by James Juo

# Unauthorized Excess

## After the death of Aaron Swartz, lawmakers have proposed reforms to the Computer Fraud and Abuse Act

AT AGE 14, Aaron Swartz was working with leading technologists to craft standards for openly sharing information on the Internet.[1] 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.[2] At 19, he was a founding developer of Reddit, a widely used social news Web site where users can post news links and vote on them.[3] Aaron later became a political activist for Internet freedom and social justice issues and formed the advocacy group Demand Progress.[4] At 26, facing a criminal trial under the Computer Fraud and Abuse Act (CFAA) for allegedly circumventing computer restrictions to an online database of academic articles, Aaron Swartz hanged himself in January.[5]

Since then, Internet groups have criticized the U.S. Department of Justice for its prosecution of Swartz, although several legal commentators have noted that the CFAA had been interpreted broadly by some courts to cover similar conduct in other cases.[6] According to Jennifer Granick, the Director of Civil Liberties at the Stanford Center for Internet and Society, the CFAA has become a legal regime that as often as not is "used against whistleblowers, disloyal employees, and activists."[7] "Aaron's Law" has become a rallying cry to reform the CFAA.

The CFAA is a computer trespass statute that has been called "one of the broadest federal criminal laws currently on the books."[8] Prohibited conduct under the CFAA includes theft of computer data, unauthorized access with intent to defraud, unauthorized access resulting in destruction, trafficking in computer passwords, and extortion by threat of damage to a computer.[9] In addition to traditional computer hacking, the statute also has been asserted against employees who take trade secrets stored on their employer's computer before leaving to join the competition.[10] In 1984, Congress enacted the CFAA to criminalize the hacking of computers in connection with national security, financial records, and government property.[11] The statute was originally designed to cover unauthorized access of such protected computers having a specified federal interest.[12]

The CFAA has been expanded a number of times.[13] For example, a 1994 amendment expanded the statute to allow private entities to assert a civil cause of action and obtain compensatory damages and other equitable relief.[14] In 1996, the CFAA was further amended to expand the class of protected computers to include any computer "used in interstate or foreign commerce or communication."[15] In the space of a dozen years, the scope of this criminal statute has gone from a limited set of protected computers to possibly every computer in the United States connected to the Internet.[16]

### Without or Exceeding Authorization

The CFAA prohibits "access without authorization" and "exceed[ing] authorized access" to a protected computer.[17] But the CFAA has been called "remarkably vague" on this point.[18] What does it mean to access a computer without authorization or to exceed authorized

**James Juo is a partner at Fulwider Patton LLP, a Los Angeles law firm specializing in intellectual property, including patents and trademarks.**

HADI FARAHANI

access? Exactly what makes one person's access authorized and another's unauthorized (or exceeded) has been the subject of much litigation. Such conduct has been alleged to include exploiting code-based security flaws,[19] launching a denial of service attack on a Web site,[20] "spoofing" IP addresses to avoid access restrictions,[21] accessing information stored on an employer's computer for a competing business,[22] allowing an unauthorized person to use the valid password of another,[23] and violating a Web site's terms of service.[24]

Should the question of authorization be focused on the means used to obtain the data (e.g., whether the defendant is alleged to have broken into the computer system), or should it further look to whether the obtained data was used improperly? Under the latter approach, if a disloyal employee were to access commercial information on the employer's computer for any purpose other than that authorized by his or her job, there could be liability under the CFAA. In recent years, many plaintiffs have used the CFAA to federalize cases that otherwise would have been treated as traditional trade secret cases but for the involvement of a computer.[25] Some recent court decisions, however, have adopted a narrower interpretation, so whether such a plaintiff would be successful may depend on which courthouse hears the case.

