ALLEN RUBY (Bar No. 47109)
JACK DICANIO (Bar No. 138782)
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
525 University Avenue, Suite 1400
Palo Alto, California 94301-1908
Telephone: (650) 470-4500
Facsimile: (650) 470-4570
Allen.Ruby@skadden.com
Jack.DiCanio@skadden.com

Attorneys for Defendants 3TAPS, INC. and DISCOVER HOME NETWORK, INC. d/b/a LOVELY

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.

3TAPS, INC., a Delaware corporation,

Counter-claimant,

v.

CRAIGSLIST, INC., a Delaware corporation,

Counter-defendant.

CASE NO.: CV-12-03816 CRB

DEFENDANT 3TAPS, INC.'S REPLY RE: MOTION TO DISMISS CAUSES OF ACTION NOS. 13 AND 14 IN PLAINTIFF'S FIRST AMENDED COMPLAINT

Honorable Charles R. Breyer

Hearing Date: July 12, 2013, 10:00 a.m.

JAMES A. KEYTE (admitted *pro hac vice*)
MICHAEL H. MENITOVE (admitted *pro hac vice*))
MARISSA E. TROIANO (admitted *pro hac vice*)
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Four Times Square
New York, New York 10036
Telephone: (212) 735-3000
Facsimile: (917) 777-3000
James.Keyte@skadden.com
Michael.Menitove@skadden.com
Marissa.Troiano@skadden.com

ABRAHAM TABAIE (Bar No. 260727)
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
300 South Grand Avenue, Suite 3400
Los Angeles, California 90071
Telephone: (213) 687-5000
Facsimile: (213) 687-5600
Abraham.Tabaie@skadden.com

Attorneys for Defendants 3TAPS, INC. and
DISCOVER HOME NETWORK, INC. d/b/a
LOVELY

TABLE OF CONTENTS

TABLE OF AUTHORITIES

PAGES

Cases

Statutes

Other Authorities

Legislative History

SUMMARY OF ARGUMENT

The Court should grant 3taps' Motion and dismiss the CFAA and Section 502 claims:

- Where the owner of a website does not configure that site to restrict access to public information, the CFAA does not apply. *See, e.g.*, *Pulte Homes, Inc. v. Laborers Int'l Union of N. Am.*, 648 F.3d 295, 299 (6th Cir. 2011); *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006).
- craigslist's argument that 18 U.S.C. § 1030(a)(2)(C) bars 3taps' scraping because there are no modifiers limiting the words "computer" and "information" is immaterial as these terms simply have nothing to do with 3taps' argument. Instead, 3taps is arguing that even though the CFAA protects all computers and the information stored on those computers, the CFAA requires "access . . . without authorization" and, by putting public information on the Internet, craigslist has *ipso facto* authorized access to that information.
- Contrary to craigslist's argument, the cases 3taps cite confirm that access to a public website is "authorized," even if the website owner otherwise attempts to block access or puts the accessor on notice that access is unauthorized. *See, e.g.*, *Pulte Homes*, 648 F.3d at 299.
- In arguing that the CFAA is analogous to trespass law, craigslist ignores the fact that a public website has no technological barriers analogous to a property boundary. In any event, navigating the publicly-available Internet is a far cry from breaking into another's property irrespective of the desire by the website owner to block visits by competitors.
- craigslist's IP blocking is not a barrier to access under the CFAA because, even after craigslist blocks an IP address, the user-generated ads on craigslist are still available on a public website and, therefore, access to them remains authorized. In any event, IP address blocking is insufficient to block access because an IP address is not tied to a specific person, and IP address blocking does not make information "private."
- Lastly, even if the Court determines that the term "without authorization" is ambiguous when a public website owner demands that access to public information cease, under the rule of lenity the Court should adopt 3taps' narrower interpretation.

