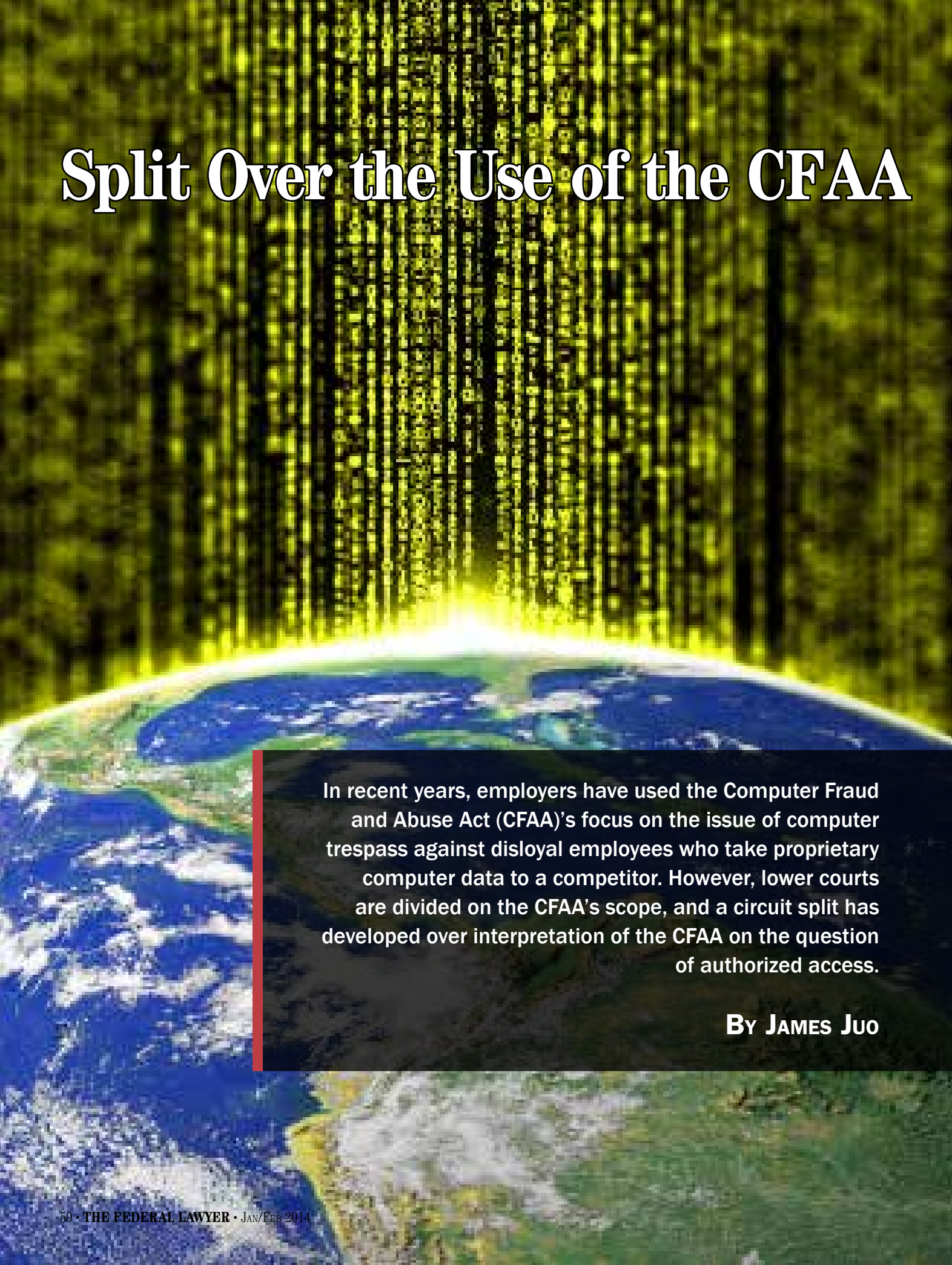


Split Over the Use of the CFAA



In recent years, employers have used the Computer Fraud and Abuse Act (CFAA)'s focus on the issue of computer trespass against disloyal employees who take proprietary computer data to a competitor. However, lower courts are divided on the CFAA's scope, and a circuit split has developed over interpretation of the CFAA on the question of authorized access.