In *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit relied on the agency relationship between an employee and employer to determine whether access was authorized.[26] The defendant, Citrin, decided to start his own business in competition with his employer, International Airport Centers (IAC). Before leaving, Citrin used a secure-erase program that permanently erased all the data (presumably including evidence of his allegedly improper conduct) on a laptop provided to him by IAC.[27] Citrin "knew the company had no duplicates of [the destroyed data]."[28]

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.[29] "[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."[30] This interpretation of access under the CFAA—finding liability for violations of corporate computer use restrictions or violations of a duty of loyalty—was adopted by the Fifth and Eleventh Circuits as well.[31]

Some district courts, however, have observed that the CFAA should be construed narrowly because it is a criminal statute, while others have adopted the broad analysis of *Citrin*.[32] The Ninth Circuit's recent decisions in *LVRC Holdings LLC v. Brekka*[33] and *United States v. Nosal*,[34] however, appear to be moving toward a narrower interpretation that does not criminalize violations of private use-based restrictions.

In *LVRC Holdings LLC v. Brekka*, the defendant was an employee who, as part of his job, had computer access to information regarding LVRC's addiction treatment business, including financial statements, budgets, and other reports.[35] Brekka traveled between his Florida home and Nevada for work and e-mailed LVRC business documents to his and his wife's personal e-mail accounts. LVRC and Brekka did not have a written employment agreement, and LVRC had no employee guidelines that would have prohibited employees from e-mailing LVRC documents to personal computers. After Brekka left the company, LVRC became concerned that Brekka had e-mailed LVRC documents to himself to further his own interests rather than those of LVRC.[36]

The Ninth Circuit expressly rejected *Citrin*'s broad interpretation of the CFAA, noting that nothing in the plain language of the statute suggests that liability for accessing a computer without authorization turns on whether the defendant breached a duty of loyalty to an employer.[37] Brekka was authorized to use LVRC's computers while he was employed at LVRC, so he did not access a computer "without authorization" under the CFAA when he e-mailed documents to himself prior to leaving LVRC.[38] "Nor did emailing the documents 'exceed authorized access,' because Brekka was entitled to obtain the documents."[39] The court further noted the rule of lenity, which requires courts to limit the reach of criminal statutes to their plain meaning and to construe any ambiguity against the government in order to avoid imposing unexpected burdens on the defendant.[40]

### *Nosal*

In *United States v. Nosal*, Nosal was a high-level employee at executive search firm Korn /Ferry International. When Nosal decided to leave, he signed an agreement to continue working for Korn/Ferry as an independent contractor in order to complete several ongoing projects, and he agreed not to compete against Korn/Ferry for one year.[41] 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 that 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 that 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."[42]

Relying on *Brekka*, the district court dismissed the CFAA claim because Nosal had permission to access the Korn/Ferry computers.[43] The district court also relied on the rule of lenity to interpret the CFAA narrowly.[44] A three-judge panel of the Ninth Circuit reversed the district court on appeal.[45] Distinguishing the earlier *Brekka* decision in which the defendant "had unfettered access to the company computer," the panel noted that Korn/Ferry had "clear and conspicuous restrictions" on an employee's computer access.[46] The panel held that "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."[47]

The Ninth Circuit reheard *Nosal* en banc and reversed the panel decision and affirmed the district court.[48] Writing for the majority, Chief Judge Alex Kozinski gave a litany of hypothetical examples of adverse consequences that may arise from giving the force of criminal law to a private party's computer use policies. Numerous dating Web sites, for instance, have terms of service that "prohibit inaccurate or misleading information." 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."[49]

Moreover, because a Web site's terms of service or an employer's policies may change at any time with little or no prior notice, what was lawful conduct one day could become unlawful the next.[50] The court suggested that the CFAA would be unconstitutionally vague if violating a Web site's terms of service (which typically are written to give the Web site's owner a broad right to cancel accounts without liability) could be construed to be unauthorized or to have exceeded authorized access under the CFAA.[51]

The tendency of a mind to "wander" and people to "procrastinate" by connecting to the Internet at work for a nonwork purpose "would make criminals of large groups of people who would have little reason to suspect they are committing a federal crime."[52] For other improper conduct involving a computer, laws such as wire fraud, trade secret, or contract law may apply instead.[53] 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*."[54]

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,[55] but a circuit split remains between *Nosal* and *Citrin*.

