PERKINS COIE LLP
BOBBIE WILSON (No. 148317)
bwilson@perkinscoie.com
BRIAN P. HENNESSY (No. 226721)
bhennessy@perkinscoie.com
J. PATRICK CORRIGAN (No. 240859)
pcorrigan@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304
Telephone: 650.838.4300
Facsimile: 650.838.4350

Attorneys for Plaintiff
craigslist, Inc.

Additional Counsel Listed on Next Page

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CRAIGSLIST, INC., a Delaware corporation,

Plaintiff,

v.

3TAPS, INC., a Delaware corporation; PADMAPPER, INC., a Delaware corporation; DISCOVER HOME NETWORK, INC., a Delaware corporation d/b/a LOVELY; BRIAN R. NIESSEN, an individual; and Does 1 through 25, inclusive,

Defendants.

Case No. CV 12-03816 CRB

PLAINTIFF CRAIGSLIST, INC.'S OPPOSITION TO RENEWED MOTION TO DISMISS; RESPONSE TO BRIEF BY AMICI CURIE

PERKINS COIE LLP
CHRISTOPHER KAO (No. 237716)
ckao@perkinscoie.com
3150 Porter Drive
Palo Alto, CA 94304
Telephone: 650.838.4300
Facsimile: 650.838.4350

PERKINS COIE LLP
GERALDINE M. ALEXIS (No. 213341)
galexis@perkinscoie.com
Four Embarcadero Center, Suite 2400
San Francisco, CA 94111
Telephone: 415.344.7000
Facsimile: 415.344.7050

Attorneys for Plaintiff
craigslist, Inc.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

LEGISLATIVE MATERIALS

SUMMARY OF ARGUMENT

The Court should deny the renewed motion to dismiss:

- The unambiguous text of the CFAA protects *all* computers and *all information* on those computers. 18 U.S.C. § 1030(a)(2)(C). There are no limitations for computers connected to the Internet, "public websites," or anything else. To the contrary, Congress did explicitly place such limitations in portions of the statute not implicated here, which means the limitations do not exist in the portions of the statute that are at issue here. *See* Part A.1., A.2., *infra*.
- The one in-district case to have considered whether access is always "authorized" under the CFAA if a computer is connected to the Internet via a "public website" rejected that argument. *See eBay, Inc. v. Digital Point Solutions, Inc.,* 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009). *See* Part B.1., *infra*.
- The out-of-district cases 3taps relies on— *Pulte Homes, Inc. v. Laborer's International Union of North America*, *Cvent, Inc. v. Eventbrite, Inc.*, and *Koch Industries, Inc. v. Does, 1-25*— stand for the proposition that a computer owner's failure to take affirmative steps to revoke authorization and / or restrict access may preclude a CFAA claim. Even if this is the standard, craigslist meets it because it (1) blocked 3taps' IP addresses, (2) unambiguously informed 3taps in writing that its access was unauthorized and told 3taps to stop, and (3) filed this lawsuit. *See* Part B.2., *infra*.
- The entire purpose of the CFAA is to provide computer owners with the same private property protections as the law of trespass. *See, e.g.,* 131 Cong. Rec. S11,872 (daily ed. Sept. 20, 1985) (describing the conduct proscribed as "akin to a trespass onto someone else's real property"). *See* Part B.3., *infra*.
- Upholding craigslist's CFAA claim would be a very narrow ruling confirming that craigslist did not give up all its rights under the CFAA by connecting its computers to the Internet. *See* Part C., *infra*.

INTRODUCTION

3taps has nothing to do with an average Internet user that views the craigslist website, and should not liken itself or its conduct to such a user, or try to speak on behalf of the same. 3taps is an admitted scraper that mass-harvests user postings for redistribution to, and misuse by, parasitical businesses. 3taps would have the Court believe its conduct is harmless. The opposite is true.

Consider a craigslist user who posts an ad on craigslist to rent her house, including her email, home address, and telephone number. She finds a tenant, edits her ad to say the house is rented, and goes on vacation. Strangely, she continues to receive emails and phone calls, and people are knocking on her new tenant's door to view the rental property. Unbeknownst to her, 3taps scraped her original ad from craigslist without her consent and redistributed it to other classified sites, which continue to advertise her house for rent. She contacts craigslist angrily demanding an explanation.

Or consider one of craigslist's largest paying customers that values craigslist for connecting it with strictly local job applicants. Suddenly it starts receiving unwanted responses from all over the world because, without its knowledge or consent, 3taps is pirating its job ads to non-local job sites. In addition, one of these sites exposes the customer's email address and phone number to voluminous spam and unwanted calls from its marketing partners, which the customer, unaware of what 3taps has done, assumes must be craigslist-related. The customer concludes that craigslist lost its local focus and its respect for customer privacy and discontinues posting, depriving craigslist users of a prime source of job openings, and craigslist of one of its best paying customers.

Or take another craigslist user, recently divorced, who places an ad in the "personals" section of craigslist. It includes his picture, name, email, height, weight, profession, and age, along with his personal and romantic interests. He finds someone nice and is happily dating. He deletes his ad, but his new girlfriend sees it listed on two other sites, courtesy of 3taps. He insists he didn't place ads on those sites. She finds this hard to believe and breaks up with him.

When a user places an ad in a specific category of a local craigslist site, he or she expects it to be seen exclusively by local craigslist users visiting that category of the craigslist site, and subject to the edit, deletion, and other self-publishing tools craigslist provides. He or she does not expect the ad to be hijacked without permission and repurposed at the whim of parasitical businesses. Congress understood the need for venue operators online, just as in the physical world, to ban harmful and destructive persons from their premises. The CFAA provides website owners like craigslist an indispensable tool for protecting users, and ensuring the venues and services they provide those users are not debased by unauthorized intruders.

Subsection (a)(2)(C) of the CFAA (the "Scraping Provision") bars unauthorized access to "a computer" to obtain "information." There are no modifiers for the type of computer or the type of information protected. Indeed, Congress specifically chose *not to* impose any limitations on the Scraping Provision, as evidenced by other parts of the statute that *do* impose limitations on the types of computers and information protected. Subsection (a)(3), for example, only protects *nonpublic* United States government computers. Congress added "nonpublic" to that section in the very same amendment that it added the Scraping Provision to the statute. It could have easily added "nonpublic" to the Scraping Provision like it did in subsection (a)(3), but specifically chose not to. Likewise, subsection (a)(2)(A) only protects certain types of financial information. Congress chose not to impose any similar limitations in the Scraping Provision.