By JAMES JUO

Against Disloyal Employees

The Computer Fraud and Abuse Act (CFAA), a computer trespass statute, has been called “one of the broadest federal criminal laws currently on the books.”¹ When enacted in 1984, the act was intended to criminalize computer hacking.² One Congressman noted that “[t]he hacker of today can become the white-collar crime superstar of tomorrow.”³ Originally designed to protect computers having a specified federal interest, such as national security, financial records, and government property,⁴ the CFAA has been expanded a number of times.⁵ For example, the statute was expanded in 1994 to allow private entities to assert a civil cause of action and obtain compensatory damages and other equitable relief.⁶ In 1996, the CFAA was amended to expand the class of protected computers to include any computer “used in interstate or foreign commerce or communication.”⁷ In about a dozen years, the scope of this criminal statute went from covering a limited set of protected computers to possibly every Internet-connected computer in the United States.⁸

The CFAA also has been called “remarkably vague,” leaving the courts to grapple with what the statute means.⁹ The CFAA has been asserted to cover a wide range of activity such as: exploiting code-based security flaws;¹⁰ launching a denial of service attack on a website;¹¹ spoofing IP addresses to avoid access restrictions;¹²

allowing an unauthorized person to use the valid password of another;¹³ violating a website’s terms of service;¹⁴ and accessing information stored on an employer’s computer for a competing business.¹⁵ In recent years, employers have used the CFAA against disloyal employees who take proprietary computer data to a competitor.¹⁶ Indeed, disgruntled employees who are about to resign still have access to computer systems and the ability to copy data prior to their departure.¹⁷ One advantage of using the CFAA is its focus on the issue of computer trespass rather than on the quality of the computer data being accessed.¹⁸

However, the lower courts “are deeply divided on the [CFAA’s] scope, with some courts concluding that the law is remarkably broad.”¹⁹ And a circuit split has developed over how to interpret the CFAA on the question of authorized access, including whether employers can continue to use the CFAA against disloyal employees.

Circuit Split Over “Access”

The CFAA prohibits “access without authorization” and “exceed[ing] authorized access” to a protected computer.²⁰ In 2006, the Seventh Circuit relied on the agency relationship between an employee and employer to determine whether access was authorized or not, in *International Airport Centers, L.L.C. v. Citrin*.²¹ The defendant Citrin decided to start his own business in competition with his employer, International Airport Centers (IAC), and used a secure-erase program that permanently erased all the data (presumably including evidence of Citrin’s allegedly improper conduct) on a laptop computer provided to him by IAC prior to quitting.²² Citrin “knew the company had no duplicates of [the destroyed data].”²³

The court noted that an employee’s authorization to access the employer’s computer data is based on the agency relationship between the employer and employee, and Citrin’s authorization ended when he breached the duty of loyalty to IAC.²⁴ “[T]he authority of the 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.”²⁵ Taking and using an employer’s proprietary information in competition against that employer would appear to constitute a serious breach of loyalty.

A broad interpretation of access under the CFAA—finding liability for an employee who violates the computer use policies of an employer—was adopted by the Fifth and Eleventh circuits as well.²⁶

The Ninth Circuit, on the other hand, was charting a different path, and, in 2012, addressed the CFAA *en banc* in *United States v. Nosal*.²⁷ Nosal was an independent contractor (and a former high-level employee) at executive search firm Korn/Ferry International who signed an agreement to not compete against Korn/Ferry for one year.²⁸ During that time, however, Nosal accessed confidential and proprietary information in the Korn/Ferry computer system to obtain customer lists and other trade secrets for a competing business he was starting. Several employees also helped access the Korn/Ferry computer system to obtain confidential information and trade secrets for Nosal. Korn/Ferry had an express computer usage policy, which was reflected in an opening computer screen warning: “This product is intended to be used by Korn/Ferry employees for work on Korn/Ferry business only.”²⁹

The Ninth Circuit held that the CFAA did not give a private party’s use policies the force of law.³⁰ Because an employer’s use-restrictions or a website’s terms of service policies may change at any time with little or no prior notice, what was lawful conduct one day could become unlawful the next.³¹ This could impose unexpected burdens on defendants. The court suggested that CFAA would be unconstitutionally vague if violating a website’s terms of service (which typically are written to give the website’s owner a broad right to cancel accounts without liability) could be construed to be unauthorized or to have exceeded authorized access that results in criminal liability.³²

Among the litany of hypothetical examples of adverse consequences that may arise from giving a private party’s use policies the force of law, Chief Judge Kozinski noted that numerous dating websites have terms of service that “prohibit inaccurate or misleading information,” and that under the government’s proposed interpretation of the CFAA, “describing yourself as ‘tall, dark and handsome,’ when you’re actually short and homely, will earn you a handsome orange jumpsuit.”³³

Many workplaces also have policies that forbid using the Internet at work for a non-work purpose, and the tendency of people’s minds to wander and procrastinate by connecting to the Internet at work for a non-work purpose “would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime.”³⁴ To police against improper conduct by an employee involving a computer, the court noted that employers would still have recourse to other laws regarding wire fraud, trade secrets, or contracts, instead of the CFAA.³⁵

The court concluded that the “exceeds authorized access” language “in the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its *use*.”³⁶

The Ninth Circuit’s narrow interpretation of the CFAA in *Nosal* has since been adopted by the Fourth Circuit and by district courts in other circuits.³⁷ So the ability to use the CFAA against disloyal employees in those jurisdictions is limited. Accordingly, employers should maintain appropriate physical and technological barriers as part of their internal security protocols and data protection strategies for sensitive information, especially for an employer with branches in multiple states. With the split between the *Nosal* and *Citrin* lines of authority, whether an employer’s computer-use policy can be the basis for a CFAA claim against a disloyal employee may depend on which part of the country the alleged unauthorized access happens to occur.