PRELIMINARY STATEMENT

Rather than address the substantive legal and public policy issues raised by Defendant 3taps, Inc.'s ("3taps") Supplemental Brief ("Brief"), Plaintiff craigslist Inc. ("craigslist") picks fights over issues not in dispute and resorts to name calling and personal attacks.[1] But the issue before the Court is very straightforward: can information that is made publicly available on a public website viewed by over 60 million users be the subject of a Computer Fraud and Abuse Act ("CFAA") violation simply because the owner of the website does not like the manner in which a particular viewer is obtaining and using that information. Respectfully, the answer is no. Where the owner of a website does not configure that site to restrict access to public information, the CFAA does not apply.

craigslist's arguments to the contrary are all without merit. Initially, craigslist hypothesizes how three craigslist users might feel were they to find out their classified ads had been disseminated outside of craigslist's website. However, because craigslist does not assert any allegations regarding "theoretical" craigslist users in its First Amended Complaint ("FAC"), these speculative musings are irrelevant.[2] Moreover, each hypothetical craigslist user is concerned about how the public information they post on a public website might be "used." (Opp'n 1-2.) But under Ninth Circuit law, such concerns over the use of information once access is authorized is outside the CFAA's scope. *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012). Simply, if craigslist believes that 3taps' "use" of information to facilitate competition with craigslist is improper, it may bring other claims (as it has) against 3taps, but it may not bring a CFAA claim.

[1] 3taps will not respond to each of the inappropriate character attacks craigslist makes against 3taps and its CEO Greg Kidd. It must be said, however, that such attacks are wholly unrelated to the legal issue at hand and statements attributed to Mr. Kidd are taken completely out of context in a misguided attempt to influence the Court's legal interpretation of a statute. craigslist is more cautious in its approach to the amicus curiae, Electronic Frontier Foundation, which supports 3taps' position in full and has craigslist's founder, Craig Newmark, as an Advisory Board Member. *See https://www.eff.org/about/advisoryboard* (last visited July 12, 2013).

[2] In fact, 3taps believes the factual record will show that instead of being "upset" at the way their classified ads are disseminated, "craigslist users" are pleased that their posts are seen by a wider audience on more user-friendly websites like padmapper.com and livelovely.com. The wider the audience, the more likely it is that their ads will be viewed by a person interested in what they are offering. Further, a craigslist user "concerned" about personal information being used after a post is no longer relevant need only do what the majority of craigslist users do: utilize craigslist's anonymized email address to protect personal information from becoming public. (*See* Opp'n 1.)

craigslist next argues that 18 U.S.C. § 1030(a)(2)(C)[3] bars 3taps' scraping[4] because there are no modifiers limiting the words "computer" and "information" in that provision, showing that Congress chose not to limit the computers or type of information protected under the CFAA. These points are merely straw men that have nothing to do with 3taps' argument. The CFAA protects all computers and the information stored on those computers. But the CFAA requires "access . . . without authorization;" and, by publishing public information on the Internet, craigslist has *ipso facto* authorized access to that information.

craigslist then contends that the cases 3taps relies on merely stand for the proposition that website owners must take affirmative steps to revoke or restrict otherwise authorized access – which craigslist believes it did through a cease-and-desist letter and IP address blocking. craigslist is wrong both legally and factually. First, case law squarely supports that access to public websites and computers is authorized, even if the website owner takes affirmative steps to block access or notifies the accessor that access is unauthorized. *See Pulte Homes, Inc. v. Laborers Int'l Union of N. Am.*, 648 F.3d 295, 299 (6th Cir. 2011). Second, craigslist cannot selectively "de-authorize" 3taps from accessing the public information on its website because, by making that information available to the public writ large on a website, craigslist loses the ability, under the CFAA, to selectively "revoke" authorization from those it does not want obtaining the public information.

Lastly, if the Court determines that the term "without authorization" is ambiguous when a

[3] Section 1030(a)(2)(C), incidentally, is not called, and never has been called, the "Scraping Provision." craigslist cannot unilaterally name § 1030(a)(2)(C) its desired interpretation when there is no evidence whatsoever that Congress contemplated scraping in enacting the provision.

[4] craigslist improperly equates "scraping" with a bad act, akin to "hacking." But, "[a] scraper, also called a 'robot' or 'bot,' is nothing more than a computer program that accesses information contained in a succession of webpages stored on the accessed computer . . . information available to anyone who views the site." *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58, 60 (1st Cir. 2003). In fact, the Internet is premised on "scraping," as search engines like Google and Bing scrape information, including the same information 3taps scrapes from craigslist. (Opp'n 5, n.4.) Google even offers a program Google calls "scraper" that anyone can use. *See* http://goo.gl/dVQ4k. According to craigslist, Google and Bing are "legitimate search engines" while 3taps employs "hackers." *Id.* craigslist's attempt to create "good scrapers" and "bad scrapers" is selective censorship and, more importantly, reveals that craigslist is concerned about "use," not access, by entities it deems to be competitors.

public website owner demands that access to public information by a competitor cease, under the rule of lenity the Court should adopt 3taps' narrower interpretation. craigslist apparently concedes this point as it only argues that the CFAA is unambiguous and that authorization was denied.