3taps ignores all of this and asks the Court to judicially impose into the CFAA fanciful concepts like "public data," "public websites," and "data commons" that appear nowhere in the statute. Its argument boils down to this: craigslist connected its computers to the Internet and did not impose any "code based" restrictions on access. As a result, 3taps asserts, the entire world—including 3taps—is forever permitted under the CFAA to access craigslist's computers, scrape classified ads and other content wholesale, and exploit the content however anyone desires. This has the law and the facts all wrong.

3taps has the law wrong because there is no basis for limiting the Scraping Provision to computers with code based restrictions. Courts routinely apply the CFAA to what 3taps would

describe as a "public website." *See* Part B.1., *infra*. The one in-district case that has considered head-on whether a computer can be rendered beyond the CFAA's scope by classifying it as a "public website" rejected that argument. *See eBay, Inc. v. Digital Point Solutions, Inc.*, 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009). On the other hand, the out-of-district cases that 3taps claims have "settled" the law in its favor come nowhere close to doing that. At most, those three cases—*Pulte Homes*, *Cvent*, and *Koch*—stand for the proposition that a computer owner's failure to take affirmative steps to revoke authorization and / or restrict access may preclude a CFAA claim. In contrast to the facts in those cases however, craigslist clearly did revoke authorization and did restrict access.

Indeed, 3taps also has the facts wrong since craigslist *does impose code based restrictions* on access to its computers. craigslist blocked 3taps' access to its computers by imposing code based barriers to the IP addresses known to be associated with 3taps. 3taps repeatedly circumvented those barriers and this Court already held those allegations sufficient to state a claim under the CFAA. Even if 3taps got its way and the Court interpreted the Scraping Provision to apply only to circumvention of code based restrictions on computers connected to the Internet, its renewed motion would therefore still need to be denied.

3taps' smoke and mirrors about public sidewalks, store windows, and "internet users" aside, this case is fundamentally about private property and craigslist's right to moderate and protect its computers, website, and users. Like any property owner, craigslist is free to choose who may and who may not access and enter its computers in the same way that a landowner is free to make the same choices about his real property. The CFAA places no limits on those choices for the same reason that the law of trespass places no limits on a landowner's ability to exclude. In fact, the CFAA's history shows that Congress intended it to apply the same protections to privately owned computers that the law of trespass affords to privately owned real property.

3taps' renewed motion should be denied.

BACKGROUND

Greg Kidd founded 3taps for the specific purpose of taking all of craigslist's content from its computers and redistributing it wholesale. Mr. Kidd boasts that he "baited" craigslist into filing this litigation and that he is willing to "burn some" of his shares in Twitter to fund it.[1] Mr. Kidd publicly states that "rules are for fools" (i.e. Copyright law, the CFAA, trespass law, etc., are "for fools")[2] while he encourages PadMapper, Discover Home Network, and others to republish scraped craigslist content for their own business purposes.[3]

3taps gets craigslist content by paying people to create and operate computer programs that overcome the barriers craigslist erects, and systematically harvest all the content from craigslist's computers. Pl.'s First Am. Compl., Dkt No. 35 ("FAC") ¶¶79-80. 3taps apparently could not hire legitimate Silicon Valley engineers to illegally scrape. Instead it looks offshore to the black market to people like co-defendant Brian Niessen. FAC ¶¶87-98. To the best of craigslist's knowledge, Mr. Niessen lives on a boat in the Caribbean island of Sint Maarten. In addition to scraping for 3taps, he operates a variety of dubious websites, including instantinternetpornstar.com, diaperclub.us, tampaxclub.com, and many others, some of which reside at the same IP addresses from which Mr. Niessen scrapes postings from craigslist's computers. FAC ¶¶88, 92-97. 3taps admits that Mr. Niessen is one of its scrapers. Def. 3taps' Answer to FAC, Dkt. No. 94, at ¶97.

3taps was not always been forthcoming about its scraping, however. It falsely represented to this Court in its Answer and Counterclaims filed on September 24, 2012 that it did not use scraped content. Def. 3taps' Answer to Compl. and Countercl., Dkt. No. 20, at 37, ¶50 ("3taps does not use scraping."); *id* at 15, ¶57. After craigslist filed its First Amended Complaint detailing facts showing that 3taps does scrape, and had been scraping, craigslist's computers,

---

[1] *See, e.g.*, http://www.sfgate.com/technology/article/3taps-PadMapper-face-Craigslist-challenge-3762765.php; http://www.youtube.com/watch?v=64Cv3gyvaFU at 25:35-25:48; http://allthingsd.com/20120727/3taps-is-raring-to-fight-craigslist-over-data-access/.

[2] *See, e.g.*, http://www.youtube.com/watch?v=uohApwNfqZA at 38:45.

[3] *See, e.g.*, http://www.youtube.com/watch?v=6Rf6JrSYZ4U; http://www.youtube.com/watch?v=B6cHjDEmGew&feature=youtu.be.

3taps admitted in its First Amended Counterclaim that it has been scraping craigslist's computers since August 2012—well before it filed its initial answer denying scraping. Def. 3taps' First Am. Countercl., Dkt. No. 47, at 21, ¶92 ("*[S]ince August 2012*, 3taps also has used third parties that scrape data from the craigslist website.") (emphasis added); *id*. at 7, ¶14 ("3Taps only is employing third parties to scrape craigslist's website."). These judicial admissions conclusively establish that on September 24, 2012 when 3taps denied scraping in its Answer and Counterclaims, *3taps was actively scraping and had been for at least two months*. Dkt. 47, at 21, ¶92 (scraping "since August 2012").

