Florida Law Review

Volume 67 | Issue 5

Article 7

March 2016

Recent Development: Craigslist and the CFAA: The Untold Story

Clark S. Splichal

Recommended Citation

Clark S. Splichal, *Recent Development: Craigslist and the CFAA: The Untold Story*, 67 Fla. L. Rev. 1845 (2016).
Available at: http://scholarship.law.ufl.edu/flr/vol67/iss5/7

RECENT DEVELOPMENT: CRAIGSLIST AND THE CFAA: THE UNTOLD STORY

Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013)
Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178 (N.D. Cal. 2013)

Clark S. Splichal[*]

INTRODUCTION 1845

I. EVOLUTION AND APPLICATION OF THE COMPUTER FRAUD AND ABUSE ACT IN THE INTERNET CONTEXT 1848

II. *CRAIGSLIST INC. V. 3TAPS INC.*: HOW THE NORTHERN DISTRICT OF CALIFORNIA GOT IT WRONG AND WHY THIS MATTERS 1854

III. THE STATUTORY SAFE HARBOR 1858

CONCLUSION 1860

INTRODUCTION

There is one area in which Craigslist Inc. appears particularly invested these days: its legal bills. Notoriously cutthroat, this online classified marketplace has steadfastly clung to its bare-boned business blueprint while resisting any form of growth or innovation over the years.[1] Craigslist has not, however, shied away from taking on its would-be competitors in court, oftentimes those attempting only to "add[] a layer

[*] First, a very special thanks to the talented and dedicated editorial staff of the *Florida Law Review* for the thoughtful work they have done to improve this piece, and to Trace Jackson and Marla Spector for making this possible. I would also like to thank Professor Dennis Calfee for guiding me through the dark times and for being my conscience and confidante, always. And finally, to my incredible parents, for their blind, unquestioning support, to my former roommate and friend Michael Polatsek, for paying the rent on time, and to my lovely wife Deborah, for tolerating this madness much longer than I thought possible. All rights reserved; all wrongs revenged.

[1] *See* Keith Patrick, *How Craigslist Makes Money*, HOUS. CHRON., http://smallbusiness.chron.com/craigslist-money-27287.html (last visited June 27, 2015) (noting that Craigslist is considering other revenue streams while remaining hesitant due to fears of taking away "from the quality of the site"); *see also* Gary Wolf, *Why Craigslist Is Such a Mess*, WIRED (Aug. 24, 2009), http://archive.wired.com/entertainment/theweb/magazine/17-09/ff_craigslist ("Besides offering nearly all of its features for free, it scorns advertising, refuses investment, ignores design, and does not innovate. Ordinarily, a company that showed such complete disdain for the normal rules of business would be vulnerable to competition, but [C]raigslist has no serious rivals. The glory of the site is its size and its price.").

of value" to the Craigslist formula.[2] Not surprisingly, Craigslist's arsenal of litigation weapons has become quite vast in recent years: claims arising under the Copyright Act, the Lanham Act, and the Computer Fraud and Abuse Act (CFAA), as well as claims of unjust enrichment, conspiracy, and even trespass to chattel,[3] all aimed at scrappy upstarts sporting a fraction of Craigslist's resources. Many of these rival companies have employed "web scrapers" to aggregate publicly available data on Craigslist's servers and then repackage or otherwise make available this content for third-party users.[4] In some cases, this activity clearly constitutes misappropriation or theft, but generalizing these companies' motives is tricky. Very often these competing companies appear to be simply trying to enhance and augment the Craigslist model, which is a desirable result in a free and unfettered market.

Several recent court orders in the U.S. District Court for the Northern District of California signal a major early victory for Craigslist over these web scrapers and data aggregators, even though much of the early media attention has centered on where Craigslist's lawsuit fell short: the copyright infringement claims.[5] Indeed, what was lost on many mainstream commentators (but certainly not legal bloggers[6]) is that the

[2] Mike Masnick, *Craigslist's Abuse of Copyright and the CFAA to Attack Websites That Make Craigslist Better Is a Disgrace*, TECHDIRT (May 1, 2013, 9:29 AM), http://www.techdirt.com/ articles/20130501/04342822905/craigslists-abuse-copyright-cfaa-to-attack-websites-that-make-craigslist-better-is-disgrace.shtml; *see* Dani Fankhauser, *Why the Web Hasn't Birthed a Prettier Craigslist*, MASHABLE (Feb. 17, 2013), http://mashable.com/2013/02/17/prettier-craigslist ("The site certainly has the funds to hire top-notch interaction designers to build a superior product, as the original Craigslist must have been for users in 1995. But instead, it focuses resources on fighting for legal domination over competitors.").

[3] *See, e.g.*, Complaint at 8–15, Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962 (N.D. Cal. 2013) (No. CV-12-3816).

[4] *See* Craigslist Inc., 942 F. Supp. 2d at 966. ("Craigslist alleges that 3Taps copies (or 'scrapes') all content posted to Craigslist in real time, directly from the Craigslist website. 3Taps markets [an Application Programming Interface] to allow third parties to access large amounts of content from Craigslist . . . ." (citations omitted)).

