which calls for construing a criminal statute in favor of the defendant, the court found that it must apply a more narrow interpretation of authorization in order to avoid an overly broad and harsh result.[41] Under this analysis, the court held that because Shamrock conceded that Gast was permitted to view the specific files he allegedly e-mailed to himself, Gast did not access the information at issue ''without authorization'' or in a manner that ''exceed[ed] authorized access.'' *Id.* at 968.

As a result of the *Shamrock* decision, Ninth Circuit law on whether insiders could be held liable under the CFAA for removing and deleting confidential company data was up in the air. By refusing to follow the persuasive authority of *Citrin* and *Shurgard*, the Arizona District court in *Shamrock* created an intra-circuit split.

Ninth Circuit Case Law: From *Brekka* to *Nosal*

The Ninth Circuit finally resolved the intra-circuit split when it decided the case of *LVRC Holdings LLC v. Brekka*,[42] in which it adopted the narrow view of ''authorization'' under the CFAA, and as a result created a circuit split by explicitly rejecting the Seventh Circuit reasoning in *Citrin*. In *Brekka*, LVRC employed Brekka to manage one of its treatment facilities. As part of this position, Brekka received access to the computer system and full access to any files or records. He often transmitted files between his work and home computers.[43] Brekka eventually decided to start his own business and e-mailed a number of company records, including confidential information, from his work computer to his home laptop.[44] LVRC sought civil damages against him for violation of the CFAA.[45] LVRC argued the agency theory of authorization endorsed in *Citrin* by stating that Brekka's authorization to access the confidential files ended when he began acting in a manner contrary to LVRC's interests.[46]

The Ninth Circuit was ''unpersuaded by [the] interpretation'' of the Seventh Circuit.[47] Instead, the court considered the plain language of the statute and the rule of lenity[48] for criminal or quasi-criminal statutes.[49] The court noted that the text of the CFAA provided no

[28] *Id.* at 1091.
[29] *Id.* at 1100.
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] 535 F. Supp. 2d at 968.
[35] *Id.* at 963.
[36] *Id.* at 964.
[37] *Id.*
[38] *Id.*

[39] *Id.*
[40] *Id.* at 965-66.
[41] *Id.* at 967.
[42] 581 F.3d 1127 (9th Cir. 2009)
[43] *Id.* at 1129
[44] *Id.*
[45] *Id.* at 1130.
[46] *Id.* at 1132.
[47] *Id.* at 1134.
[48] The rule of lenity mandates that courts interpret ambiguous criminal statutes in favor of the defendant in order to avoid unexpected burdens. *Brekka*, 581 F.3d at 1134. According to *Brekka*, the ''rule of lenity, which is rooted in considerations of notice, requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government.'' *Id.* at 1135 (citing *United States v. Romm*, 445 F.3d 990, 1001 (9th Cir. 2006)).
[49] *Id.* at 1134-35.

definition of "authorization," so the court turned to its common usage.[50] For this, the court turned to a straightforward dictionary definition of "authorization" as "permission or power granted by an authority."[51] The court found no language in the CFAA that supported LVRC's agency-based definition, which finds that liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer.[52] The court held that "for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.' "[53] Thus, the court concluded that a person uses a computer "without authorization" when the person has not received permission to use the computer for any purpose or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.[54]

This holding, though, was short-lived, as it was limited by the recent case of *United States v. Nosal*,[55] which distinguished *Brekka* and adopted a more expansive interpretation of the term "without authorization" under a subsection of the CFAA that covers criminal actions. The defendant in *Nosal* was an executive for Korn/Ferry International, an executive search firm. After he left the company, he allegedly engaged three Korn/Ferry employees to help him start a competing business.[56] The government alleged that the three employees obtained trade secrets and other proprietary information by accessing the Korn/Ferry computer system.[57] The employees had signed agreements that expressly restricted the use and disclosure of proprietary information to legitimate Korn/Ferry business and warned employees that access to the computer system in violation of the agreement could lead to disciplinary action or criminal prosecution.[58]

The government charged Nosal with conspiring with the remaining employees to exceed their authorized access to the firm's computer systems in violation of 18 U.S.C § 1030(a)(4), which subjects to punishment anyone who "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value."[59] Nosal moved to dismiss the Section 1030(a)(4) counts, arguing that the phrase "exceeds authorized access" precludes an individual from using access to one part of a computer network to enter an otherwise forbidden part of a network, but that it does not preclude an individual from accessing files that are otherwise freely available. Nosal asserted that the files at issue were open to all employees and that neither he nor his alleged co-conspirators exceeded their authorized access to those files.[60] The district court agreed with Nosal and dismissed the CFAA counts, holding that under the Ninth Circuit's decision in *Brekka*, employees do not exceed authorized access to a computer network for CFAA purposes unless they clearly lack authority to enter or use the portion of the network at issue.[61]