ARGUMENT

I. The CFAA Does Not Apply to Publicly Available Information On a Public Website

craigslist's principle argument is that because the terms "computer" and "information" are not limited by § 1030(a)(2)(C), and they are limited in other parts of the CFAA, Congress specifically sought to protect public information on public websites. (Opp'n 6-7.) While the CFAA does not limit the type of information that *can* be protected on computers, craigslist fails to properly contextualize § 1030(a)(2)(C). To be liable under that provision, one must "access[] a computer *without authorization* . . . and thereby obtain information . . ." 18 U.S.C. § 1030(a)(2)(C) (emphasis added). 3taps is arguing that craigslist has *authorized* the public to view and obtain information stored on its computer by making the information on its website publicly available.[5]

Therefore, the terms "protected computer" and "information," however broadly defined, have nothing to do with the issue before the Court.[6] For example, consider an apartment owner who posts an apartment rental classified ad on craigslist. To be sure, the owner's computer is a "protected computer" under the CFAA, even though it is connected to the Internet. Similarly, *all* the information on his computer also is protected regardless of whether the information is personal and private or otherwise publicly available elsewhere. But the information the apartment owner

[5] The manner in which 3taps obtains information from craigslist's website is irrelevant under the CFAA. The CFAA makes no distinction between reading information and copying it. *See* S. REP. NO. 104-357, at 7 (1996) ("[T]he term 'obtaining information' includes merely reading it.").

[6] For the same reason, craigslist also is incorrect in arguing that the use of the term "nonpublic computer" elsewhere in the statute confirms that public information on a public website is protectable. craigslist notes the distinction between a public and "nonpublic computer" in order to wrongly imply that Congress purposefully protected all publicly available information on a public website. (*See* Opp'n 6-7.) Congress determined that, for "nonpublic" government computers, it should be a crime to access the computers even if information is *not obtained* as long as the access "affects the use" of those computers. *See* 18 U.S.C. § 1030(a)(3). This distinction between access to obtain information and access merely affecting use does not speak to the issue before the Court: whether craigslist has necessarily *authorized* the entire public to access the information on its website by making that information publicly available.

posts on craigslist's website is not protected under the CFAA, because the apartment owner has *authorized* access to such information by placing it on a public website.

3taps, therefore, does *not* contend, as craigslist inexplicably argues, that by "connecting a computer to the Internet" one somehow loses any protection afforded under the CFAA. What 3taps *does* contend is that by publishing information on a public website, one has *authorized* all Internet users to access the computer on which the information is stored to obtain the information.

II. 3taps Is Authorized Under the CFAA Because It Obtains Publicly Available Information from a Public Website

A. craigslist Did Not Merely "Connect A Computer To The Internet," It Made Open Access To Its Website an Integral Part of Its Business Model

craigslist mischaracterizes 3taps' position to suggest that if a computer is connected to the Internet without a password, the entire world is forever "authorized" under the CFAA to access the computer "for any purpose." (Opp'n 8, 20.) 3taps does not make the argument that simply connecting a computer to the Internet relinquishes the right to bring a CFAA claim. craigslist, however, does not just "connect its computer to the Internet." On the contrary, its business model is such that it profits by making user-generated classified ads publicly available on its website. "A person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party" unless the person employs "protective measures" to keep the information private. *United States v. Gines-Perez*, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (holding no "expectation of privacy" in photographs posted to a publicly available website).

Having used the limitless and open nature of the Internet to its full advantage, while earning substantial profits, craigslist now tries to deny others – most notably more innovative competitors – access to the very same public information. The Eleventh Circuit has noted the dangers associated with such tactics:

> Through the World Wide Web, individuals can easily and readily access websites hosted throughout the world. Given the Web's ubiquitous and public nature, it becomes increasingly important in cases concerning electronic communications available through the Web for a plaintiff to demonstrate that those communications are not readily accessible. If by simply clicking a hypertext link, after ignoring an

> express warning, on an otherwise publicly accessible webpage, one is liable under [unauthorized access statutes], then the floodgates of litigation would open and the merely curious would be prosecuted.

Snow v. DirecTV, Inc., 450 F.3d 1314, 1321 (11th Cir. 2006) (interpreting 18 U.S.C. § 2701(a), which is almost identical to the CFAA).