[5] *E.g.*, Derek Khanna, *Craigslist's Allegations of "Copyright" Violations Thrown Out*, FORBES (Apr. 30, 2013, 7:17 PM), http://www.forbes.com/sites/derekkhanna/2013/04/30/craigslists-allegations-of-copyright-violations-thrown-out.

[6] *See, e.g.*, Eric Goldman, *Craigslist's Anti-Consumer Lawsuit Threatens to Break Internet Law*, FORBES (May 23, 2013, 11:50 AM), http://www.forbes.com/sites/ericgoldman/2013 /05/23/craigslists-anti-consumer-lawsuit-threatens-to-break-internet-law; *see also* Jam Kotenko, *Padmapper and 3Taps Win Copyright Case Against Craigslist, but the Battle Isn't Over*, DIGITAL TRENDS (May 1, 2013), http://www.digitaltrends.com/web/padmapper-wins-copyright-case-against-craigslist-but-still-faces-other-claims/#!IxRnz (noting that, even after the rulings on copyright infringement, an apartment listing site and its data collector and provider still faced potential charges based on the CFAA); Adi Robertson, *Craigslist Lawsuit Ruling Says Evading an IP Address Block Can Violate Anti-Hacking Laws*, VERGE (Aug. 19, 2013, 11:27 AM), http://www.theverge.com/2013/8/19/4636154/craigslist-ruling-says-evading-ip-address-block-violates-cfaa (focusing on the CFAA claims).

Craigslist Inc. v. 3Taps Inc. orders continue to perpetuate the absurd application of the CFAA to online "intrusion," specifically to Craigslist's competitors' web scraping activities. The April and August 2013 orders on the defendants' motions to dismiss found these activities actionable under the CFAA,[7] which is alarming because the scraped data in question was available on freely accessible, public websites. Moreover, these orders subvert a recent decision from the U.S. Court of Appeals for the Ninth Circuit, *United States v. Nosal*,[8] which had narrowed the application of the CFAA and its use as a weapon of private enforcement against web scrapers and other data aggregators.[9] In brief, *Nosal* stands for the proposition that users' violations of a website's "Terms of Use" (TOU) could not alone form the basis of CFAA liability.[10] The *Nosal* case is significant because it seemingly halted the runaway train that the CFAA had become in California. Further, it marked a departure from other circuits by offering a lean, sensible interpretation of the CFAA's thorniest provision: what activities constitute "unauthorized access." However, the *Craigslist* orders still leave open questions about whether *Nosal* was the great panacea that it first appeared to be, or if it managed to change anything at all.

While there are causes of action that ought to be (and are) available to plaintiffs wishing to guard against unwanted intrusion, CFAA civil actions should not be among them. This cause of action is poorly suited to address complex property issues in the digital age, and it may simultaneously chill web innovation and foster anticompetitive behavior in the market. While it is unclear whether the Northern District of California will ever reach the merits in *Craigslist*, these early decisions suggest that the court may have misapplied *Nosal*, or may be poised to misapply it in the future. While *Nosal* seemed to take a forward step in squaring the circle—particularly with regard to the CFAA's more troubling provisions—the Northern District's misguided application of the CFAA post-*Nosal* illustrates deeper infirmities within the CFAA. Indeed, courts cannot and should not stretch the CFAA to cover unanticipated and uncontemplated forms of technology, and in this regard the CFAA is ripe for a simple statutory fix. A CFAA "safe harbor" of sorts, borrowed from language found in a related statute, would help modernize a statute that has, over time, swept within its ambit a new class of unintended defendants.

[7] *See Craigslist*, 942 F. Supp. 2d at 970 (April 2013 order granting in part and denying in part motions to dismiss); Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1180 (N.D. Cal. 2013) (August 2013 order denying motion to dismiss CFAA count).

[8] 676 F.3d 854 (9th Cir. 2012).

[9] *Id.* at 863.

[10] *See id.*

Part I of this Comment begins by tracking the CFAA's evolution in the Ninth Circuit as applied in the internet realm. Part II examines the *Nosal* decision and whether the court properly applied it in *Craigslist*. Part II also examines the implications for web start-ups seeking to exploit existing, publicly available data if the Northern District eventually holds against 3Taps Inc. at trial or on summary judgment. Finally, Part III proposes a statutory solution that creates a safe harbor within the CFAA for users accessing public computer systems, effectively removing these defendants from the purview of the CFAA. This Comment focuses on developments principally in the Ninth Circuit, as California web companies are perhaps most poised to litigate these types of issues.