On appeal, the panel in *Nosal* ruled that an employee exceeds authorized access within the meaning of the CFAA "when he or she violates the employer's computer access restrictions—including use restrictions."[62] The *Nosal* ruling narrowly interpreted the prior *Brekka* decision. The court stated that its decision was "simply an application of *Brekka*'s reasoning."[63] It noted that in *Brekka*, it held that it was the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or "without authorization." Therefore, it concluded that "the only logical interpretation of 'exceeds authorized access' is that the employer has placed limitations on the employee's 'permission to use' the computer and the employee has violated—or 'exceeded'—those limitations."[64] In addition, the court distinguished *Brekka* by noting that in *Nosal* there existed "a computer use policy that placed clear and conspicuous restrictions on the employees' access" both to employer's computer system in general and to specific data in question. No such agreement was in place in *Brekka*.[65] The court went on to say that as "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."[66]

Effectively, this case allows employers to bring a CFAA claim against Insiders who have access to company computers for specified purposes, but who access computers for purposes contrary to express policies of the company.

Aftermath of *Nosal*

After the panel issued its ruling, the opinion sparked a outburst of reaction in the press and among bloggers.[67] Some called for the decision to be reviewed *en banc* both because the decision is "hard to reconcile

[50] *Id.* at 1132.
[51] *Id.* at 1133.
[52] *Id.* at 1135.
[53] *Id.* at 1133.
[54] *Id.* at 1135.
[55] 642 F.3d 781 (9th Cir. 2011).
[56] *Id.* at 783.
[57] *Id.*
[58] *Id.*
[59] *Id.* at 782.

[60] *Id.* at 783.
[61] *Id.* at 784.
[62] *Id.* at 785.
[63] *Id.* at 787.
[64] *Id.*
[65] *Id.*
[66] *Id.* at 788.
[67] See, e.g., David Kravets, *Appeals Court: No Hacking Required to Be Prosecuted as a Hacker*, WIRED (Apr. 29, 2011), http://www.wired.com/threatlevel/2011/04/no-hacking-required (last visited March 5, 2012); John D. McLachlan, *Ninth Circuit Reverses Course on Computer Fraud and Abuse Act*, NON-COMPETE AND TRADE SECRETS BLOG, http://www.noncompetenews.com/post/2011/05/16/Computer-Fraud-Abuse-Act-Ninth-Circuit-Rerverses-Course.aspx (May 16, 2011) (last visited March 5, 2012); Michael Risch, *When the Right Interpretation of the Law is a Scary One (CFAA Edition)*, PRAWFSBLAWG, http://prawfsblawg.blogs.com/prawfsblawg/2011/04/when-the-right-interpretation-of-the-law-is-a-scary-one-cfaa-edition.html (Apr. 28, 2011) (last visited March 5, 2012).

  LW ISSN 0148-8139

with *Brekka* and because *Nosal* has such astonishing implications for the scope of government power.''[68] Others saw the decision as finally providing clear guidance for employers who want a remedy against dishonest employees who exceed their authorized access of their employers' computer systems.[69]

The importance of the *Nosal* decision beyond the context of criminal prosecutions can be seen in the fact that it was soon used in CFAA civil litigation. For example, in the case of *Facebook Inc. v. MaxBounty Inc.*,[70] the court relied on the *Nosal* holding to deny a motion to dismiss a claim for violating the CFAA. MaxBounty argued that ''because Facebook granted it access to the Facebook site, it could not have exceeded its 'authorized access' within the meaning of the CFAA.''[71] Facebook argued that ''MaxBounty and its affiliates registered for Facebook accounts and accepted Facebook's terms of use, which places restrictions on their use of the Facebook site'' and thus violated the CFAA by exceeding the restrictions placed on their accounts. Relying on *Nosal's* holding that ''an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed [ed] authorized access,'' the court held that Facebook's allegations were sufficient to sustain a claim under the CFAA.[72]

Nosal's influence, though, was soon suspended by the Ninth Circuit's Oct. 27, 2011 decision to grant *en banc* review.[73] Upon granting the *en banc* petition, the Ninth Circuit proclaimed that the three-judge panel decision in *Nosal* was no longer valid precedent and ''shall not be cited as precedent by any court.''[74]

Oral argument was held before the Ninth Circuit on Dec. 15, 2011.[75] At oral argument, the Department of Justice argued that the proper definition of the term ''exceed authorized access'' is where the employee is given limited authority to access information but goes beyond that authority. When pressed on whether the government was reading a ''use'' component to the statute, the government denied such a reading and stated that it was a restriction on access, not use. According to the government, the employee was violating access restrictions when the employee accessed information for a purpose that was beyond what was authorized by the employer.