Discovery just began in this case, so the full nature and extent of 3taps' activities, as well as the techniques used by it and its scrapers, are not entirely clear. But this much is known:

- Since at least August 2012, 3taps has directly or through its agents accessed craigslist's servers and "scraped" all the content from those computers. FAC ¶¶79-80; Dkt. 47, at 21, ¶92.
- 3taps claims that prior to August 2012 it did not directly access craigslist's computers and scrape content, but it has never offered any support for these assertions other than vague statements about craigslist content being "publicly available." *Id.* at 2, ¶¶6-7.
- On March 7, 2012, craigslist notified 3taps by letter that its access to craigslist's computers was not authorized and demanded that it stop scraping craigslist and stop accessing craigslist's computers altogether. FAC ¶132.
- After 3taps refused to stop accessing craigslist's computers and harvesting information from them, craigslist identified the IP addresses from which 3taps was operating and blocked those IP addresses from accessing craigslist's computers. *Id*. at ¶81.
- Once craigslist would block a 3taps IP address, 3taps (or its agents) would switch to another IP address in an effort to circumvent craigslist's defenses against it. *Id*. at ¶82.
- Eventually 3taps started using IP rotation technology that constantly switches the IP address from which access to craigslist's computers is initiated to make it even harder to identify and block 3taps intrusions.[4] *Id*. at ¶84.

[4] It is also worth noting that the legitimate search engines to which 3taps would like to compare itself (Google, Bing, etc.) are highly respectful of the rights and wishes of web site owners like craigslist, use consistent IP addresses, employ easily recognizable software agents, and make it extremely easy to opt out of being crawled and indexed. Hackers operating from the Caribbean behind anonymous proxy networks are notably absent from their approach.

After 3taps enters craigslist's computers and harvests all of the information found on them, it distributes the information to anyone that wants it. *Id*. at ¶¶3, 63-64. That includes parasitical classified advertising "innovators" and anyone else that wants to republish, data mine, or otherwise misuse the information. *Id*. at ¶¶4-6, 63, 65.

ARGUMENT

A. The Text Of The CFAA Clearly Prohibits 3taps' Conduct.

The Scraping Provision reads, in its entirety, as follows:

> (a) Whoever—
> (2) intentionally accesses a **computer** without authorization or exceeds authorized access, and thereby obtains—
> (C) **information** from any protected computer;
> shall be punished as provided in subsection (c) of this section. 18 U.S.C. § 1030(a)(2)(C) (emphasis added). [5]

That text is clear. There is no basis to conclude that it does not apply to 3taps' access to craigslist's computers.

1. The Statute Protects All Computers.

First, there are no limitations whatsoever on the type of computers protected. It applies to *all* computers, whether they are password protected, generally accessible without code based restrictions, connected to the Internet, and so on. In fact, Congress contemplated the very limitation that 3taps is trying to read into the statute—a limitation to "nonpublic" computers—*and rejected it*.

Specifically, subsection (a)(3) prohibits certain access to "nonpublic" United States government computers. 18 U.S.C. § 1030(a)(3) ("intentionally, without authorization to access any *nonpublic* computer of a department or agency") (emphasis added). By modifying computers with the word "nonpublic," Congress meant to exclude from protection "publicly available"

[5] Subsection (a)(2)(C) is not the only CFAA provision that bars scraping. Subsections (a)(4) and (a)(5) also prohibit 3taps' conduct, and craigslist's claims under these provisions also survive 3taps' motion to dismiss because 3taps' access to craigslist's computers is without authorization for the reasons discussed *infra*.

computers accessible "via an agency's World Wide Web site." S. REP. NO. 104-357, at 8 (1996). Congress chose not to do this in the Scraping Provision.

The inclusion of "nonpublic" in subsection (a)(3) and exclusion of "nonpublic" from the Scraping Provision is dispositive proof that the Scraping Provision protects both "public" and "nonpublic" computers. Congress knew exactly how to exclude from protection computers that are "publicly available" via a "World Wide Web site." S. REP. NO. 104-357, at 8. It specifically chose not to do so in the Scraping Provision.[6] *See, e.g.*, *Franklin Nat'l Bank of Franklin Square v. New York*, 347 U.S. 373, 378 (1954) (there is "no indication that Congress intended to make this phase of national banking subject to local restrictions, as it has done by express language in several other instances"); *see also Keene Corp. v. U.S.*, 508 U.S. 200, 208 (1993) ("[W]here Congress includes particular language in one section of a statute but omits it in another . . . , it is generally presumed that Congress acts intentionally and purposefully in the disparate inclusion or exclusion.") (quoting *Russello v. U.S.*, 464 U.S. 16, 23 (1983)); *King v. St. Vincent's Hosp.*, 502 U.S. 215, 220-21 (1991) ("Given the examples of affirmative limitations on reemployment benefits conferred by neighboring provisions, we infer that the simplicity of subsection (d) was deliberate . . . to provide its benefit without conditions on length of service.").

What's more, the 1996 amendment that added the Scraping Provision to the CFAA *is the exact same amendment* that modified subsection (a)(3) to limit it to "nonpublic" government computers. The negative inference that the Scraping Provision applies to *all* computers is therefore even stronger. *See Field v. Mans*, 516 U.S. 59, 75 (1995) ("The more apparently deliberate the contrast, the stronger the inference, as applied, for example, to contrasting statutory sections originally enacted simultaneously in relevant respects.") (citation omitted).

2. The Statute Protects All Information.

There are likewise no limitations on the type of information—public, private, personal, etc.—protected. Here again, "information" is not modified or qualified in the CFAA. And, here

[6] Subsections (a)(4) and (a)(5) contain no limitations on the type of computers protected for the same reasons. Congress could have modified the type of computers protected in those sections to only include "nonpublic" computers. It chose not to and no such limitation exists or applies.

again, Congress *did* include modifiers elsewhere in the statute when discussing "information." *See* 18 U.S.C. § 1030(a)(2)(A) (barring unauthorized access to a computer to obtain "information contained in a financial record . . . or of a card issuer"). It therefore specifically and intentionally chose not to place such limitations on the Scraping Provision. *See, e.g.*, *Keene Corp.*, 508 U.S. at 208; *see also* Orin S. Kerr, *Cyber Security: Protecting America's New Frontier*, U.S. House of Representatives Committee on the Judiciary Subcommittee on Crime, Terrorism and Homeland Security, at 3 (Nov. 15, 2011) ("The statute does not require that that information be valuable or private. *Any* information of *any* kind is enough."), 7 ("[T]he current version of § 1030(a)(2) is triggered when an individual obtains *any* information.").

Congress could easily have limited the CFAA so that "publically available information" was not protected by the CFAA. It chose not to.

B. Connecting A Computer To The Internet Does Not Forever Authorize The Entire World To Access It Under The CFAA.

Since the statute places no limitations on the types of computer or information protected, 3taps is left in the awkward position of arguing that the entire world is forever "authorized" under the CFAA to access a computer if it is connected to the Internet without password protection. There is no support for that.