I. EVOLUTION AND APPLICATION OF THE COMPUTER FRAUD AND ABUSE ACT IN THE INTERNET CONTEXT

Congress enacted the CFAA[11] in 1986 with the goal of protecting "a vast array of property that, in many cases, is wholly unprotected against crime" given the vast "proliferation of computers and computer data."[12] Primarily a criminal statute targeting computer hackers, the CFAA also provides for a civil cause of action for "[a]ny person who suffers damage or loss by reason of a violation of this section" for compensatory damages and injunctive relief.[13] Congress appeared animated by a desire to prevent theft and misappropriation of guarded data, but also that untrammeled access onto another's computer system itself posed a serious independent threat.[14]

Most CFAA private causes of action turn on the operation of 18 U.S.C. § 1030(a)(4), the statute's key provision: "Whoever . . . knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access . . . shall be punished."[15] The statute somewhat circularly defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[16] The statute, however, does not clarify the meaning of "unauthorized access." These ambiguities and omissions have prompted

[11] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030 (2012)).

[12] S. REP. NO. 99-432, at 2 (1986) [hereinafter Senate Report]; *see also* Robert D. Sowell, Comment, *Misuse of Information Under the Computer Fraud and Abuse Act: On What Side of the Circuit Split will the Second and Third Circuits Wind Up?*, 66 FLA. L. REV. 1747, 1747–49 (2014) (providing background on the legislative history of the CFAA).

[13] 18 U.S.C. § 1030(g) (2012).

[14] *See* Senate Report*, supra* note 12, at 10 ("Mere trespasses onto someone else's computer system can cost the system provider a 'port' or access channel that he might otherwise be making available for a fee to an authorized user.").

[15] 18 U.S.C. § 1030(a)(4) (2012).

[16] *Id.* § 1030(e)(6).

much debate among academics and the courts.[17]

Over time, due to the transformation of the technological landscape, courts have applied the CFAA more frequently in the internet realm and further outside the strict "hacking" context. Indeed, with the addition of the civil cause of action in 1994, the CFAA has morphed into an expansive right of private enforcement against all forms of digital intrusion.[18] A number of cases in the Ninth Circuit illustrate the CFAA's expansive reach. This Comment spotlights the following cases because their facts are the most similar to the web scraping activity at issue in *Craigslist Inc. v. 3Taps Inc.* Further, many of these cases examine issues of first impression, as they involve nascent and novel technologies employed to either access or extract data from web servers.[19] At the outset, note that many of these cases never proceeded past either the Rule 12(b)(6)[20] or summary judgment stage, likely due to disparities in resources between plaintiffs and defendants. Although there is a lack of decisions on the ultimate merits of these claims, these preliminary orders still shed considerable light on California courts' approach to CFAA claims.

In 2007, the U.S. District Court for the Central District of California granted Ticketmaster LLC's motion for a preliminary injunction against RMG Technologies premised on various federal and state law claims.[21] Defendant RMG employed a web scraping-like technology known as the "Ticket Broker Acquisition Tool" (TBAT), which Ticketmaster alleged was an "automatic device[]" prohibited by the site's TOU.[22] Website TOUs typically take the form of "'browsewrap' licenses, in which the user does not see the contract at all but in which the license terms provide that using a Web site constitutes agreement to a contract."[23] Put differently, a website user may at times implicitly assent to the site's TOU without having read it. Courts are still divided, however, on whether

[17] *E.g.*, Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1554–55 (2012) ("Over the past decade, three distinct approaches have emerged for how to interpret and apply what it means to access a computer without, or in excess of, authorization: (1) the contract-based approach; (2) the agency-based approach; and (3) the code-based approach.").

[18] *See* Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677, 693–94 (2009).

[19] As this Comment argues, this is a fundamental problem with applying the CFAA to these types of actions. *See infra* Part II.

[20] FED. R. CIV. P. 12(b)(6) (failure to state a claim).

[21] Ticketmaster LLC v. RMG Techs., Inc., 507 F. Supp. 2d 1096, 1102 (C.D. Cal. 2007) (order granting a preliminary injunction). The plaintiff brought the motion for preliminary injunction based on five claims, including a CFAA claim. *Id.* While the CFAA claim failed because it did not meet the monetary damage threshold, the court granted the motion for preliminary injunction on the basis of the plaintiff's remaining claims. *Id.* at 1113.

[22] *Id.* at 1102–03.

[23] Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 460 (2006).

TOUs are enforceable when lacking some affirmative action on the part of the user.[24]

Ticketmaster claimed that the defendant's automated tool not only violated its TOU, but also allowed the defendant to bypass the site's CAPTCHA[25] and flood the site with unwanted queries.[26] While the court's analysis of the plaintiff's CFAA claim is scant, the court suggests that the facts alleged were sufficient to maintain an "unauthorized access" claim under § 1030(a)(4).[27] The court stated, "It appears likely that Plaintiff will be able to prove that Defendant gained unauthorized access to, and/or exceeded authorized access to, Plaintiff's protected computers" based on the TBAT's culling reams of data via automatic search queries.[28] In other words, based on a preliminary sketch of the facts, it appears that the court was satisfied that the defendant's conduct—violating Ticketmaster's TOU and skirting the CAPTCHA checkpoint—constituted actionable "unauthorized access" under § 1030(a)(4).