A computer user who simply "connects to the Internet," *but has not actively disseminated information to the public on the Internet*, has not authorized others to access his computer to obtain such information. Similarly, a website owner that has non-public information protected by a password, firewall, or similar restriction, has not authorized access to those who overcome such technological barriers to entry. However, by making public information available on its public website, craigslist has "authorized" access to the information on its computers under the CFAA.

B. Case Law Confirms That the CFAA Does Not Apply To Publicly Available Information on a Public Website

Despite craigslist's arguments to the contrary, the principles underlying the cases cited by 3taps (*see* Brief 4-6) confirm that access to a public website is authorized even if the website owner takes affirmative steps to block access or puts the accessor on notice that access is unauthorized.

craigslist's attempt to distinguish *Pulte Homes* on the ground that the defendant was not "on notice" that its "attack" was unauthorized lacks credibility. (Opp'n 10-11.) In *Pulte Homes*, Pulte's general counsel told the union to stop its "attack" and, like craigslist, sent a cease-and-desist letter to the union demanding it stop the calls and emails.[7] 648 F.3d at 299. The court held that the company's "phone and email systems," like "an unprotected website," "were open to the public, so [the union] was authorized to use [them]" even though the union was on notice that the attack was purportedly unauthorized. *Id.* at 304 (internal quotations and citations omitted); *see also Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932-33 (E.D. Va. 2010) (dismissing CFAA claim even though lawsuit seeking to enjoin access put defendant on notice that continued access was purportedly "unauthorized").

[7] craigslist's statement that "it is not even clear that Pulte sent a letter to the defendant in that case" is incorrect. (*See* Opp'n 12 n.9.) The court found that "Pulte's general counsel faxed and overnighted a cease-and-desist letter to [the union], in which Pulte demanded that [the union] stop encouraging the calls and e-mails and that it 'use every means available to [it] to put an end to this activity.'" *Pulte Homes*, 648 F.3d at 306.

craigslist's attempt to distinguish *Koch Industries, Inc. v. Does* is equally unavailing. First, craigslist argues that Koch did not complain that the defendants lacked authorization to access its computers. (Opp'n 12.) That is simply untrue. *See Koch Indus., Inc. v. Does*, No. 2:10CV1275DAK, 2011 WL 1775765, at *7 (D. Utah May 9, 2011) ("Koch asserts that in creating the fake website Defendants acted without authorization . . . ."). Second, craigslist argues that the court focused on the fact that "Koch did not impede anyone's access," and that, here, craigslist did through a cease-and-desist letter and IP blocking. (Opp'n 12.) But in *Koch*, the court held that the information was "publicly available on the Internet, without requiring any login, password, or other individualized grant of access. By definition, therefore, [the defendants] could not have 'exceeded' [their] authority to access that data." *Koch*, 2011 WL 1775765, at *8 (internal quotations and citations omitted). The outcome would not have been affected if Koch had sent a cease-and-desist letter or blocked any IP addresses. According to the court, "'by definition,'" defendants had authority to obtain information "'publicly available on the internet.'" *Id.*

craigslist is "an unprotected website" that is "'open to the public, so [anyone is] authorized to use'" it. *See Pulte Homes*, 648 F.3d at 304. Like the plaintiff in *Pulte Homes*, craigslist does not approve of how 3taps accesses its website. But as *Pulte Homes*, *Cvent*, and *Koch* make clear, craigslist's disapproval regarding the access and use of information on its website is irrelevant even if 3taps is on notice of such disapproval. Further, craigslist's argument that notice of an access restriction is enough to make access to a public website unauthorized has been expressly rejected by the Eleventh Circuit. In *Snow*, the plaintiff alleged that his website "was maintained by warning notices forbidding access by DirecTV," 450 F.3d at 1321 n.7, and argued that DirecTV's access was "unauthorized" because, before viewing his website, a user had to "affirm his non-association with DirecTV." *Id.* at 1321. In rejecting the plaintiff's argument, the court held: "Nothing inherent in any of these steps prompts us to infer that access by the general public was restricted . . . . In order to be protected by [the statute prohibiting against unauthorized access], an Internet website must be configured in some way so as to limit ready access by the general public." *Id.* at 1321-22.

craigslist's business model is configured to provide the general public access to classified ads. Case law confirms that by making information publicly available on its website, craigslist

"authorized" 3taps' access to such information even though it put 3taps "on notice" that it does not want 3taps to access its website because it disapproves of 3taps' use of the information.