1. The Statute And Established Case Law Defeat 3taps' Theory.

The entire premise of the CFAA is to protect *computers connected to the Internet*. In *Nosal*, for example, the Ninth Circuit concluded that "protected computer" under the statute means "effectively all computers with Internet access." *U.S. v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012); *see also Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 891-92 (N.D. Cal. 2010). According to the Ninth Circuit and the plain language of the statute, in other words, connecting a computer to the Internet does not somehow render access to that computer "authorized" under the CFAA.

That leaves 3taps drawing a distinction between computers connected to the Internet that are password protected and those that are not. The CFAA protects the ones with passwords, says

3taps, but not the ones without.[7] Dkt. 94, at 2, 4-6; *see also* Br. of Amici Curiae in Resp. to the Court's Request for Supplemental Briefing Re: Motion to Dismiss, Dkt. No. 92-1, at 8-9. That is even true, according to 3taps, if (1) the computer owner explicitly informs a user that it is not authorized to access the computer, (2) demands that all such access cease, and (3) blocks the user's access to the computer. *See id*. (computer owner not entitled to "de-authorize" access).

Yet the statutory text draws no such distinction, as explained above. *See* Parts A.1., A.2., *supra*. Bending over backward to read "without authorization" in the statute to *exclude* all situations in which a non-password protected computer is connected to the Internet would do violence to the plain, unambiguous language of the statute that applies to *all computers*. *See id*.

The weight of authority also rejects the distinction. The defendant in *eBay v. Digital Point Solutions*, for example, argued that access to the eBay website is always "authorized" under the CFAA because "eBay is a public website that may be accessed by anyone." 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009). The Court (Fogel, J.) rejected that argument and upheld eBay's CFAA claim. *Id*. at 1164; *see also Weingand v. Harland Fin. Solutions, Inc.*, No. C-11-3109 EMC, 2012 WL 2327660, at *3 (N.D. Cal. June 19, 2012) (concluding that "one need not engage in . . . rigorous technological measures to block someone from accessing files in order to limit their 'authorization'" under the CFAA and rejecting the argument that "the only 'authorization' to which the statute speaks is 'code' authorization").

eBay v. Digital Point Solutions is the only case from this district to have considered the argument that 3taps makes here. But at least one Circuit Court of Appeals has considered, and like the *eBay* Court, rejected 3taps' argument. The First Circuit in *EF Cultural Travel BV v. Zefer Corporation* refused to accept a "'presumption' of open access to Internet information."

[7]The Amici's suggestion that craigslist's ability to restrict access to its content and computers is somehow limited to "requiring a username and login" is nonsensical. Requiring users to enter a username and password to enter the site would inconvenience users, but it would not restrict access by fraudsters and interlopers such as 3taps. They could register usernames and passwords like everyone else. Were craigslist to institute a username and password requirement tomorrow, Amici would then argue that the entire world is still "authorized" to access craigslist's computers under the CFAA since everyone is able to register for an account. The best way for craigslist to block scraping of (and other unauthorized access to) its computers is to block IP addresses, which it did.

318 F.3d 58, 63 (1st Cir. 2003). The court noted that "[t]he CFAA, after all, is primarily a statute imposing limits on access and enhancing control by information providers," such as an Internet website. *Id*.

There are also myriad other cases from this district and elsewhere that, while not directly addressing the argument made here by 3taps, nevertheless uphold CFAA claims involving privately-owned, non-password protected, Internet-connected computers like craigslist's. *See, e.g.*, *Sw. Airlines v. Farechase, Inc.*, 318 F. Supp. 2d 435, 438-40 (N.D. Tex. 2004) (access to non-password protected Southwest Airlines website could be unauthorized under the CFAA); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251-53 (S.D.N.Y. 2000) (access to non-password protected www.register.com via "automated search robot" was unauthorized access under the CFAA); *Barnstormers, Inc. v. Wing Walkers, LLC*, No. EP-10-CV-261-KC, 2011 WL 1671641, at *9 (W.D. Tex. May 3, 2011) (accessing non-password protected website after website owner demanded that the access was "unauthorized access" under the CFAA); *Ticketmaster LLC v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) ("It appears likely that Plaintiff will be able to prove that Defendant gained unauthorized access to . . . Plaintiff's protected computers" connected to the Internet via the non-password protected www.ticketmaster.com).

2. The Cases Cited By 3taps Do Not Support Its Argument.

3taps hangs its hat on three out-of-district cases: (1) *Pulte Homes, Inc. v. Laborer's International Union of North America*, (2) *Cvent, Inc. v. Eventbrite, Inc.*, and (3) *Koch Industries, Inc. v. Does, 1-25*. Dkt. 94, at p 4-5. None of these cases even addressed the clear statutory language, which imposes a "nonpublic" limitation in an unrelated part of the statute, but not in the Scraping Provision. At most, these cases stand for the proposition that access under the CFAA is not "unauthorized" unless the computer owner takes affirmative steps to block access or put the violator on notice that his access is unauthorized. Even were this the law—and there are serious doubts about that given the plain language of the statute and the authority discussed above—it does not advance 3taps' cause at all. craigslist *did* use code based restrictions to block 3taps'

access. It also provided written notice that 3taps was not authorized to be on craigslist's computers.

At issue in *Pulte* was the defendant's incessant barrage of e-mails and phone calls to the plaintiff. *Pulte Homes, Inc. v. Laborer's Int'l Union of N. Am.*, 648 F.3d 295, 301 (6th Cir. 2011). The question facing the court was whether the defendant "had *any* right to call Pulte's offices and e-mail its executives." *Id*. at 304 (emphasis in original). Pulte did not do anything to block access to its e-mail servers or phone systems. Nor did it even allege that any single call or e-mail was unauthorized. The court, not surprisingly, concluded that the defendant had authorization to call and e-mail Pulte and dismissed the CFAA claim. *Id*. The court mentioned that Pulte's computers were "open to the public," so the defendant was "authorized to use" them. *Id*. (internal quotations omitted). But that was just another way of saying that Pulte didn't do anything to block or restrict access to anyone.