Two years later, eBay Inc. brought CFAA and RICO[29] claims against a number of defendants, alleging that they engaged in an elaborate "cookie stuffing" scheme to fraudulently redirect advertising revenue to themselves.[30] In essence, the scheme involved displacing legitimate cookies used to track user behavior and "revenue actions" on eBay's site with fraudulent cookies crediting the defendants for any user revenue action.[31] Much like web scraping, the activity in question appeared to involve user proxies,[32] was to a degree automated, and entailed otherwise

[24] *Compare* Cairo, Inc. v. Crossmedia Servs., Inc., No. C 04-04825 JW, 2005 WL 756610, at *5 (N.D. Cal. Apr. 1, 2005) (holding that the site's TOU was binding in this case, where the defendant had actual or imputed knowledge of the plaintiff's terms when using the website), *with* Specht v. Netscape Commc'ns Corp., 150 F. Supp. 2d 585, 596 (S.D.N.Y. 2001) (holding that "browse-wrap" licenses did not "provide adequate notice either that a contract is being created or that the [TOU] will bind the user").

[25] "A CAPTCHA is a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot." *CAPTCHA: Telling Humans and Computers Apart Automatically*, CAPTCHA, http://www.captcha.net (last visited June 27, 2015).

[26] *Ticketmaster*, 507 F. Supp. 2d at 1102–03.

[27] *Id.* at 1113. However, since Ticketmaster alleged no facts showing that it had suffered at least $5000 of harm (as required under § 1030(a)(4)), the court ultimately denied the motion. *Id.*

[28] *Id.*

[29] Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961–68 (2012).

[30] eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1160 (N.D. Cal. 2009).

[31] *Id.*

[32] According to the complaint, "While the exact method used by Defendants is unknown, eBay surmises that Defendants first placed software code on a web user's computer surreptitiously, without the user's knowledge. The software code then directed the user's browser to eBay's website, without the user's knowledge or any affirmative action on the part of the user." (paraphrasing the complaint) *Id.* (citation omitted).

permitted access.[33] Defendant Digital Point Solutions launched into a refrain common among CFAA defendants: The plaintiff's website was not a "protected computer" within the meaning of the CFAA, and no "unauthorized access" occurred because "eBay is a *public* website that may be accessed by anyone."[34] eBay countered that such access and use of the site were outside the scope of eBay's TOU, and the defendant's "only purpose [in accessing the site] was to defraud eBay."[35] The court appeared satisfied with eBay's "purpose" argument and saved the CFAA claim from the defendant's 12(b)(6) motion.[36]

A year later, Craigslist brought suit in the Northern District of California against Naturemarket, Inc., a company in the business of selling automated ad posting software.[37] According to the defendant, its software "makes the difficult Craigslist posting process child's play and helps you manage and multi-post your ads."[38] Predictably, Craigslist was none too pleased. Craigslist argued that the defendant's software facilitated automated access that both violated the site's TOU and circumvented the site's CAPTCHA software.[39] The court held that these facts as alleged were sufficient to maintain the CFAA claim.[40]

Apart from the differences in the precise technologies employed to "access" the plaintiffs' websites, these cases have one thing in common: violating a site's TOU appeared to per se constitute "unauthorized access" or activity "exceeding authorized access" under the first prong of § 1030(a)(4). Whether these TOUs bound users in a legally significant way apart from § 1030 appeared largely beside the point.

This all changed when the Ninth Circuit finally weighed in on the precise effect of the phrases "unauthorized access" and "exceeds unauthorized access" in CFAA civil claims. Before the pivotal *United States v. Nosal*, the Ninth Circuit first had occasion in *LVRC Holdings LLC v. Brekka*[41] to engage in a "plain language" analysis of the CFAA's operative provisions.[42] The problem was seemingly that there was a fraught distinction between "access" and "use," where parties (and

[33] *Id.*

[34] *Id.* at 1164 (emphasis added).

[35] *Id.*

[36] *Id.*

[37] Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1048–49 (N.D. Cal. 2010).

[38] *Id.* at 1049 (quoting Answer at 14, *Naturemarket, Inc.*, 694 F. Supp. 2d 1039 (No. CV 08-5065 PJH)) (internal quotation marks omitted).

[39] *Id.* at 1050.

[40] *Id.* at 1057.

[41] 581 F.3d 1127 (9th Cir. 2009).

[42] *Id.* at 1132.

courts) had consistently conflated the latter with the former.[43] In *Brekka*, the defendant accessed his employer's computer system, and then saved and transmitted the data.[44] Once his employer terminated his employment, the defendant continued to access his employer's site.[45] The court declined to find that one who *uses* information freely accessed on a computer system contrary to its owner's best interest has "exceeded authorized access" within the meaning of § 1030(a)(4). Regarding the statute's plain meaning, the court explained:

> This leads to a sensible interpretation of §§ 1030(a)(2) and (4), which gives effect to both the phrase "without authorization" and the phrase "exceeds authorized access": a person who "intentionally accesses a computer without authorization" accesses a computer without any permission at all, while a person who "exceeds authorized access" has permission to access the computer, but accesses information on the computer that the person is not entitled to access.[46]

In other words, the court held that it was legally insignificant under the CFAA whether the employee, with access freely given, put the information gathered to some nefarious end, or similarly, possessed a disloyal state of mind while freely accessing his employer's computer.[47] Ultimately, the court held that the defendant did not violate the CFAA either before or after his term of employment.[48] *Brekka* is important because it was the first case in California to constrain what had been an expansive reading of § 1030(a)(4), and though it addressed rather broadly a company policy restricting or placing limits on computer access, it did not explicitly address TOUs.