### The Facts of the Swartz Case

Aaron Swartz once wrote, "Stealing is wrong. But downloading isn't stealing."[56] In 2008, Swartz wrote a computer program that rapidly downloaded millions of pages of court filings from PACER after a pilot program was started to allow free access to PACER.[57] Swartz's downloads were then made freely accessible on the servers at public.resource.org.[58] Shortly thereafter, the government ended the pilot project of free access for PACER.[59] The FBI investigated Swartz but closed its file in 2009.[60]

About a year later, Swartz allegedly attempted to access and rapidly download a large numbet of academic articles from JSTOR, a nonprofit that provides a searchable database of digitized articles archived from over 1,000 academic journals.[61] Libraries and universities pay a subscription fee fot access to JSTOR's collection of digitized journals.[62] JSTOR's terms of service prohibit downloading or exporting documents from JSTOR using automated computer programs.[63] JSTOR also uses technical measures to prevent automated downloading.[64]

Swartz allegedly used a laptop connected to the computer network of the Massachusetts Institute of Technology (MIT), a JSTOR subscriber, to access JSTOR.[65] (MIT has a very permissive computer culture, and its network is open and available to anyone on campus. Anyone on the MIT campus could have access to JSTOR.[66]) In response to Swartz's rapid downloading of JSTOR articles, JSTOR blocked the Internet Protocol (IP) address for MIT that had been assigned to Swartz's laptop. Swartz then established a new IP address on the MIT network to sidestep JSTOR's block.[67] JSTOR complained to MIT about this, 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.[68] Swartz avoided MIT's block by changing (or spoofing) his laptop's MAC address.[69]

The cat-and-mouse game continued about two weeks until Swartz physically plugged his laptop directly into MIT's computer network in an unlocked wiring closet located in a basement on MIT's campus.[70] There, he allegedly continued to download articles from JSTOR. MIT traced the location of the laptop in the closet and decided to treat the downloading as a ctiminal matter. Local police were called and were joined by a Secret Service agent, who recommended installing a surveillance camera.[71] In early January, the camera allegedly recorded Swartz (with his face obscured by a bicycle helmet) entering the wiring closet and removing the laptop.[72] Later that day, he was arrested. JSTOR declined to pursue legal action against Swartz aftet he turned over his hard drives, which contained 4.8 million JSTOR documents.[73] In July 2011, however, a federal indictment charging Swartz with violations of the CFAA was unsealed in the U.S. District Court for the District of Massachusetts.[74] He was accused of violating JSTOR's use policies and circumventing JSTOR's and MIT's technical restrictions. A press release by the U.S. Attotney's Office stated that Swartz "faces up to 35 years in prison, to be followed by three years of supervised release, restitution, forfeiture and a fine of up to $1 million."[75]

Later, Carmen M. Ortiz, the U.S. Attorney overseeing the case, stated that "stealing is stealing, whether you use a computer command or a crowbar, and whether you take documents, data or dollars."[76] It has been reported that the government asserted the documents downloaded from JSTOR were worth $2 million.[77] The downloaded documents apparently included publications such as the 1942 edition of the *Journal of Botany*.[78] As Lessig argued, "[A]nyone who says that there is money to be made in a stash of ACADEMIC ARTICLES is either an idiot or a liar."[79]

A computer expert for the defense asserts that Swartz did not hack JSTOR under any reasonable definition—Swartz 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.[80] It is unclear whether this defense would have been successful, even with the recent case law developments in the Ninth and Fourth Circuits. The CFAA prohibits more than just traditional hacking, and Swartz may have found himself on the wrong side of the circuit split.

The Swartz case was pending in the District of Massachusetts, and the First Circuit previously had taken a broad interpretation of the CFAA in a case in which the plaintiff had sought to prevent a competitor from using an automated computer program (referred to as a scraper) that would download the contents of its public Web site to create a competing travel service.[81] Although the Fitst Circuit would not infer a prohibition under the CFAA against automated access, the circuit did state in dicta that explicit restrictions set forth on a public Web site's terms of service could be enforced under the CFAA.[82] Thus, a Massachusetts court may not have followed *Nosal*'s narrow interpretation of the CFAA, which would have excluded terms-of-service violations. Swartz was offered a plea bargain requiring a felony conviction, under which the government would recommend a prison term (although his defense counsel could argue to the judge for probation instead).[83] Faced with the government's demand for jail time, Aaron Swartz took his own life in January.[84]

### Aaron's Law

In the wake of Swartz's death, there have been several proposals to amend the CFAA. These proposed amendments have been referred to as Aaron's Law.