The Story of Aaron Swartz

While there has been speculation that the circuit split over the CFAA may eventually come before the U.S. Supreme Court, interest in legislative reform of the CFAA has since escalated as a result of the tragic death of Aaron Swartz.

At age 14, Swartz was working with leading technologists to craft open standards such as the RSS specification for sharing information on the Internet.³⁸ He then helped Lawrence Lessig with Creative Commons, which promotes the use of simple, standardized copyright licenses that give the public permission to share and use creative works.³⁹ At age 19, he was a founding developer of Reddit, a widely used social news website where users can post news links and vote on them.⁴⁰ Swartz later became a political activist for Internet freedom and social justice issues, and formed the advocacy group Demand Progress.⁴¹

In late 2010, however, Swartz allegedly attempted to access and download a large number of academic articles from JSTOR (or Journal Storage), a nonprofit that provides a searchable database of digitized academic journals.⁴² Libraries and universities pay a subscription fee to JSTOR for access.⁴³ JSTOR’s terms of service (TOS) prohibit downloading or exporting documents using automated computer programs, and JSTOR also uses technological measures to prevent such automated downloading.⁴⁴

Swartz allegedly used a laptop connected to the computer network of the Massachusetts Institute of Technology (MIT), a JSTOR subscriber, to access the database.⁴⁵ MIT is known to have a permissive computer culture, and its network is open and available to anyone on campus, whether or not they are part of the school. As a result, anyone on the MIT campus could have access to JSTOR.⁴⁶

In response to Swartz’s downloading of JSTOR articles, JSTOR blocked the Internet protocol (IP) address for MIT that had been assigned to Swartz’s laptop to prevent further access. Swartz then established a new IP address on the MIT network to sidestep JSTOR’s technical block.⁴⁷ JSTOR complained to MIT about this activity, and MIT blocked the Swartz laptop from its network based on the laptop’s MAC address (which is a unique identifier assigned to each computer’s network interface).⁴⁸ Swartz avoided MIT’s block by changing (spoofing) his laptop’s MAC address.⁴⁹ This cat-and-mouse game went on for a few weeks in September 2010 but later ceased as Swartz apparently became more interested in the upcoming November elections than in this academic downloading escapade.

Later, in November or December 2010, Swartz allegedly plugged his laptop directly into MIT’s computer network in an unlocked wiring closet located in a basement on MIT’s campus, and continued to download articles from JSTOR, but at a slower rate.⁵⁰ MIT traced the location of the laptop in the closet and decided to treat the downloading as a criminal matter. Local police were joined by a Secret Service agent, who recommended installing a surveillance camera in the closet.⁵¹ A few days later, in early January 2011, Swartz allegedly entered the wiring closet and removed the laptop.⁵² He was arrested later that day.

JSTOR declined to pursue legal action against Swartz after he turned over his hard drives, which contained 4.8 million JSTOR documents.⁵³ But the federal government charged Swartz with violations of the CFAA in the U.S. District Court for the District of Massachusetts.⁵⁴ For violating JSTOR’s use policies and technical restrictions, the U.S. Attorney’s Office stated that Swartz “faces up to 35 years in prison ... and a fine of up to \$1 million.”⁵⁵ Carmen M. Ortiz, the U.S. attorney overseeing the case, was quoted as saying that “stealing is stealing, whether you use a computer command or a crowbar, and whether

you take documents, data or dollars.”⁵⁶ It has been reported that the government asserted the documents downloaded from JSTOR were worth \$2 million, which would justify a seven year prison sentence.⁵⁷ But the downloaded documents apparently included archaic publications such as the 1942 edition of the *Journal of Botany*.⁵⁸ According to Professor Lessig, “[A]nyone who says that there is money to be made in a stash of academic articles is either an idiot or a liar.”⁵⁹

A computer expert for the defense asserted that Swartz did not “hack” the JSTOR website under any reasonable definition because he did not use parameter tampering, break a CAPTCHA, or do anything more complicated than automate a process that downloads a file in the same manner as clicking “Save As” from a browser.⁶⁰ Whether this defense would have been successful is questionable because the CFAA prohibits more than just traditional hacking. Furthermore, the case was pending in the District of Massachusetts, and in *EF Cultural Travel BV v. Zefer Corp.*, the First Circuit previously had stated in dicta that explicit restrictions set forth on a website’s terms of service could be enforced under the CFAA.⁶¹ Thus, a Massachusetts court might not have followed *Nosal’s* narrow interpretation of the CFAA that would have excluded terms of service violations.