United States v. Nosal[49] finally closed that gap. In *Nosal*, the court reinforced *Brekka*'s interpretation of §§ 1030(a)(4) and (6) and waxed expansive about the sheer absurdity that would result from adopting the contract-based approach to CFAA liability[50]—i.e., treating breaches of sites' TOUs as per se "unauthorized access," which had ruled the day in the Ninth Circuit. Put simply, similar to an employer's policy of granting broad computer access but restricting certain uses, a site's TOU could *not*

[43] *See id.* at 1133 (explaining that "[i]t is the employer's decision to allow or to terminate an employee's authorization . . . that determines whether the employee is with or 'without authorization'").

[44] *Id.* at 1130.

[45] *Id.*

[46] *Id.* at 1133 (citations omitted).

[47] *See id.* (holding that the mental state of the user who lacked authorization is an unpersuasive interpretation of §§ 1030(a)(2) and (4)).

[48] *Id.* at 1137.

[49] 676 F.3d 854 (9th Cir. 2012).

[50] *Id.* at 861–62.

serve as an actual limitation on access if the website otherwise freely gave access to users.[51] Reinforcing the "plain meaning" principle articulated in *Brekka*, the court held that restrictions on "use" must not be conflated with "access" for purposes of determining CFAA liability.[52]

The court then illustrated a series of scenarios where to hold otherwise would result in an unacceptable expansion of criminal and civil liability under the CFAA.[53] The court arguably takes this riff reductio ad absurdum, but the basic point is clear: "Our access to [websites] is governed by a series of private agreements and policies that most people are only dimly aware of and virtually no one reads or understands"—a nod perhaps to the line of cases that declined to recognize enforceable agreements by way of TOUs as a separate matter.[54] Since most websites' TOUs deal with restrictions on *use* of the website and proprietary data hosted therein, "[i]f Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly."[55] Though the court made a sweeping policy appeal, its reasoning was grounded in a well-trod principle: the plain meaning of "unauthorized access" does not and cannot contemplate a website's imposed restrictions on *use*.

Several cases have followed *Nosal* and applied this more exacting standard based on the tighter interpretation of § 1030(a)(4).[56] The newfangled standard necessarily requires a more fact-intensive inquiry—no longer would violations of a website's TOU automatically trigger liability under the CFAA. Removing TOUs from the equation, the court must now determine, among other things, whether and by what means the website blocked or restricted access;[57] whether the website granted access for certain areas of a site or database but not others; and whether a would-be intruder's "purpose" in accessing a site is relevant at all. The *Nosal* case is notable for not listing any types of affirmative steps a website could take to block access that it otherwise freely gives, and as a result,

[51] *Id.* at 862–63.

[52] *Id.* at 863.

[53] *See id.* at 860–63 (discussing issues of TOU breaches regarding Facebook, eHarmony, and MySpace that did not result in violations of the CFAA).

[54] *Id.* at 861.

[55] *Id.* at 863.

[56] *E.g.*, Farmers Ins. Exch. v. Steele Ins. Agency, Inc., No. 2:13-cv-00784-MCE-DAD, 2013 WL 3872950, at *20 (E.D. Cal. July 25, 2013) (granting motion to dismiss on other grounds, but finding that plaintiff had alleged sufficient facts to show defendant had "exceeded authorized access" by using others' login credentials to access computer for which his access was restricted).

[57] One case decided between *Brekka* and *Noral* suggested that only "technical barriers" could effectively restrict access, the circumvention of which would constitute "unauthorized access." Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *12 (N.D. Cal. 2010).

the contours of the doctrine prior to *Craigslist Inc. v. 3Tap Inc.* were still rather blurred.

II. *CRAIGSLIST INC. V. 3TAPS INC.*: HOW THE NORTHERN DISTRICT OF CALIFORNIA GOT IT WRONG AND WHY THIS MATTERS

While the litigation is ongoing, a few preliminary decisions from the Northern District of California in the *Craigslist Inc. v. 3Taps Inc.* controversy have arguably set the tenor and tone should the case eventually reach trial or a summary judgment motion. In *Craigslist*, the three named defendants engaged in the practice of "scraping" Craigslist's servers for user-generated listings that they would then repackage for other third parties to use.[58] Web scraping—also known as "screen scraping" or "web harvesting"—commonly utilizes software to copy data from websites in bulk via an automated process, in effect bypassing the time limitations a single user would encounter when extracting and copying such data.[59] In *Craigslist*, defendants Padmapper, 3Taps, and Lovely each employed web scraping processes to extract and republish ad listings from Craigslist's website.[60]