Here it is the opposite. craigslist notified 3taps in writing that its access to craigslist's computers was unauthorized and it blocked 3taps' access—*protected its computers*—by blocking 3taps' IP addresses. FAC ¶¶81-86, 132; *see also Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1038 (N.D. Cal. 2012) ("*Facebook II*") (concluding that circumventing IP blocks constituted "circumvent[ing] technical barriers to access the Facebook site, and thus access[ing] the site 'without permission'"). In fact, craigslist laboriously identified and blocked 3taps' IP addresses over and over and over again, many dozens if not hundreds of times, until 3taps resorted to a technique common to "black hat" hackers of accessing craigslist's computers using ever-changing networks of anonymous proxy IP addresses. 3taps' claim that it "accessed an unprotected public website and obtained information available to anyone with Internet access" under *Pulte* is thus patently false. Dkt. 94, at 4. craigslist's computers are protected and the only reason they became available to 3taps is because it went to great lengths to circumvent those IP block protections.[8] FAC ¶¶81-84, 86.

[8] 3taps' characterization of the cease and desist letter sent by Pulte and its import to this case is also wrong. It is not even clear that Pulte sent a letter to the defendant in that case. All we know is that Pulte's general counsel contacted the defendant. *Pulte*, 648 F.3d at 299. But the key fact that rendered the

Cvent, Inc. v. Eventbrite, Inc. is no more useful to 3taps than *Pulte*. There the court simply concluded that Cvent's terms of use were insufficient to render the defendant's scraping activities unauthorized because Cvent "takes no affirmative steps" to block anyone's access to Cvent's computers. 739 F. Supp. 2d 927, 932 (E.D. Va. 2010). This meant that "the entire world was given unimpeded access" to Cvent's computers. *Id*. at 933. Here, of course, craigslist uses IP blocking software to impede access by 3taps. FAC ¶¶81-83. So even under the facts and holding of *Cvent*, craigslist's CFAA claim remains well-founded.

Koch Industries v. Does is even less helpful to 3taps than *Pulte* and *Cvent*. In ruling that the defendants' use of Koch's website was not unauthorized under the CFAA, the court focused on the fact that Koch, like Cvent, did not impede anyone's access. *Koch Indus., Inc. v. Does, 1—25*, No. 2:10CV1275DAK, 2011 WL 1775765, at *8 (D. Utah May 9, 2011). Moreover, Koch did not even complain that the defendants lacked authorization to access Koch's computers. Rather, the complaint was that they "ultimately used the information in an unwanted manner." *Id*. That was a claim for unauthorized *use*, said the court, which the CFAA did not cover. *Id*.

3taps' cases are all factually distinguishable and none of them stand for the broad, CFAA-eviscerating propositions that 3taps wishes they did. Further, none of these cases even addressed the clear statutory language, which only imposes a "nonpublic" limitation in an unrelated part of the statute. There is no such limitation in the Scraping Provision.[9]

---

communication ineffective under the CFAA is that all general counsel did was ask that the barrage of e-mails and phone calls stop. *Id*. He did not tell the defendant that all access, or that any access for that matter, was unauthorized. *Id*. The opposite is true here. FAC ¶132.

[9] 3taps cites *Loud Records LLC v. Minervini* in a parenthetical. Dkt. 94, at 6. All of that court's musings about the CFAA are irrelevant, since a CFAA claim was not even at issue. *See Loud Records LLC v. Minervini*, 621 F. Supp. 2d 672, 674 (W.D. Wisc. 2009) (copyright claim at issue). At any rate, the *Loud Records* court's statement that it is tenuous to suggest that a computer is "protected" under the CFAA is wrong according to well-settled authority, including the definition of "protected computer" under the statute. *See* 18 U.S.C. § 1030(e)(2)(B) (defining "protected computer"); *Nosal*, 676 F.3d at 859 (interpreting that definition to mean any computer connected to the Internet). Thus, the *Loud Records* court's statement that "any allegation that . . . plaintiffs acted without authorization is tenuous at best" since the files "were accessible by the public" is not buttressed by any reasoning whatsoever and is contrary to established law. *See* Parts A.1., A.2., B.1., *supra*.

3. Reading The Dramatic Restrictions Proffered By 3taps Into The CFAA Would Gut The Statute In Harmful Ways Because It Would Eliminate The Private Property Protections That Congress Specifically Sought To Enact.

craigslist's computers are private property. Congress recognized that computers are private property, and the protection of that property was its specific aim in enacting the Scraping Provision. The legislative history is replete with compelling discussions:

- The Scraping Provision "would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited *in the same way theft of physical items are protected.*" S. REP. NO. 104-357, at 7.
- The Scraping Provision "is intended to protect against the interstate or foreign *theft of information by computer*." *Id.*
- "The conduct prohibited is analogous to that of '*breaking and entering*.'" H.R. REP. NO. 98-894, at 20 (1984).
- CFAA enacted to address "access *(trespass into) both private and public computer systems*, sometimes with potentially serious results." *Id.* at 10.
- Statute punishes "those who improperly use computers to obtain . . . information of nominal value *from private individuals or companies*." S. REP. NO. 104-357, at 7.

Indeed, Congress modeled the CFAA after the quintessential common law doctrine that protects private real property: the law of trespass. "The basic legal concept underlying the CFAA is the concept of 'unauthorized access,' a concept derived from the idea of trespass." Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass and Privacy*, 62 Bus. Law 1395, 1403 (2007). According to the Congress that enacted the CFAA, the conduct proscribed "*is akin to a trespass onto someone else's real property*." 131 Cong. Rec. S11,872 (daily ed. Sept. 20, 1985) (emphasis added); *see also* S. REP. NO. 99-432, at 7 (1986) (using "trespass" as shorthand for unauthorized access); S. REP. NO. 104-357, at 10-11 (same).[10]

3taps wants the Court to judicially amend the CFAA to impose limitations on the type of private property protected in ways that would totally undermine the purpose (let alone the

[10] Conversely, the common law trespass elements mimic the CFAA. *Emeryville Redevelopment Agency v. Eltex Inv. Corp.*, No. C 04-02737, 2004 WL 2359862, at *7 (N.D. Cal. Oct. 19, 2004) ("The essence of the cause of action for trespass is an unauthorized entry onto the land of another.") (internal quotation omitted).

unambiguous text) of the statute. Protecting only computers with password protections is akin to the law of trespass protecting only landowners that require visitors to speak a secret password before entering. That is not the law. Property owners are free to choose how they use their property and to whom they will allow access. That is the premise underlying the very concept of private property. *See Allred v. Harris*, 14 Cal. App. 4th 1386, 1390 (1993) ("[T]he right to exclude persons is a fundamental aspect of private property ownership."). An owner need not provide access to everyone, or anyone in particular. *See id*. Yet according to 3taps, the Court should read limitations into the CFAA that render craigslist completely unable to protect its property. Simply because craigslist chose to connect its computers to the Internet, all protections are lost and its computers become *public property* for every person in the world to do with them whatever he or she may please? That is an absurd result contrary to the spirit and purpose of the CFAA, which is to extend well-established principles of private property ownership to computers connected to the Internet, including the right to exclude unwanted intruders.