Moreover, a later post-*Nosal* case, *Craigslist, Inc. v. 3Taps, Inc.*, held that changing one’s IP address to circumvent IP address blocking could constitute unauthorized access under the CFAA.⁶² The defendant, 3Taps, was accused of scraping data from the Craigslist

person does not use ‘anonymous proxies’ to bypass an IP block set up to enforce a banning communicated via personally addressed cease-and-desist letter.”⁶⁸ The court concluded that “a meaningful distinction exists between restricting uses of a website for a certain purpose and selectively restricting access to a website altogether.”⁶⁹

The court noted that 3Taps had articulated “intuitive ways that Congress might draw the relevant statutory lines,” such as suggesting that the CFAA should only protect “non-public information protected by a password, firewall, or similar restriction.”⁷⁰ But the statute currently “protects all information on any protected computer accessed ‘without authorization,’” and nothing in the statutory language excludes the computers for a website from being protected by the CFAA.⁷¹ Although the “current broad reach of the CFAA may well have impacts on innovation, competition, and the general ‘openness’ of the internet ... it is for Congress to weigh the significance of those consequences and decide whether amendment would be prudent.”⁷²

For Swartz, facing criminal charges under the broad reach of the CFAA for a year-and-a-half, the government offered him a plea bargain requiring a felony conviction, under which the government would recommend a six-month prison term (although his defense counsel could argue to the judge for probation instead).⁷³ The government would not back off its demand for jail time.⁷⁴ With his case moving toward trial, 26-year-old Swartz took his own life in January 2013.⁷⁵

Chief Judge Kozinski noted that under the government’s proposed interpretation of the CFAA, “describing yourself as ‘tall, dark and handsome’ when you’re actually short and homely, will earn you a handsome orange jumpsuit.”

website to aggregate and republish ads from that website. Craigslist sent 3Taps a cease-and-desist letter and blocked the IP addresses associated with 3Taps—but 3Taps continued to access the Craigslist website by changing its IP addresses.⁶³

Craigslist was a public website, but the court noted that Craigslist had exercised its power to revoke the general permission it granted to the public to access the information on its website on a case-by-case basis through its cease-and-desist letter and IP blocking measures, so further access by 3Taps after that rescission could be without authorization.⁶⁴ While the court acknowledged that “IP blocking may be an imperfect barrier to screening out a human being who can change his IP address,” the court found that “it is a real barrier.”⁶⁵

Circumventing of an IP address block after receiving a cease-and-desist letter was distinguished from merely violating terms of service (which under *Nosal* would not be a CFAA violation). The court noted that having one’s IP address blocked after receiving a letter constituted clear notice that one’s specific right to access the website had been revoked.⁶⁶ But the court also noted that there could be “difficult questions concerning the precise contours of an effective ‘revocation’ of authorization to access a generally public website.”⁶⁷ Accordingly, the notice issue may turn on how clearly the website ban is communicated to the defendant, together with the technological restriction employed.

Addressing 3Taps’ argument that prohibiting people from accessing websites they have been banned from could criminalize large swaths of ordinary behavior under the CFAA, the court noted that “the average

Aaron’s Law

There have been several proposals to amend the CFAA after Swartz’s death became a rallying cry to have Congress reform the CFAA.

Orin Kerr, a professor at the George Washington University Law School and a former federal prosecutor, has proposed a number of changes to the CFAA including “(1) eliminating liability for exceeding authorized access, (2) tightening the felony thresholds throughout the statute, and (3) eliminating several sections of the statute, including ... the civil liability provision, which is chiefly responsible for the overly expansive readings of the statute.”⁷⁶ He also proposed that “access without authorization” means “to circumvent technological access barriers to a computer or data without the express or implied permission of the owner or operator of the computer.”⁷⁷ Kerr later posted a series of scenarios in an attempt to help identify what should be the proper line between access to a computer that is authorized versus not under the CFAA.⁷⁸ Those scenarios included examples of circumventing cookie-based restrictions and CAPTCHA gates.⁷⁹

The Electronic Frontier Foundation (EFF) has proposed defining “without authorization” to mean “to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to access the computer, file, or data, but does not include circumventing a technological measure that does not effectively control access to a computer, file, or data.”⁸⁰ The EFF wants to avoid penalizing “people who have permission to access data but use light technical work-arounds to access that data.”⁸¹ The EFF appears to have borrowed

language from the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA), which have been interpreted to mean that a technological measure restricting one form of access but leaving another route wide open, does not “effectively control access.”⁸²