C. craigslist's Cases Do Not Address Access To Information on a Public Website

Arguing that the "weight of authority" rejects the notion that everyone is authorized to access public information on a public website (Opp'n 9), craigslist mainly relies on *eBay v. Digital Point Solutions*, 608 F. Supp. 2d 1156 (N.D. Cal. 2009). In *eBay*, defendants allegedly engaged in a "cookie stuffing scheme" in which they surreptitiously inserted software code on third-party computers, causing the computers to visit eBay's website without the third-party's knowledge and resulting in defendants obtaining improper payments of advertising fees. *Id.* at 1160. Defendants *only* argued that eBay's computers were not "protected" under the CFAA because eBay is a public website. *Id.* at 1164. The court rejected the argument because defendants allegedly "caused users to access eBay's website solely to corrupt eBay's advertising affiliate data." *Id.*

First, *eBay* is distinguishable because 3taps does not argue that craigslist's servers are not "protected computers" under the CFAA; it argues that Internet users are *authorized* to obtain public information on a public website. More importantly, in *eBay*, defendants used software code to *corrupt advertising data*. *See id.* Corrupting a website's operations is, of course, access without authorization under the CFAA. 3taps, however, only obtains classified ads posted on craigslist's website – which every Internet user is authorized to do.

EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003), is the only other case craigslist relies on that addresses information on a public website. In *Zefer*, the court recognized that once a website owner makes information publicly available, it cannot complain about the use of the information. *Id.* Although the court opined, in dicta, that terms of use might limit access to a public website, *id.* at 62, the Ninth Circuit specifically rejected that view in *Nosal*. *See* 676 F.3d at 863-64. Importantly, the *Zefer* court also noted that if the website owner "purport[ed] to exclude competitors from looking at its website[,] any such limitation would raise serious public policy concerns." 318 F.3d at 63. craigslist is doing exactly that: purporting to prevent 3taps, its direct competitor, from looking at its website, and trying to create criminal liability in the process.

While craigslist cites several other cases upholding CFAA claims, as craigslist admits, none of these cases actually addresses the public nature of the website or information at issue. (Opp'n 10 (citing *Ticketmaster LLC v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1113 (C.D. Cal. 2007) (stating, without analysis, that unauthorized access appeared likely); *Register.com, Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238, 251-53 (S.D.N.Y. 2000) (same), *aff'd as modified by* 356 F.3d 393 (2d Cir. 2004); *Barnstormers, Inc. v. Wing Walkers*, LLC, No. EP-10-CV-261-KC, 2011 WL 1671641, at *3-4 (W.D. Tex. May 3, 2011) (entering default judgment)).) In fact, *Ticketmaster*, like *eBay*, did not involve obtaining information from a website; rather, the defendants bombarded Ticketmaster's website with thousands of automated requests, preventing other users from purchasing tickets. 507 F. Supp. 2d. at 1103-04. Moreover, these pre-*Nosal* cases rely on a website owner's use prohibition, which *Nosal* rejects. *See, e.g.*, *Sw. Airlines v. Farechase*, 318 F. Supp. 2d 435, 439 (N.D. Tex. 2004) ("[Defendant] knew that Southwest prohibited the use of any [scraper.]"); *Barnstormers*, 2011 WL 1671641, at *9 ("Plaintiff has adequately alleged that Defendants exceeded the scope of [their] authorization by using the information found on the website for other purposes.").

D. There Is No Property Interest in Public Information on a Public Website and Therefore Trespass Law Is Inapplicable

craigslist next argues that because its computers are private property and Congress intended to model the CFAA after trespass law, craigslist is "free to choose how [it] use[s its] property and to whom [it] will allow access." (Opp'n 14.) In so arguing, craigslist ignores the fundamental difference between trespass and navigating a public website on the Internet.