Consider a world where the San Francisco Giants franchise is unable to exclude any individual spectator from the free public viewing area behind the fence in right field. According to 3taps' logic, simply because the team decided to open up an area of its stadium for free public viewing, the Giants can never exclude *any individual person*. This is true even if they are stealing signs and relaying them to the opposing team, displaying ad banners, or broadcasting a radio play by play that competes with "Kruk & Kuip" on KNBR 680. The Giants would be without recourse to remove or deny that person access in the future, simply because the Giants opened the free viewing area to the public. All the Giants could do, according to 3taps' logic, is close the door to everyone.

A museum that offers free admission to the public provides another example. According to 3taps' logic, the mere fact that the museum is open to the public means that nobody can ever be excluded. That would include a patron that repeatedly violates the museum's prohibitions on eating and drinking or insists on touching the artwork. Or perhaps this "patron" decides to take high resolution photographs of all of the images in a photography exhibit despite the museum's

posted prohibitions, passes out pamphlets explaining why no one needs to follow the museum's rules, and then insists on his right to sell his photographs in competition with the museum gift shop. If 3taps' logic is accepted, the museum cannot exclude any person from its private property, regardless of their conduct.

Even 3taps' own hypothetical cuts against its argument. What 3taps is doing could not be further removed from window-shopping. *See* Dkt. 94, at 13. 3taps helps itself to millions of craigslist user postings per day—far more than any ordinary craigslist user, let alone the mere window shopper to which 3taps compares itself. 3taps believes it is entitled to ignore "3taps Keep Out!" signs, maneuver around numerous barriers it knows are designed specifically to keep it out, have numerous agents enter the "store" millions more times than any legitimate customer would, take every last bit of content from the store on an hourly basis, and make a business out of redistributing it to third parties for whatever purpose the third parties wish. In what bizarre world is leaving the shades open an invitation to this sort of conduct?

These examples illustrate why 3taps' theory of the CFAA contradicts the fundamental principles of property ownership, which the CFAA is designed to protect. But the need for craigslist to protect its private computers from interlopers is not just a matter of principle. The privacy and expectations of craigslist's users mandate it. craigslist users upload information to craigslist's computers expecting and trusting that the content will remain there. A user selling a piece of furniture, for example, posts an ad to craigslist trusting that when she edits her ad to change the price or conditions of sale, she will not receive calls, emails, or in-person visits from persons insisting on her prior price or terms because they viewed the unedited ad republished on other classified sites a la 3taps. Likewise, someone posting a "personals" ad to craigslist trusts and expects that that personals ad will only be presented to other members of his or her craigslist community and not be republished, thanks to 3taps, on various other dating sites he or she had already decided not to use. Similarly, the user trusts that once he or she deletes the ad or it expires, there will be no more inquiries from date-seekers. No such protections exist, however, if content can be lifted from craigslist's computers without consequence and republished all over

the Internet at the whim of 3taps and its customers.[11] As in the physical world, a web site operator must be able to exclude parties, including would-be competitors, who insist upon degrading the user experience.

C. 3taps' And The Amici's Parade Of Horribles And Policy Arguments Are Not Persuasive.

Upholding craigslist's CFAA claim on the facts here would be a narrow ruling. The Court has already concluded that 3taps' receipt of cease and desist letters from craigslist and circumvention of craigslist's code based restrictions on access (its IP address blocks) are enough to state a claim. *See* Dkt. 74, at 7-8. All the Court needs to do here is make the unremarkable determination that craigslist did not give up all of its rights under the CFAA by connecting its computers to the Internet. That would not result in any of the doomsday scenarios presented by 3taps or the Amici.

1. There Is Nothing Wrong With Empowering A Computer Owner To Restrict Access To Its Computers, Even If Violations May Result In Criminal Liability.

"There are countless situations in which the State prohibits conduct only when it is objected to by a private person most closely affected by it." *Planned Parenthood of Central Mo. v. Danforth*, 428 U.S. 52, 93 n.1 (1976) (White, J. concurring in part) (noting that the state "may enact and enforce trespass laws against unauthorized entrances"). This is just one of those situations.

3taps catastrophizing about the "arbitrary determinations" of private property owners does not remove the CFAA from this framework. Dkt. 94, at iii, 2, 7. craigslist's computers are private property and it has every right to decide who may and who may not access them. That includes pirates like 3taps, parasitical "innovators," and anyone else. If, for example, the owner

[11] 3taps may argue that ads deleted from craigslist are promptly removed by it and each of its customers. craigslist's research found the opposite, however. In any case, 3taps is advocating for a world where anyone can scrape craigslist's website, and redistribute user postings to an unlimited number of other sites across the Internet, where they can be misused in various ways and live on for arbitrary lengths of time, regardless of whether in the meantime those ads have been edited or deleted on craigslist by the users who posted them.

of an entertainment venue tells an obnoxious and chronically misbehaving guest that he is no longer welcome and is prohibited from entering that venue, there is nothing wrong with imposing civil or criminal liability on that unwelcome person should they insist upon entering the venue anyway. The ability to impose such liability is absolutely necessary, and indeed is the very foundation for every law on the books that protects private property. *See Allred*, 14 Cal. App. 4th at 1390. The facts of this case illustrate that this ability is every bit as necessary on the Internet, as recognized by Congress.

2. Blocking IP Addresses And Sending Letters Specifically Communicating Lack Of Authorization Provide More Than Enough Notice Of Unauthorized Access And Potential Penalties.

3taps argues that enforcing the CFAA against it would render the statute unconstitutionally vague for lack of notice. Dkt. 94, at 11-12. This falls well short.