Craigslist responded by sending multiple cease-and-desist letters to the defendants, as well as by engaging "IP blockers" to selectively bar access from defendants' computers.[61] The court ultimately found that, even in light of *Norsal*, Craigslist had alleged facts that were sufficient to withstand a 12(b)(6) motion.[62]

A few things are troubling about the court's reasoning. First, when addressing TOUs in the April 2013 *Craigslist* order, the court announced that "[t]he relationship between a website's terms of use and the CFAA is somewhat unclear in light of *Nosal*."[63] The court suggests that *Nosal* makes an assumption that TOUs will necessarily involve restrictions on use *only*,[64] which may very well be a correct reading of the case. Admittedly, *Nosal* does not draw a clear line between its indictment of TOUs and the "use/access" distinction on which its ultimate opinion rested, but it is a fair inference that, by definition website TOUs deal only with *use*. However, reading *Nosal* one gets a sense that, all "plain meaning" aside, the court desired to lay to rest the notion that contractual

[58] Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 966 (N.D. Cal. 2013).

[59] *See What Is Web Scraping?*, WEBHARVY, https://www.webharvy.com/articles/what-is-web-scraping.html (last visited June 27, 2015) (website offering web scraping software); *see also* Zachary Levine, *FAQS*, 12 E-COMMERCE L. REP., no. 10, at 18 (2010) (defining web scraping as "a form of data mining where a program, or person, scours the web making copies of data found on target Web sites").

[60] *Craigslist*, 942 F. Supp. 2d at 966.

[61] *Id.* at 969.

[62] *See id.* at 969–70.

[63] *Id.* at 968.

[64] *Id.* at 969.

liability could work as a stand-in for CFAA liability. Indeed, maybe *Nosal* is clearer than people think; and further, maybe a repudiation of the contract-based approach to the CFAA coincides with the Ninth Circuit's plain-meaning interpretation of "unauthorized access." The line from *Craigslist* is ultimately a throwaway, but it highlights courts' continued confusion over CFAA doctrine. Until a court is faced with website TOUs that purport to restrict *access*, the matter will remain unsettled.

The August 2013 *Craigslist* order is perhaps more illuminating on these points and suggests that the use/access comparison may ultimately be a distinction without a difference. Here, the court artfully distinguished *Nosal* from the instant case by explaining that the former clearly involved restrictions on use, while the latter involved revoking access by way of technological barriers and cease-and-desist letters.[65] 3Taps responded that this characterization (as was common in pre-*Nosal* decisions) conflates access with use, and that Craigslist's measures to block access were thinly-veiled use restrictions after all—Craigslist banned access for certain users based solely on how those users would put the scraped data to use.[66] While the court rejected this argument, it may pay to take heed because it raises an important question: Do not all access restrictions become use restrictions when dealing with data from a website that grants broad access to the public at large? In other words, in this environment, are not access restrictions applied to specific users *necessarily* to prevent certain types of uses? Otherwise, why discriminate among users when *all* users enjoy full access by default?

Secondly, the court gives legal significance to the cease-and-desist letters Craigslist sent the defendants.[67] The court is right to point out that there are conflicting holdings in the Northern District regarding whether defiance of a cease-and-desist letter—where permission to access a site is affirmatively withheld—constitutes unauthorized access.[68] The court is wrong, however, to take the position that per *Nosal*, technological or otherwise physical barriers are no different from softer barriers, such as a cease-and-desist letter or a contractual provision. This betrays the spirit of *Nosal*, which subscribed to the canon of lenity in interpreting the

[65] Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1184 (N.D. Cal. 2013).

[66] *Id.* at 1184–85.

[67] *See* Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969–70 (N.D. Cal. 2013).

[68] *Compare* Facebook, Inc. v. Power Ventures, Inc., No. C 08-05780 JW, 2010 WL 3291750, at *10 (N.D. Cal. July 20, 2010) (finding that cease and deist letters do not abrogate permission for the purposes of the CFAA), *with* Weingand v. Harland Fin. Solutions, Inc., No. C 11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (holding that the CFAA applies to all restrictions on access).

CFAA, a *criminal* statute first and foremost.[69] Therefore, an interpretation that would result in citizens having "fair notice of the criminal laws . . . [and] Congress hav[ing] fair notice of what conduct its laws criminalize" necessarily must exclude TOUs or other "soft" measures to restrict access within the meaning of the CFAA.[70] To echo the Ninth Circuit in *Nosal*, if Congress wished to include violations of cease-and-desist letters in the definition of "exceeds authorized access," then it should have done so. At least one commentator has weighed in, noting that it would indeed be unprecedented to give these "unregulated wish lists" such sweeping legal effect.[71]

Finally, the plaintiff's utilization of IP blockers poses a thornier problem. These measures more closely resemble the "physical" technological barriers to access, whose circumvention the court suggested would constitute unauthorized access under the CFAA. However, far from the bulwark that Craigslist and the court seem to ascribe to IP blockers, these barriers often amount to a mere "No Trespassing" sign, offering little or no protection against unwanted intrusion.[72] Both orders suggest that circumvention of a technological barrier would constitute "unauthorized access," and such a rule seems sensible. But, as several commentators have pointed out, it is not readily clear that IP address blockers present such a "barrier," and the Northern District shirked from this analysis.[73] Unlike a more conventional barrier (such as data encryption or passwords), users can easily avoid IP address blockers by either changing the IP address or simply accessing the Internet from a different computer.[74] In this sense, an IP blocker works as a technological barrier only "in the very short term but not in the long

[69] *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (discussing issues of TOU breaches regarding YouTube, eHarmony, and MySpace that did not result in violations of the CFAA).