On the heels of these proposals, Rep. Zoe Lofgren (D-Cal.), along with Reps. James Sensenbrenner (R-Wis.), Mike Doyle (D-Pa.), Yvette Clarke (D-N.Y.), and Jared Polis (D-Co.), introduced Aaron’s Law Act of 2013 to reform the CFAA.⁸³ Sen. Ron Wyden (D-Ore.) introduced companion legislation in the Senate.⁸⁴ The bill would eliminate the “exceeds authorized access” language from the statute and define “access without authorization” to mean obtaining information on a protected computer that the accessor lacks authorization to obtain by circumventing one or more technological measures that exclude or prevent unauthorized individuals from obtaining or altering that information.⁸⁵ Lofgren’s accompanying summary identifies examples of technological or physical measures as “password requirements, cryptography, or locked office doors.”⁸⁶ The summary further states that the proposed changes are intended to codify the *Nosal* line of decisions, and make clear that the CFAA does not outlaw mere violations of terms of service, while “bypassing technological or physical measures via deception (as in the case with phishing or social engineering), and scenarios in which an authorized individual provides a means to circumvent to an unauthorized individual (i.e., sharing login credentials)” would be prohibited.⁸⁷ This proposed legislation would require employers nationwide to focus more on technological measures to secure their computer systems rather than on corporate policies in order to assert the CFAA against a disloyal employee who misuses his or her access to the employer’s computer data.

It may be a long political journey for these legislative proposals to reform the CFAA especially since “Congress rarely scales back criminal laws.”⁸⁸ And proposals to narrow the scope of a criminal statute often include provisions for increased penalties.⁸⁹ “To be successful, [the effort to pass Aaron’s Law] will likely take substantial time and require sustained and intense support from all of you,” according to Lofgren.⁹⁰ ◻

James Juo is a partner at Fulwider Patton LLP, a Los Angeles law firm specializing in intellectual property including patents and trademarks. He can be reached at jjuo@fulpat.com. © 2014 James Juo. All rights reserved.

Endnotes

¹Paul J. Larkin, Jr., *United States v. Nosal: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIR. REV. 257, 261 (2012).

²Technically speaking, the CFAA was a 1986 amendment to 18 U.S.C. § 1030, but the common convention is to refer to Section 1030 as a whole as the CFAA. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 n.2 (2012). The original 1984 statute was called the Comprehensive Crime Control Act (CCCA). *Id.* at 1563-64.

³Thomas P. O’Brien, et al., *Access Versus Use: Nosal Decision Creates Circuit Split*, LOS ANGELES DAILY JOURNAL (May 25, 2012).

⁴The legislative history of the CFAA refers to the 1983 movie *WarGames*, whose plot involved a teenager gaining unauthorized access to a classified government computer and nearly causing World War III. See H.R. Rep. No. 98-894, at 6 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3695 (“For example, the motion picture *WarGames* showed a realistic representation of the automatic dial-

ing and access capabilities of the personal computer.”); see also Matthew Kapintanyan, *Beyond WarGames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL’Y FOR INFO. SOC’Y 405, 410 (Winter 2012).

⁵Kerr, *supra* note 2, at 1566.

⁶*Id.* (citing 18 U.S.C. § 1030(g)).

⁷*Id.* at 1567-68 (citing 18 U.S.C. § 1030(e)(2)).

⁸*Id.* at 1571 (“Perhaps the only identifiable exclusion from the scope of protected computers is a ‘portable handheld calculator.’”).

⁹*Investigating and Prosecuting 21st Century Cyber Threats: Hearing Before United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations*, 113th Cong. 1 (Mar. 13, 2013) (written statement of Orin S. Kerr, Fred C. Stevenson Research Prof., George Washington Univ. Law School), available at www.volokh.com/wp-content/uploads/2013/03/KerrCFAATestimony2013.pdf.

¹⁰See, e.g., *United States v. Morris*, 928 F.2d 504, 505 (2d Cir. 1991) (using an Internet worm to exploit a security flaw in a computer’s programming code); *YourNetDating, Inc. v. Mitchell*, 88 F. Supp. 2d 870, 871 (N.D. Ill. 2000) (hacking a dating service website and diverting its users to a porn site).

¹¹See, e.g., *Pulte Homes, Inc. v. Laborers’ Int’l Union of N. Am.*, 648 F.3d 295, 299-98 (6th Cir. 2011) (impairing a computer network by directing a large number of e-mails at a specific address).

¹²See, e.g., *Four Seasons Hotels & Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1298 (S.D. Fla. 2003) (“[S]poofing is forging an IP address so that when a person receives a data packet or communication they believe it is coming from somewhere else.”), *aff’d in part, rev’d in part*, 138 F. App’x 297 (11th Cir. 2005); *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1037 (N.D. Cal. 2012) (“[O]ne of the objectives of the [proxy system] design was to reconfigure the IP connections if an IP address was blocked.”).

¹³See, e.g., *State Analysis, Inc. v. Am. Fin. Servs.*, 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) (“KSE accessed StateScape’s website using usernames and passwords that did not belong to it.”).

¹⁴See, e.g., *Am. Online, Inc. v. Nat’l Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1260 (N.D. Iowa 2000) (violating AOL’s terms of service to send bulk emails).

¹⁵See, e.g., *Meats by Linz, Inc. v. Dear*, No. 10-1511-D, 2011 WL 1515028, at *1 (N.D. Tex. Apr. 20, 2011) (downloading employer’s confidential information after hours and then e-mailing resignation two hours later).