As a threshold matter, the relevant question is not whether "applying the CFAA to persons who access publicly available websites would render the CFAA unconstitutionally vague," as 3taps suggests. Dkt. 94, at 11. Rather, it is whether the law would be vague *as applied to 3taps and the conduct in which it engaged*.[12] *See Holder v. Humanitarian Law Project*, 130 S.Ct. 2705, 2718-19 (2010) (reversing the Ninth Circuit for considering a "statute's application to facts not before it" and reiterating that "[w]e consider whether a statute is vague as applied to the *particular facts at issue*, for '[a] plaintiff who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others'") (emphasis added).

Here there is nothing vague or unknown about whether 3taps' access is unauthorized. 3taps is not an innocent lamb that unknowingly stumbled onto a computer in a manner that turns out to be unauthorized for no apparent reason. To the contrary, craigslist told 3taps not to enter its computers, 3taps then circumvented craigslist's IP blocks,[13] accessed the computers, and

[12] Concerns about the CFAA's implication to cases involving "browsewrap" licenses (*see* Dkt. 92-1, at 8) or any other hypothetical scenarios are not relevant here. In this case, the restrictions imposed on 3taps spring from (1) cease and desist letters, (2) IP blocks, and (3) this lawsuit.

[13] 3taps' strained argument that blocking a person's IP address does not constitute a form of withholding or blocking access has been rejected already. This Court rejected it in its April 30, 2013

harvested the information anyway. 3taps, moreover, designed its entire business plan—with "white papers" and all—around knowingly and purposefully accessing craigslist's computers without authorization in order to scrape the content there. It expected, indeed even hoped to be sued. This is exactly the sort of situation that the CFAA was unambiguously written to address. The notion that application of the CFAA to 3taps' conduct is somehow vague or unknown is not credible.[14]

Further, the notion that Internet users in general will unknowingly become criminals if the Court finds in craigslist's favor is absolutely false. craigslist does not seek to enforce its rights against unknowing and unsuspecting Internet users. craigslist is enforcing its rights against a persistently malicious entity that assaults its users by mass scraping and redistributing all of their ads after being notified repeatedly by craigslist to desist.

Lastly, the fact that criminal penalties could theoretically result from this behavior is not craigslist's doing. Congress drafted and enacted a statute to prohibit this exact type of behavior. Congress provided for civil and criminal enforcement. craigslist filed a civil suit to enforce the right that Congress provided to computer owners. craigslist is therefore not "criminalizing" anything.

3. The Rule Of Lenity Does Not Apply Here Because The Statute Is Unambiguous.

The "touchstone of the rule of lenity is statutory ambiguity." *Moskal v. U.S.*, 498 U.S. 103, 107 (1990) (internal quotations omitted). And the ambiguity must be "grievous." *Muscarello v. U.S.*, 524 U.S. 125, 138-39 (1998).

---

order. *See* Dkt. 74, at 7-8. Judge Ware also rejected it in his February 16, 2012 order granting summary judgment for Facebook where he concluded that breaking through IP blocks constitutes "circumvent[ing] technological barriers." *Facebook II*, 844 F. Supp. 2d at 1038.

[14] 3taps' First Amendment-based constitutional argument is also a nonstarter. *See* Dkt. 94, at 14. Restrictions on how private property can be used—including restrictions on what people write on private property and how they assemble on private property—are the foundation of all laws protecting private property and do not implicate the First Amendment. The First Amendment is not implicated, for instance, because the law of trespass bars the public from protesting in someone's backyard. Nor is it implicated in Facebook's terms of use, which prohibit harassing content posted to Facebook's website. *See* www.facebook.com/legal/terms at ¶3.

A "grievous ambiguity" does not exist simply because a defendant is able "to articulate a construction more narrow than that urged by the" party prosecuting the statute. *Moskal*, 498 U.S. at 108. Rather, the rule of lenity comes into play only in "those situations in which a reasonable doubt persists about a statute's intended scope even *after* resort to the language and structure, legislative history, and motivating policies of the statute." *Id*. (emphasis in original and internal quotations omitted).

Here, the phrase "without authorization" is unambiguous and has already been construed by the Ninth Circuit. Citing Webster's Dictionary, the court construed "without authorization" to mean having "no rights, limited or otherwise, to access the computer in question." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). 3taps concedes that this construction gives "without authorization" its "ordinary, contemporary, common meaning." *See* Dkt. 94, at 3 (citing *Brekka*). It is also entirely consistent with the statute's language and structure, legislative history, and motivating policies. *See* Parts A.1., A.2. B.3., *supra*. Manufacturing a theoretical additional construction—which 3taps never actually articulates other than to simply say that it is authorized to access craigslist's computers because they are connected to the Internet—gets 3taps nowhere since there is no ambiguity in the first instance. *See Moskal*, 498 U.S. at 108. The rule of lenity therefore is not implicated. *Id*.

4. This Case Is About *Access* Restrictions, Not Use Restrictions, And 3taps' And The Amici's Attempt To Conflate The Two Is Not Successful.

The Ninth Circuit in *Nosal* rejected the idea that a contractual restriction on how one may *use* information obtained from a computer that he is authorized to access may serve as the foundation of a CFAA claim. *Nosal*, 676 F.3d at 863. Mr. Nosal, in other words, was authorized to access the computers and customer lists that he ended up *using* in an unauthorized way. That did not violate the CFAA, according to the Ninth Circuit, because it was the breach of a *use* restriction, not an *access* restriction. *See id*. at 863-64. This case is completely different.

3taps has no authorization to *access* craigslist's computers or information in the first place. FAC ¶¶81-86, 132. craigslist made this clear by sending 3taps a cease and desist letter, filing this

lawsuit, and blocking 3taps' IP addresses. craigslist is entitled to restrict access for any reason it wants, including because it knows that a scraper like 3taps is going to abuse access to harm craigslist and its users. Prohibiting and blocking access, for this or any other reason, is still an *access* restriction. *See Brekka*, 581 F.3d at 1133 (access restriction is found when there are "no rights, limited or otherwise, to access the computer in question"). There is also no question that craigslist is entitled to revoke authorization to those that may have had authorization to access its computers in the past. *See id*. at 1135 (including in the definition of "without authorization" situations in which the computer owner "rescinded permission to access the computer and the defendant uses the computer anyway").