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."[85] Kerr also proposed that "access without authorization" mean "to circumvent technological access barriers to a computer or data without the express or implied permission of the owner or operator of the computer."[86] Kerr later posted a series of scenarios in an attempt to help identify what should be the proper line between authorized and unauthorized access to a computer.[87] The scenarios include examples of circumventing cookie-based restrictions and CAPTCHA gates.[88]

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."[89] The EFF wants to avoid penalizing "people who have permission to access data but use light technical workarounds to access that data."[90] Language in the EFF proposal appears to be borrowed from the anticircumvention provisions of the Digital Millennium Copyright Act, 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" and would not be given the force of law.[91] This appears intended to exempt IP and MAC address spoofing and similar forms of technological circumvention that Swartz was accused of committing.[92] The EFF also has a link on its Web site encouraging people to take action to amend the CFAA.[93]

Representative Zoe Lofgren has posted a draft bill, christened as "Aaron's Law," to revise the CFAA.[94] A revised draft of the bill eliminates the "exceeds authorized access" language from the statute and adds a more detailed definition of "access without authorization."[95] The revised draft states:

> "[A]ccess without authorization"—(A) means (i) to obtain or alter information on a protected computer; (ii) that the accesser lacks authorization to obtain or alter; and (iii) by circumventing one or more technological measures that exclude or prevent unauthorized individuals from obtaining or altering that information; and (B) does not include the following, either in themselves or in combination—(i) a violation of an agreement, policy, duty, or contractual obligation regarding Internet or computer use, such as an acceptable use policy or terms of service agreement with an online service provider, Internet website, or employer; or (ii) efforts to prevent personal identification of a computer user, or identification of a user's hardware device or software, through a user's real name, personally identifiable information, or software program or hardware device identifier(s).[96]

In March, a group of Internet companies and organizations signed a letter to the House Subcommittee on Crime, Terrorism, and Homeland Security in support of the efforts led by Lofgren to reform the CFAA.[97]

Even with the bipartisan support of Representative Darrell Issa and Senator Ron Wyden, the fate of these proposals is uncertain.[98] As Tim Wu, a professor at Columbia Law School, has observed, "Congress rarely scales back criminal laws."[99] Moreover, proposals to narrow the scope of a criminal statute often include provisions for increased penalties.[100] According to Lofgren, the effort to pass Aaron's Law "will likely take substantial time and require sustained and intense support."[101] Time will tell whether Aaron's Law will become law. ■

---

[1] Tim Carmody, *Memory to Myth: Tracing Aaron Swartz through the 21st Century*, THE VERGE (Jan. 22, 2013), http://www.theverge.com/2013/1/22/389858/aaron-swartz-profile-memory-to-myth.

[2] Lawrence Lessig, *Prosecutor as Bully*, LESSIG BLOG, v2 (Jan. 12, 2013), http://lessig.tumblr.com/post/40347463044/prosecutor-as-bully [hereinafter Lessig].

[3] Larissa MacFarquhar, *Requiem for a Dream*, THE NEW YORKER (Mar. 11, 2013), http://nyr.kr/ZUnMMv [hereinafter MacFarquhar].

[4] *See* DEMAND PROGRESS, http://www.demandprogress.org/ (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), http://slate.me/YevwGC [hereinafter Peters].

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

[6] *See, e.g.*, Orin Kerr, *The Criminal Charges against Aaron Swartz (Part 1: The Law)*, THE VOLOKH CONSPIRACY (Jan. 14, 2013), http://www.volokh.com/2013/01/14/aaron-swartz-charges; Jennifer Granick, *With the CFAA, Law and Justice Are Not the Same: A Response to Orin Kerr*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 14, 2013), https://cyberlaw.stanford.edu/blog/2013/01/cfaa-law-and-justice-are-not-same-response-orin-kerr.