¹⁶*Guest-Tek Interactive Entm’t Inc. v. Pullen*, 665 F. Supp. 2d 42, 45-46 (D. Mass. 2009) (“As the Third Circuit has noted, ‘[e]mployers... are increasingly taking advantage of the CFAA’s 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.’” (quoting *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005))); Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 9 Duke Law & Tech. R. 1, 12 (2010) (“plaintiffs have until recently found the federal courts amenable to its use in civil suits against disloyal employees”); Pamela Taylor, *To Steal Or Not To Steal: An Analysis of the Computer Fraud and Abuse Act and Its Effect on Employers*, 49 Hous. L. Rev. 201, 208 (2012) (the CFAA “is increasingly used against former employees”).

¹⁷Taylor, *supra* note 16 at 208-209.

¹⁸Kapintanyan, *supra* note 4 at 418 (“the CFAA provides a remedy



without requiring the employer to prove the breach of an employment agreement or that the data taken is secret or confidential”); *see also* Jennifer Granick, *Towards Learning from Losing Aaron Swartz*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 14, 2013, 4:37 PM), cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz. (“Another way to look at the CFAA, is that it protects the box”).

¹⁹Kerr, *supra* 9.

²⁰See 18 U.S.C. § 1030(a)(2); *see also* Jennifer Granick, *Thoughts on Orin Kerr’s CFAA Reform Proposals: A Great Second Step*, The Center for Internet and Society (Jan. 23, 2013, 9:43 PM), cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step (“Historically, the CFAA partitioned the world of computer criminals into two camps, outsiders who ‘access without authorization’ and wayward insiders who abuse their position of trust to ‘exceed authorized access’ and obtain information they were not entitled to.”).

²¹*Int’l Airport Centers, L.L.C. v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

²²*Id.* at 419-20.

²³*Id.* at 421.

²⁴*Id.*; *see also Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000) (cited and relied upon by *Citrin*).

²⁵*Citrin*, 440 F.3d at 421.

²⁶*United States v. John*, 597 F.3d 263, 273 (5th Cir. 2010) (bank employee accessed customer accounts for the improper purpose of incurring fraudulent charges on those accounts.); *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010) (employee of the Social Security Administration (SSA) used an SSA database for personal reasons).

²⁷*United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc).

²⁸*Id.* at 856.

²⁹*Id.* at 856 n.1.

³⁰*Id.* at 860; *see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1134 (9th Cir. 2009) (noting that nothing in the plain language of the CFAA suggests that liability for accessing a computer without authorization turns on whether the defendant breached a duty of loyalty to an employer).

³¹*Nosal*, 676 F.3d at 862.

³²*Id.*; *see also United States v. Drew*, 259 F.R.D. 449, 466 (C.D. Cal. 2009) (finding that the CFAA did not apply to violations of a website’s terms of service).

³³*Nosal*, 676 F.3d at 861-62.

³⁴*Id.* at 859-60; *see also Drew*, 259 F.R.D. at 467 (noting that a broad interpretation of the CFAA would result in a “standardless sweep”).

³⁵*Nosal*, 676 F.3d at 863.

³⁶*Id.* at 864 (emphasis in original). The dissent criticized the majority’s focus on hypotheticals and “hyper-complicated [parsing of the CFAA] that distorts the obvious intent of Congress.” *Id.* (Silverman, J., dissenting). On April 24, 2013, in a jury trial after the remand, Nosal was found guilty of violating the CFAA for using a borrowed password to access Korn/Ferry’s computer database. *United States v. Nosal*, CR-08-0237 EMC, 2013 WL 4504652, at *3-*4 (N.D. Cal. Aug. 15, 2013) (Mr. Nosal also was convicted of violating the Economic Espionage Act (“EEA”) in addition to the CFAA).

³⁷*See WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 203 (4th Cir. 2012); *JBCHoldings NY, LLC v. Pakter*, 931 F. Supp. 2d 514, 522-23 (S.D.N.Y. 2013). Even so, courts are still exploring the limits of Nosal. *See Synopsys, Inc. v. ATopTech, Inc.*, No. 13-cv-

02965, 2013 WL 5770542, at *10 (N.D. Cal. Oct. 24, 2013) (“the state of CFAA doctrine in the Ninth Circuit suggests that while a breach of a contractual provision may in some cases be enough to allege unauthorized access, *see* Craigslist Inc., 2013 WL 1819999, at *4, such an alleged breach must be pled with enough clarity and plausibility to state that access itself—not just a particular use—was prohibited”).

³⁸Tim Carmody, *Memory to Myth: Tracing Aaron Swartz Through the 21st Century*, THE VERGE (Jan. 22, 2013, 12:30 PM), www.theverge.com/2013/1/22/3898584/aaron-swartz-profile-memory-to-myth.

³⁹Lawrence Lessig, *Prosecutor as Bully*, LESSIG BLOG, v2 (Jan. 12, 2013), lessig.tumblr.com/post/40347463044/prosecutor-as-bully.