The panel repeatedly challenged the governments position on the scope of the CFAA. After the government argued that intentionally violating the terms of service on, for example, Facebook or Match.com, was in fact a federal crime under 18 U.S.C. § 1030(a)(2)(C), but stated that DOJ would never prosecute such a case, Chief Judge Alex Kozinski asked the DOJ attorney, ''we don't really want to allow everybody in the country to be at the mercy of their local U.S. attorney, do we? That would be exceedingly bad policy and to be avoided at all costs—to give the hands of the government the ability to prosecute everybody who has access to a computer and say 'I can't imagine they would go after it.' That would be a really dangerous thing to do, wouldn't it?''

Nosal's basic argument was that the scope of ''exceed authorized access'' should be limited to the circumvention of technological or code-based barriers not based on written employer restrictions on use. Nosal's counsel stated that the definition of ''exceed authorized access'' and ''without authorization'' are not collapsed under the code-based definition. Instead, ''without authorization'' applies to outside hackers while ''exceed authorized access'' applies to inside hackers, those who have access to one part of the computer system and use that access to gain access to another part of the system they were never given permission to access. Nosal's counsel faced the toughest questions from Judge Richard Tallman, who suggested that the court could rule for the government without upsetting the *Brekka* precedent. Judge Barry G. Silverman also weighed in skeptically, noting that other circuits have not gone Nosal's way. Finally, one of the judges asked if accepting Nosal's position would create a clear circuit split with the 11th Circuit in *United States v. Rodriguez*[76]. Nosal's counsel commented that there already exists a circuit split in how courts have interpreted the term ''exceed authorized access.''

Overall, it was unclear how the court would rule. Judge Kozinski was fairly clearly on the side of Nosal while Judge Tallman seemed to side with the government. Most of the other judges did not tip their hand on their position.

The fact that the Ninth Circuit accepted en banc review does not bode well for DOJ's position. If the Ninth Circuit limits the application of the CFAA to outside hackers, employers in the Ninth Circuit will not have a remedy under the federal law against employees who had authorized access to the company's computers. Such a decision will result in a spit between the Ninth Circuit and the First, Seventh, Fifth, and Eleventh circuits.[77] Ultimately, the U.S. Supreme Court will likely be asked to resolve the conflict.

---

[68] *See* Orin Kerr, *Ninth Circuit Holds That Violating Any Employer Restriction on Computer Use ''Exceeds Authorized Access'' (Making It a Federal Crime)*, THE VOLOKH CONSPIRACY (April 28, 2011), http://volokh.com/2011/04/28/ninth-circuit-holds-that-violating-any-employer-restriction-on-computer-use-exceeds-authorized-access-making-it-a-federal-crime (last visited March 5, 2012); *see also* Steve Kalar, *Case o' The Week: NSFW*—Nosal *and ''Unauthorized'' Access to an Employer's Computer*, NINTH CIRCUIT BLOG *(May 8, 2011), http://circuit9.blogspot.com/search?q=CFAA (noting that dissent had better reasoned argument) (last visited March 5, 2012)*.

[69] *See* Robert Milligan, *The Federal Computer Fraud and Abuse Act is Back in Play for Employer Suits Against Dishonest Employees in the Ninth Circuit*, http://www.tradesecretslaw.com/2011/05/articles/computer-fraud-and-abuse-act/the-federal-computer-fraud-and-abuse-act-is-back-in-play-for-employer-suits-against-dishonest-employees-in-the-ninth-circuit (May 2, 2011) (last visited March 5, 2012).

[70] No. 10-cv-4712, 011 WL 4346514 (N.D. Cal. Sept. 14, 2011).

[71] *Id.* at * 5.

[72] *Id.*

[73] *See* United States. v. Nosal, 80 U.S.L.W. 561 (9th Cir. Oct. 27, 2011).

[74] *Id.*

[75] *See* http://www.ca9.uscourts.gov/datastore/calendaring/2011/11/23/nsfEB12_11.pdf.

[76] 628 F.3d 1258, 1263, 79 U.S.L.W. 1856 (11th Cir. 2010).

[77] *Brekka*, 581 F.3d at 1131 (9th Cir. 2009); *EF Cultural Travel BV v. Explorica Inc.*, 274 F.3d 577, 582 (1st Cir. 2001); *Citrin*, 440 F.3d at 420-21 (7th Cir. 2006); *United States v. John*, 597 F.3d 263, 271 (5th Cir. 2010); *Rodriguez*, 628 F.3d at 1263, (11th Cir. 2010).