[7] Jennifer Granick, *Towards Learning from Losing Aaron Swartz*, THE CENTER FOR INTERNET AND SOCIETY (Jan. 14, 2013), https://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz [hereinafter Granick, *Learning*].

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

[9] 18 U.S.C. §1030.

[10] *See* Incorp Servs. Inc. v. Incsmart.Biz Inc., No. 11-4660, 2012 WL 3685994, at *4 (N.D. Cal. Aug. 24, 2012); American Family Mut. Ins. Co. v. Rickman, 554 F. Supp. 2d 766, 771 (2008).

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

[12] Matthew Kapitanyan, *Beyond WarGames: How the Computer Fraud and Abuse Act Should Be Interpreted in the Employment Context*, 7 I/S: J.L. & POL'Y FOR THE INFO. SOC'Y 405, 410 (Winter 2012).

[13] Kerr, *supra* note 11, at 1566.

[14] *Id.* (citing 18 U.S.C. §1030(g)).

[15] *Id.* at 1567–68 (citing 18 U.S.C. §1030(c)(2)).

[16] *Id.* at 1571.

[17] *See* 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), https://cyberlaw.stanford.edu/blog/2013/01/rthoughts-orin-kerrs-cfaa-reform-proposals-great-second-step [hereinafter Granick, *Thoughts*] ("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.").

[18] *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), *available at* http://www.volokh.com/wp-content/uploads/2013/03/KerrCFAATestimony2013.pdf.

[19] *See, e.g.*, United States v. Morris, 928 F. 2d 504, 505 (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 (2000) (hacking a dating service Web site and diverting its users to a porn site).

[20] *See, 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 amount of e-mail at a specific address).

[21] *See, 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.").

[22] *See, 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).

[23] *See, e.g.*, State Analysis, Inc. v. American Fin. Servs., 621 F. Supp. 2d 309, 316 (E.D. Va. 2009) ("KSE accessed StateScape's Web site using usernames and passwords that did not belong to it.").

[24] *See, e.g.*, America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1260 (N.D. Iowa 2000) (violating AOL's terms of service to send bulk e-mail).

[25] *See, e.g.*, Chas. S. Winner, Inc. v. Polistina, 2007 WL 1652292, at *2, (D. N.J. June 4, 2007) ("Absent diversity jurisdiction, a case of this kind sounds in state statutory and common law and is heard in state court.").

[26] International Airport Ctrs., L.L.C. v. Citrin, 440 F. 3d 418 (7th Cir. 2006).

[27] *Id.* at 419-20.

[28] *Id.* at 421.

[29] *Id.*; *see also* Shurgard Storage Ctrs., Inc. v. Safeguard

Self Storage, Inc., 119 F. Supp. 2d 1121, 1125 (W.E. Wash. 2000) (cited and relied upon by *Citrin*).

[30] Citrin, 440 F. 3d at 421.

[31] United States v. John, 597 F. 3d 263, 273 (5th Cir. 2010) (bank employee accessed customer accounts for the 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 used an SSA database for personal reasons).

[32] *Compare* ViChip Corp. v. Lee, 438 F. Supp. 2d 1087, 1100 (N.D. Cal. 2006) (following *Citrin*'s broad interpretation of CFAA) *with* United States v. Drew, 259 F.R.D. 449, 467 (C.D. Cal. 2009) (noting that a broad interpretation of the CFAA would result in a "standardless sweep").

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

[34] United States v. Nosal, 676 F. 3d 854 (9th Cir. 2012) (en banc).

[35] Brekka, 581 F. 3d at 1129-30.

[36] *Id.*

[37] *Id.* at 1134.

[38] *Id.* at 1135.

[39] *Id.* at 1129.

[40] *Id.* at 1134; *see also* Warren Thomas, *Lenity on Me:* LVRC Holdings LLC v. Brekka *Points the Way toward Defining Authorization and Solving the Split over the Computer Fraud and Abuse Act*, 27 GA. ST. U. L. REV. 379, 400 (2011).