⁴⁰Larissa MacFarquhar, *Requiem for a Dream*, THE NEW YORKER (Mar. 11, 2013), www.newyorker.com/reporting/2013/03/11/130311fa_fact_macfarquhar?currentPage=all.

⁴¹*See* DEMAND PROGRESS, www.demandprogress.org/ (last visited Mar. 25, 2013); *see also* Justin Peters, *The Idealist: Aaron Swartz Wanted to Save the World. Why Couldn’t He Save Himself?*, SLATE (Feb. 7, 2013, 9:47 PM), www.slate.com/articles/technology/technology/2013/02/aaron_swartz_he_wanted_to_save_the_world_why_couldn_t_he_save_himself.html.

⁴²Superseding Indictment at 1, *United States v. Swartz*, No. 11-cr-10260, Dkt. No. 53 (D. Mass. Sept. 12, 2012). The motivation for Swartz to have engaged in this alleged downloading is unclear, but the FBI previously had investigated him for having downloaded a large number of freely available court documents from PACER about two years earlier. Ryan Singel, *FBI Investigated Coder for Liberating Paywalled Court Records*, WIRED (Oct. 5, 2009, 8:48 PM), www.wired.com/threatlevel/2009/10/swartz-fbi/.

⁴³Superseding Indictment, *supra* note 42, at 2. The subscription fees are shared with the publishers who hold the original copyrights. *Id.*

⁴⁴*Id.*

⁴⁵*Id.* at 4. Swartz registered under the false name “Gary Host” and gave his computer the client name “ghost laptop.” *Id.*

⁴⁶*Id.* at 2; *see also* MacFarquhar, *supra* note 40.

⁴⁷Superseding Indictment, *supra* note 42, at 5. JSTOR also temporarily blocked other IP addresses at MIT from having access to JSTOR. *Id.* at 6.

⁴⁸*Id.*

⁴⁹*Id.* at 7.

⁵⁰Noam Cohen, *How M.I.T. Ensnared a Hacker, Bucking a Freewheeling Culture*, N.Y. TIMES (Jan. 20, 2013), www.nytimes.com/2013/01/21/technology/how-mit-ensnared-a-hacker-bucking-a-freewheeling-culture.html?pagewanted=all.

⁵¹Motion to Suppress No. 1 at 3-5, *United States v. Swartz*, No. 11-cr-10260, Dkt. No. 59 (D. Mass. Oct. 5, 2012); *see also Two Days Before MIT and Cambridge Cops Arrested Aaron Swartz, Secret Service Took Over the Investigation*, EMPTYWHEEL (Jan. 13, 2013), www.emptywheel.net/2013/01/13/two-days-before-cambridge-cops-arrested-aaron-swartz-secret-service-took-over-the-investigation/ (arguing that under the Secret Service’s Electronic Crimes guidelines, the agency should not have been involved).

⁵²Peters, *supra* note 41; *see also* Superseding Indictment, *supra* note 61, at 8.

⁵³*See* Lessig, *supra* note 39 (“JSTOR figured ‘appropriate’ out: They declined to pursue their own action against Aaron, and they asked the government to drop it”).

⁵⁴Press Release, United States Attorney's Office for the District of Massachusetts, *Alleged Hacker Charged with Stealing Over Four Million Documents from MIT Network* (July 19, 2011), www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html.

⁵⁵*Id.*

⁵⁶*Id.*

⁵⁷MacFarquhar, *supra* note 40.

⁵⁸*Id.*

⁵⁹Lessig, *supra* note 39 (emphasis in original).

⁶⁰Alex Stamos, *The Truth About Aaron Swartz's "Crime,"* UNHANDLED EXCEPTION (Jan. 12, 2013), unhandled.com/2013/01/12/the-truth-about-aaron-swartzs-crime/.

⁶¹*EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003).

⁶²*Craigslist Inc. v. 3Taps Inc.*, No. 12-03816, 2013 WL 4447520, at *6 (N.D. Cal. Aug. 16, 2013).

⁶³*Id.* at *1.

⁶⁴*Id.* at *3–*4.

⁶⁵*Id.* at *6 n.7. Commenting on the *Craigslist* decision, Professor Kerr wrote: "IP addresses are very easily changed, and most people use the Internet from different IP addresses every day. As a result, attempting to block someone based on an IP address doesn't 'block' them except in a very temporary sense. ... Is that enough to constitute a technological barrier?" Orin Kerr, *District Court Holds That Intentionally Circumventing IP Address Ban Is "Access Without Authorization" Under the CFAA*, THE VOLOKH CONSPIRACY (Aug. 18, 2013), www.volokh.com/2013/08/18/district-court-holds-that-intentionally-circumventing-ip-address-block-is-unauthorized-access-under-the-cfaa/.