Furthermore, the policy concerns underlying the *Nosal* opinion do not apply here. The *Nosal* court was concerned about criminalizing an employee's *use* of a work computer for mundane things like reading ESPN.com, visiting a Sudoku website, or doing myriad other things with computers that people are otherwise authorized to *use*. 676 F.3d at 860-61.

3taps' conduct has nothing to do with these concerns. craigslist prohibited *all access* to its computers by 3taps. 3taps is not authorized to *use* craigslist's computers for any purpose whatsoever since it is not entitled to access those computers in the first place. The restriction is an *access* restriction, therefore, not a *use* restriction. The notion that a corporation ignoring specific instructions to keep out, circumventing IP blocks, harvesting hundreds of millions of user postings from craigslist's computers without permission, and redistributing those postings to anyone that wants to misuse them is somehow akin to reading ESPN.com at work is absurd. *Nosal* does not in any way support 3taps' effort to avoid the CFAA's reach here.

D. 3Taps' Legislative History Argument Fails As Well.

Legislative history only guides statutory interpretation when the statute is unclear. "Judges interpret laws rather than reconstruct legislators' intentions. Where the language of those laws is clear, we are not free to replace it with an unenacted legislative intent." *INS v. Cardoza-Fonesca*, 480 U.S. 421, 452-53 (1987) (Scalia, J. concurring); *see also Ratzlaf v. U.S.*, 510 U.S.

135, 147-48 (1994) ("[W]e do not resort to legislative history to cloud a statutory text that is clear.").

Here the statute is clear. *See* Parts A.1., A.2., *supra*. The words are unambiguous and Congress specifically chose *not to* limit the computers or information protected. *Id*. Trying to manufacture an ambiguity into the phrase "without authorization" does not allow 3taps to resort to legislative history, particularly when the interpretation 3taps proposes directly conflicts with the clear language of the statute. *See Ratzlaf*, 510 U.S. at 147-48.

At any rate, the legislative history is not even in 3taps' favor. 3taps boldly declares that "the CFAA's lengthy legislative history confirms" its argument that the statute only protects "private and confidential" information. Dkt. 94, at 9. The legislative history is indeed lengthy. But 3taps is tellingly only able to point to four statements in it that use the word "privacy" and *none* that use the word "confidential." *Id.* at 10-11. That is because the legislative history does not come close to "confirming" 3taps' argument. To the contrary, it confirms that the statute was modeled after common law trespass and contains no limitations on the computers or information protected.[15] S. REP. NO. 104-357, at 7-8; H.R. REP. NO. 98-894, at 10, 20.

E. The CFAA and California Penal Code Section 502 Claims Should Not Be Dismissed Because Factual Determinations Are Required.

Even if the Court were to conclude that the CFAA and California Penal Code Section 502 do not apply to "public websites" or "publically available information," the Court must still make findings of fact regarding whether craigslist's website conforms to the definition of either of these terms. craigslist's website is not accessible to all members of the public. Indeed, craigslist has blocked thousands of IP addresses from accessing its website for a variety of different reasons. Users are unable to access craigslist's website from these IP addresses. There is nothing "public" about the craigslist website for these users. craigslist's ability to exclude users from its website renders the craigslist website and the information thereon "private"—not "public." At a

[15] Even if protecting "private" information was a policy goal of the CFAA, that goal is met by enforcing the statute here since craigslist is using the statute to protect its users' privacy by preventing their postings from being republished and repurposed by other businesses without permission.

minimum, however, the Court must go beyond the FAC and engage in fact finding in order to determine whether craigslist's website is "public" or that the information thereon is "publically available." For this reason, alone, 3taps' renewed motion should be denied.

F. The Court Should Decline Amici's Request To Legislate From The Bench.

The thrust of the Amici's argument is that the entire world is authorized under the CFAA to access information on a computer—no matter what the computer owner says or does to restrict access—if the information can also be viewed on the Internet. *See* Dkt. 92-1, at 6-11. But no such requirement exists in the statute or the case law, as discussed above, and the Amici's own literature confirms this.

One of the Amici, Professor Davik (a.k.a. Professor Galbraith) writes, for example, that the CFAA should be *amended* so as to eliminate "information on public display" from the Scraping Provision's protections. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Available Internet Websites*, 63 Md. L. Rev. 320, 366-67 (2004). In that article, and in contrast to the arguments in the Amici's brief, Professor Davik correctly admits many times that the CFAA currently contains no such limitations. *Id*. at 331 (the "act as drafted appears to include protection for any type of information"), 335-36 (statute does not limit the type of information protected).

Likewise, another of the Amici, Jennifer Granick, writes that the CFAA implements "a bright line protecting the box [the computer], and even otherwise public data stored on the box is thereby subject to the system owner's control." Jennifer Granick, *Toward Learning From Losing Aaron Swartz*, available at http://cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz.

What the Amici are really doing, therefore, is asking the Court to amend the CFAA to add limitations that are not currently there. That is Congress' job.

Finally, none of the seemingly harsh or potentially unfair scenarios that the Amici use to justify their cries for amending the statute come anywhere close to the CFAA's implications in this case. This is a case about a persistent corporate interloper that incessantly accesses

craigslist's computers in the face of formal written prohibition, circumventing IP blocks, harvesting all of craigslist's content, and redistributing that content on a wholesale basis. This hurts craigslist's users, craigslist, and others who may be impacted by harmfully repurposed craigslist ads from 3taps' chop shop. This case is not about people that "view" information on a website, people fudging their age to create a Facebook account, or a seventeen year old visiting a website whose terms of use requires readers to be eighteen. The Amici may or may not be right that those or other scenarios might lead to uncomfortable results under the CFAA. But those are not the facts before the Court, nor is this the forum in which to address those issues.

CONCLUSION

The Court should deny the renewed motion to dismiss.

July 2, 2013

PERKINS COIE LLP

By:/s/ Bobbie Wilson
Bobbie J. Wilson (SBN 148317)
bwilson@perkinscoie.com

Attorneys for Plaintiff
craigslist, Inc.

I, Brian Hennessy, hereby attest, pursuant to N.D. Cal. Local Rule 5-1(i)(3), that the concurrence to the filing of this document has been obtained from each signatory hereto.

July 2, 2013

PERKINS COIE LLP

By:/s/ Brian Hennessy
Brian Hennessy (SBN 226721)
bhennessy@perkinscoie.com

Attorneys for Plaintiff
craigslist, Inc.