[41] United States v. Nosal, 676 F. 3d 854, 856 (9th Cir. 2012) (en banc).

[42] *Id.* at 856 n.1.

[43] United States v. Nosal, No. 08-0237, 2010 WL 934257, at *7 (N.D. Cal. Jan. 6, 2010), *rev'd*, 642 F. 3d 781 (9th Cir. 2011), *rev'd en banc*, 676 F. 3d 854 (9th Cir. 2012).

[44] *Id.*

[45] United States v. Nosal, 642 F. 3d 781, 789 (2011), *rev'd en banc*, 676 F. 3d 854 (2012).

[46] *Id.* at 787. ("Because LVRC had not notified Brekka of any restrictions on his access to the computer, Brekka had no way to know whether—or when—his access would have become unauthorized.") *Id.*

[47] *Id.* at 788. *But see id.* at 790 (Campbell, J., dissenting).

[48] United States v. Nosal, 676 F. 3d 854, 863-64 (2012) (en banc).

[49] *Id.* at 861-62.

[50] *Id.* at 862.

[51] *Id.*; *see also* United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009) (finding the CFAA did not apply to violations of a Web site's terms of service).

[52] Nosal, 676 F. 3d at 859-60.

[53] *Id.* at 863.

[54] *Id.* at 864. In a jury trial after the remand, Nosal was found guilty of violating the CFAA because he used a borrowed password to access Korn/Ferry's computer database. *See* Vanessa Blum, *Nosal Found Guilty in Trade Secret Case*, THE RECORDER (Apr. 24, 2013), http://www.law.com/jsp/ca/PubArticleCA.jsp?id=202597433473. Nosal's attorneys vowed to appeal the verdict. *Id.*

[55] *See* WEC Carolina Energy Solutions LLC v. Miller, 687 F. 3d 199, 203 (2012); Dana Ltd. v. American Axle & Mfg. Holdings, Inc., No. 10-450, 2012 WL 2524008, at *4-5 (W.D. Mich. June 29, 2012); Wentworth-Douglass Hosp. v. Young & Novus Prof'l Assoc., No. 10-120, 2012 WL 2522963, at *3-4 (D. Conn. June 29, 2012); JBCHoldings NY, LLC v. Pakter, No. 12-7555, 2013 WL 1149061, at *5 (S.D. N.Y. Mar. 20, 2013).

[56] *See* http://www.aaronsw.com/weblog/001112.

[57] John Schwartz, *An Effort to Upgrade a Court Archive System to Free and Easy*, N.Y. TIMES, Feb. 12, 2009, http://www.nytimes.com/2009/02/13/us/13records.html?_r=0 [hereinafter Schwartz].

[58] Ryan Singel, *FBI Investigated Coder for Liberating Paywalled Court Records*, WIRED (Oct. 5, 2009), http://www.wired.com/threatlevel/2009/10/swartz-fbi [hereinafter Singel].

[59] Schwartz, *supra* note 57. The RECAP add-on for the Firefox browser now allows users to automatically save paid-for court filings downloaded from PACER onto a public server that can later be accessed for free by other RECAP users. Singel, *supra* note 58.

[60] *Id.*, *see also* Aaron Swartz, *Wanted by the FBI*, RAW THOUGHT (Oct. 5, 2009), http://www.aaronsw.com/weblog/fbifile.

[61] Superseding Indictment at 1, United States v. Swartz, No. 11-cr-10260, Dkt. No. 53 (D. Mass. Sept. 12, 2012).

[62] *Id.* at 2. The subscription fees are shared with the publishers who hold the original copyrights. *Id.*

[63] *Id.*

[64] *Id.*

[65] *Id.* at 4. (Swartz registered under the name "Gary Host" and gave his computer the client name "ghost laptop.") *Id.*

[66] *Id.* at 2; *see also* MacFarquhar, *supra* note 3.

[67] Superseding Indictment, *supra* note 60, at 5. JSTOR also temporarily blocked other IP addresses at MIT. *Id.* at 6.

[68] *Id.*

[69] *Id.* at 7.