⁶⁶*Craigslist*, at *5 ("The banned user has to follow only one, clear rule: do not access the website."); *see also Southwest Airlines Co. v. Farechase, Inc.*, 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) ("repeated warnings and requests to stop scraping" in violation of website's terms of service).

⁶⁷*Craigslist*, at *7.

⁶⁸*Id.*, at *5. But some privacy tools use proxy servers to maintain anonymity online, in order to "keep your browsing invisible to the eyes of a nosy employer, ISP, or a repressive government regime," or "to unblock certain websites." *IP Rental - Anonymous Proxy & VPN IP Address Service*, www.iprental.com (last visited Sept. 22, 2013); *see also* Ingrid Lunden, *Is The #NBCFail On Olympics Coverage Giving Rise To VPN Pirates?*, TECHCRUNCH (July 31, 2012), techcrunch.com/2012/07/31/is-the-nbcfail-on-olympics-coverage-giving-rise-to-vpn-pirates/ ("an army of VPN service providers ... offer U.S. users IP addresses from other countries so that they can consume Olympic content from [U.K.] streams that are normally geo-blocked").

⁶⁹*Craigslist*, at *5.

⁷⁰*Id.* at *7–*8.

⁷¹*Id.* at *8; *see also* Granick, *supra* note 18 ("Another way to look at the CFAA, is that it protects the box").

⁷²*Craigslist*, at *8.

⁷³MacFarquhar, *supra* note 40; *see also* Jennifer Granick, *Towards Learning From Losing Aaron Swartz: Part 2*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 15, 2013, 3:54 PM), cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2 (discussing the "great practical risk" in pleading to a felony).

⁷⁴Peters, *supra* note 41; *see also* Lessig, *supra* note 39 ("[T]he

question this government needs to answer is why it was so necessary that Aaron Swartz be labeled a 'felon.' For in the 18 months of negotiations, that was what he was not willing to accept.").

⁷⁵John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html?_r=0.

⁷⁶Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, THE VOLOKH CONSPIRACY (Jan. 20, 2013, 1:10 PM), www.volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030/.

⁷⁷Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030* (Jan. 20, 2013), www.volokh.com/wp-content/uploads/2013/01/Amend-ed10302.pdf (redline of Kerr's proposed amendments against the existing language of 18 U.S. § 1030).

⁷⁸Orin Kerr, *More Thoughts on the Six CFAA Scenarios About Authorized Access vs. Unauthorized Access*, THE VOLOKH CONSPIRACY (Jan. 28, 2013, 3:40 PM), www.volokh.com/2013/01/28/more-thoughts-on-the-six-cfaa-scenarios-about-authorized-access-vs-unauthorized-access/.

⁷⁹*Id.*

⁸⁰Cindy Cohn & Marcia Hofmann, *Part 2: EFF's Additional Improvements to Aaron's Law*, DEEPLINKS BLOG (Jan. 23, 2013), www.eff.org/deeplinks/2013/01/part-2-effs-additional-improvements-aarons-law.

⁸¹*Id.*

⁸²Granick, *supra* note 20 (citing *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004)). *But see* Stewart Baker, *A Dubious Proposal for Amending the Computer Fraud and Abuse Act*, THE VOLOKH CONSPIRACY (Jan. 28, 2013, 7:07 PM), www.volokh.com/2013/01/28/a-dubious-proposal-for-amending-the-computer-fraud-and-abuse-act/.

⁸³Rep Zoe Lofgren Introduces Bipartisan Aaron's Law (last visited Sept. 23, 2013), www.lofgren.house.gov/latest-news/rep-zoe-lofgren-introduces-aarons-law-to-reform-the-cfaa.

⁸⁴*Id.*

⁸⁵Proposed "Aaron's Law Act of 2013," available at www.lofgren.house.gov/images/user_images/gt/stories/pdf/aarons%20law%20lofgren%20-%20061913.pdf.

⁸⁶*Id.* The issue of IP address blocking, however, is not addressed in the summary.

⁸⁷Section-by-Section Summary, available at www.lofgren.house.gov/images/stories/user_images/gt/stories/pdf/aarons%20law%20summary%20%20lofgren%20-%20061913.pdf.

⁸⁸Tim Wu, *Fixing the Worst Law in Technology*, THE NEW YORKER NEWS DESK (Mar. 18, 2013), www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html.

⁸⁹*See* Orin Kerr, *Recent Developments—Both in the Courts and in Congress—on the Scope of the Computer Fraud and Abuse Act*, THE VOLOKH CONSPIRACY (July 30, 2012, 11:35 PM), www.volokh.com/2012/07/30/recent-developments-both-in-the-courts-and-in-congress-on-the-scope-of-the-computer-fraud-and-abuse-act/.

⁹⁰Tony Romm, *After Activist Aaron Swartz's Death, a Tough Slog for Aaron's Law*, POLITICO (Feb. 8, 2013, 4:48 AM), www.politico.com/story/2013/02/activist-aaron-swartz-death-aarons-law-87332.html.