[70] *Id.* at 863.

[71] Eric Goldman, *Craigslist Wins Routine but Troubling Online Trespass to Chattels Ruling in 3Taps Case (Catch-up Post)*, TECH. & MKTG. L. BLOG (Sept. 20, 2013), http://blog.ericgoldman.org/archives/2013/09/craigslist_wins_1.htm ("This is one of the reasons why I favor threats actions, so that senders of overclaiming C&D letters feel some legal risk before they pop off. Because C&D letters are effectively unregulated wish lists, it's troubling to see courts treat them as relevant to the legal conclusion.").

[72] *See* Steven J. Vaughan-Nichols, *US Court Rules Masking IP Address to Access Blocked Website Violates Law*, ZDNET (Aug. 21, 2013, 9:30 PM), http://www.zdnet.com/us-court-rules-masking-ip-address-to-access-blocked-website-violates-law-7000019701.

[73] *See* Orin Kerr, *District Court Holds That Intentionally Circumventing IP Address Ban Is "Access Without Authorization" Under the CFAA*, VOLOKH CONSPIRACY (Aug. 18, 2013, 7:40 PM), http://www.volokh.com/2013/08/18/district-court-holds-that-intentionally-circumventing-ip-address-block-is-unauthorized-access-under-the-cfaa; Vaughan-Nichols, *supra* note 72.

[74] *See* Kerr, *supra* note 73.

term,"[75] and would seem to share more in common with the softer cease and desist letter or TOU provision in this regard—a measure more symbolic than functional, perhaps evincing a website's intent[76] to ban access without effectively doing so. This begs the question of whether *any* type of technological barrier could effectively ban access in a web environment that is so pervasively "open" to begin with.

The apparent follies in the court's reasoning are less evidence of a misapplication of *Nosal* and more a symptom of the doctrinal mess that the CFAA has become in California. The *Craigslist* decisions illustrate that *Nosal*'s rejiggering of the "without authorization" standard, while producing some clarity, has left lower courts with (1) a use/access distinction that is conceptually fraught, especially in the public website context; (2) little guidance as to which types of technological barriers whose circumvention would trigger CFAA liability; and (3) whether TOUs may ever impose access restrictions, and if so, whether this could be reconciled with *Nosal*'s holding regarding TOU violations. Simply, the CFAA is not well-adapted for this type of interpretative jerry-rigging.

It is time that Congress revisit the CFAA in light of new changes in the technological landscape and developments in "cyberculture." Courts must not be continually tasked (and taxed) with adapting old doctrine to emerging trends in technology, which results in unpredictable and inconsistent outcomes. The court's decision may have only postponed the doomsday scenario the *Nosal* court described—visions of unchecked CFAA liability in a digital world governed by obscure, one-sided TOUs. A statutory solution is required to prevent websites from using the CFAA to snuff out their competitors. When evaluating 3Taps's argument that *public* websites cannot effectively revoke authorization, the court suggested that there comes a point where the court's interpretation of § 1030 breaks down and it must defer to the plain meaning of the text: "Congress apparently knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public vs. nonpublic distinction—but § 1030(a)(2)(c) contains no such restrictions or modifiers."[77] Indeed, until the statute explicitly exempts from the scope

[75] *Id.*

[76] While it is outside the scope of this analysis, Professor Orin Kerr makes an interesting observation regarding the August 2013 *Craigslist* order:

> So whatever unauthorized access means, the person must be guilty of doing that thing (the act of unauthorized access) intentionally to trigger the statute. Judge [Charles] Breyer seems to mix up those elements by focusing heavily on the fact that 3taps knew that Craigslist didn't want 3taps to access its site. According to Judge Breyer, the clear notice meant that the case before him didn't raise all the notice and vagueness issues that prompted the Ninth Circuit's decision in *Nosal*.

Id.

[77] Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1182–83 (N.D. Cal. 2013).

of liability information on websites freely accessible and open to the public, this will continue to be a losing argument for defendants.