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

[71] Motion 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), http://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).

[72] Peters, *supra* note 4; *see also* Superseding Indictment, *supra* note 60, at 8.

[73] *See* Lessig, *supra* note 2.

[74] Press 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), http://www.justice.gov/usao/ma/news/2011/July/SwartzAaronPR.html [hereinafter Press Release].

[75] *Id. See also* Steven Musil, *U.S. Attorney Defends Office's Conduct in Aaron Swartz Case*, CNET (Jan. 16, 2013), http://news.cnet.com/8301-1023_3-57564414-93/u.s-attorney-defends-offices-conduct-in-aaron-swartz-case/.

[76] Press Release, *supra* note 74.

[77] MacFarquhar, *supra* note 3.

[78] *Id.*

[79] Lessig, *supra* note 2 (emphasis in original).

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

[81] *See* EF Cultural Travel BV v. Zefer Corp., 318 F. 3d 58 (1st Cir. 2003) (EF Cultural II); EF Cultural Travel BV v. Explorica, Inc., 274 F. 3d 577 (1st Cir. 2001) (EF Cultural I).

[82] EF Cultural II, 318 F. 3d at 63.

[83] MacFarquhar, *supra* note 3; *see also* Jennifer Granick, *Towards Learning from Losing Aaron Swartz: Part 2*, The Center for Internet and Society (Jan. 15, 2013), https://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz-part-2. (discussing the great practical risk in pleading to a felony)

[84] Peters, *supra* note 4; *see also* Lessig, *supra* note 2 ("[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.").

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

[86] Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, THE VOLOKH CONSPIRACY (Jan. 20, 2013), http://www.volokh.com/wp-content/uploads/2013/01/Amended10302.pdf.

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

[88] *Id.*

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

[90] *Id.*

[91] Granick, *Thoughts*, *supra* note 17 (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), http://www.volokh.com/2013/01/28/a-dubious-proposal-for-amending-the-computer-fraud-and-abuse-act/.

[92] Cohn & Hofmann, *supra* note 89; *see also* EFF, Explanation of Effects of Aaron's Law with EFF Proposed Amendments to "Access Without Authorization" (Jan. 23, 2013), https://www.eff.org/sites/default/files/Explanation%20of%20Aaron%E2%80%99s%20law%20with%20EFF%20access%20amendments.pdf (public discussion draft).

[93] EFF.org, *The Computer Fraud and Abuse Act Is Broken. Tell Congress to Fix It*, https://action.eff.org/o/9042/p/dia/action/public/?action_KEY=9005.

[94] Adam Clark Estes, *The Congressional Backlash over Aaron Swartz's Suicide Has Begun*, THE ATLANTIC WIRE (Jan. 15, 2013), http://www.theatlanticwire.com/politics/2013/01/congressional-backlash-over-aaron-swartzs-suicide-has-begun/61048/.

[95] Discussion Draft, http://lofgren.house.gov/images/stories/pdf/aarons%20law%20revised%20draft%20013013.pdf.

[96] *Id.*; *see also* Orin Kerr, *Drafting Problems with the Second Version of "Aaron's Law" from Rep. Lofgren*, THE VOLOKH CONSPIRACY (Feb. 2, 2013), http://www.volokh.com/2013/02/02/drafting-problems-with-the-second-version-of-aarons-law-from-rep-lofgren.

[97] *See* Mark M. Jaycox, *Startups and Innovators Send Letter to Congress Demanding CFAA Reform*, DEEPLINKS BLOG (Mar. 12, 2013), https://www.eff.org/deeplinks/2013/03/startups-and-innovators-send-letter-congress-demanding-cfaa-reform.

[98] Tony Romm, *After Activist Aaron Swartz's Death, a Tough Slog for Aaron's Law*, POLITICO (Feb. 8, 2013), http://politi.co/XVjnau [hereinafrer Romm].

[99] Tim Wu, *Fixing the Worst Law in Technology*, THE NEW YORKER NEWS DESK (Mar. 18, 2013), http://nyr.kr/YCubsS.

[100] *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), http://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.

[101] Romm, *supra* note 98.