III. THE STATUTORY SAFE HARBOR

Before addressing a proper statutory fix that would reduce the CFAA's use as an expansive right of private enforcement, a brief comparison to the Digital Millennium Copyright Act (DMCA)[78] might be instructive. In 1998, Congress enacted the DMCA with the objective of "facilitat[ing] the robust development and worldwide expansion of electronic commerce, communications, research, development, and education . . . . [while adapting the current law] in order to make digital networks safe places to disseminate and exploit copyrighted materials."[79] Consistent with this goal as well as in order to foster new creation and growth of internet industries, Congress felt it necessary to free online service providers from the litigious grip that content owners might impose on them, especially when third parties conducted infringing activity.[80] What followed was the creation of four statutory "safe harbors,"[81] which were aimed at exempting from liability certain activities that had erstwhile been actionable under common law theories of secondary copyright infringement. In sum, the DMCA safe harbors attempted to adapt the law to the realities of the market and new developments in technology. Technology had simply outpaced these common law doctrines, and Congress recognized that courts could no longer reliably stretch doctrine to cover unanticipated changes in technology (namely, the Internet as a medium for copying and transmitting copyrighted content).

Similarly, the CFAA is due for a safe harbor of its own given the "current broad reach of the CFAA . . . [that] impacts . . . innovation, competition, and the general 'openness' of the internet."[82] The CFAA did not envisage the Internet as it exists currently, where users may freely connect with a multitude of servers—which themselves are connected with other servers—and where the notion of "access" lacks any real significance. The legislative history of the CFAA reveals a core preoccupation with the protection of "computer systems" generally *not*

[78] Pub. L. No. 105-304, 112 Stat. 2860 (1998) (codified as amended in scattered sections of 5, 17, 28, 35 U.S.C.).

[79] S. REP. NO. 105-190, at *1–2 (1998).

[80] *See* Liliana Chang, Recent Development, *The Red Flag Test for Apparent Knowledge Under the DMCA § 512(c) Safe Harbor*, 28 CARDOZO ARTS & ENT. L.J. 195, 198 (2010).

[81] The four DMCA safe harbors cover the following categories of material: (1) digital transmissions, (2) temporary system caching, (3) content residing on a system or network at the user's direction, and (4) information location tools. 17 U.S.C. § 512(a)–(d) (2012).

[82] *Craigslist*, 964 F. Supp. 2d at 1187 (citing Reply Brief for Defendant at 15, *Craigslist*, 964 F. Supp. 2d 1178 (No. CV-12-03816 CRB)).

open to public[83] (this was 1986, after all). However, as *Craigslist* points out, the CFAA does draw a distinction between public and nonpublic systems and information housed therein, but this distinction was not based on an understanding of "public" as people now understand and experience the Internet. Thus, it seems clear that the CFAA considered treating different categories of information differently for purposes of establishing CFAA liability; it seems equally clear that had the drafters understood the intrinsically open character of the Internet as it exists today, they would have likely limited or restricted liability when it came to *access*—authorized or not.

In its reply brief, 3Taps draws the court's attention to such a limitation found in the Stored Communications Act (SCA):[84] "It shall not be unlawful under this [law] for any person to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is *readily accessible to the general public*."[85] 3Taps proposed that, due to the striking, policy-based similarities between the CFAA and SCA, the court should import this limitation into the CFAA.[86] Not surprisingly, the court declined such an invitation, but the implications are clear. Congress should amend the CFAA to include this general limitation on liability, and it should thus read: "It shall not be unlawful for any person to access data housed on a computer system where such system is readily accessible to the general public." At present, the CFAA portends of "a permission-based regime for public websites" where permission freely given could be instantly revoked, with or without notice, upon the whimsy or caprice of public websites.[87] Such a safe harbor would once and for all restrict liability for user activity in the web environment, including the web scraping and data aggregation at issue in *Craigslist*.

There are undoubtedly instances where the means employed to cull data for public websites would legitimately impede or interfere with the target computer system, and there are certainly defendants who would not readily fit the "brave innovator" mold that commentators have ascribed to companies such as 3Taps and Padmapper. However, ample causes of action exist—from copyright infringement to unfair competition—for website owners to properly respond to less scrupulous activity. But the CFAA should, once and for all, be cast from plaintiffs' arsenal.

[83] *See* Senate Report, *supra* note 12, at 3.

[84] 18 U.S.C. §§ 2701–2712 (2012).

[85] 18 U.S.C. § 2511(2)(g)(i) (2012) (emphasis added).

[86] *Craigslist*, 964 F. Supp. 2d at 1183.

[87] *Id.* at 1184 (quoting Defendant's Supplemental Briefing re: Motion to Dismiss Causes of Action Nos. 13 & 14 in Plaintiff's First Amended Complaint at 13, *Craigslist*, 964 F. Supp. 2d 1178 (No. CV-12-03816 CRB)).

CONCLUSION

While it remains uncertain how the Northern District of California will handle the § 1030 issue on the merits,[88] the early signs weigh heavily in Craigslist's favor. It is likely that the parties will draw out litigation to the extent that 3Taps and others' resources are depleted and the case ultimately settles. Until there is legislative intervention, parties will continue to engage in pitched battles over application and construction of the CFAA—a statute that has outlived its usefulness and demands strained interpretations to reach activity that it obviously never contemplated.

[88] On October 1, 2013, the court referred the case to a federal magistrate judge for discovery. Since then, the matter remains in the discovery phase, with the last filing on the docket occurring on March 19, 2015. *Craigslist*, 964 F. Supp. 2d 1178 (No. 3:12-CV-03816).