First, as explained in 3taps' Brief, while the concept of trespass and authorized access "may be clear enough in the physical world[,] . . . when one accesses another computer in a network, one merely transmits data from one computer to another." Peter A. Winn, *The Guilty Eye: Unauthorized Access,Trespass and Privacy*, 62 Bus. Law 1395, 1405 (2007). "Computers in a networked environment literally lack borders . . . ." *Id* . at 1417. The "Internet is a means for communicating via computers: Whenever we access a webpage . . . we are using one computer to send commands to other computers at remote locations" to request information. *Nosal*, 676 F.3d at

861. Therefore, each time 3taps' computers communicate with craigslist's computers, craigslist necessarily authorizes access by willingly interacting with 3taps' computers and providing the publicly available information on its website.

craigslist's cease-and-desist letter and IP blocks are merely attempts to stop 3taps from making requests for information in this technologically open environment. But critically, the CFAA does not criminalize persistent and unwanted requests, but rather only unauthorized intrusions into a computer (*i.e.*, hacking). Phrased in terms of trespass, craigslist, by business necessity, has configured a website that has no property boundaries and houses content (created by users) that is *not* its own. But, unhappy with how 3taps ultimately uses the information, craigslist has taken measures to try and stop 3taps from visiting a publicly available website or obtaining publicly available content. From a CFAA perspective, 3taps has done nothing more than be persistent in making requests where no technological barrier exists.

Thus, while Congress modeled the CFAA after trespass, "the conduct prohibited is [actually] analogous to that of 'breaking and entering,'" H.R.REP. NO. 98-894, at 20 (1984), and "ensure[s] that the theft of intangible information by unauthorized use of a computer is prohibited in the same way theft of physical items are protected." S. REP. NO. 104-357, at 7. It is simply disingenuous for craigslist to argue that the classified ads *users* generate and post on craigslist's public website – which are necessarily intended to be disseminated to the public writ large – are being "stolen" when they are obtained by 3taps.[8] Therefore, given the property rights Congress sought to protect in enacting the CFAA, 3taps has not violated § 1030(a)(2)(C) by obtaining user-generated information that craigslist made available to the public.

Second, even if Congress expected the CFAA to co-opt trespass doctrines (which it did not), and the Court believes that accessing public information from a public website equates to entering private land (which it does not), 3taps *still* is not liable under the CFAA. "Even in traditional trespass cases . . . the question of permission was never allowed to remain a simple

[8] Contrary to craigslist's assertions (*see* Opp'n 21), the legislative history *confirms* that the CFAA was meant to protect against the theft of *private* and *confidential* information, not publicly available information. *See* S. REP. NO. 104-357, at 7 ("The bill would amend section 1030(a)(2)(C) to increase protection for the privacy and confidentiality of computer information.").

matter of the subjective will of the landowner. To achieve balance, courts [adopted the legal doctrines] 'implied permission' and 'apparent consent.' They would find implied licenses as a matter of law when property owners were perceived to be arbitrarily blocking socially productive and otherwise reasonable forms of access."[9] Winn, 62 Bus. Law at 1398; *see also Desnick v. Am. Broad. Cos., Inc.*, 44 F.3d 1345, 1352-53 (7th Cir. 1995) (holding ABC not liable for trespass when it secretly filmed a doctor in violation of a contract ABC signed with the doctor because there was no interference with the possession of the property). Similarly, here, access to publicly available information on a public website is a socially productive act, or at least a reasonable form of access given that the Internet is premised on the free flow of information. (*See* Brief 11.)

Stated plainly, craigslist cannot argue that it has a private property interest in non-copyrightable information that it affirmatively publishes to the world on a publicly-accessible website. In this context, "trespass" makes no sense. Even if trespass law were adopted wholesale under the CFAA (which it should not be) and craigslist had some form of property interest, 3taps, like the rest of the world, has implied permission or apparent consent to obtain and use the information on craigslist's website because the openness of the Internet requires the free flow of information on public websites. Indeed the "socially prudent" benefits of finding an implied license in these circumstances far outweigh any social utility derived from allowing a website owner to selectively block access to publicly available information, including by competitors.[10]

---

[9] Examples of "'implied permission'" or "'apparent consent'" trumping the subjective intention of the owner include: "a general license to hunt and fish . . . on private land[]," and entering an inn or public house. Winn, 62 Bus. Law at 1422-23. Similarly, First Amendment concerns can trump trespass claims. *See e.g.*, *In re Hoffman*, 67 Cal. 2d 845, 851 (1967) (holding that because "[t]he railroads seek neither privacy within nor exclusive possession of their station," they cannot invoke the law of trespass to prohibit the passing out of anti-war leaflets).

[10] craigslist's hypotheticals are nonsensical, including the Giants example. (Opp'n 14.) First, the Giants have always controlled access to the free viewing area. And, of course, the Giants can expel a patron from the area for interfering with the game. But they cannot expel someone watching the game simply because he is an Oakland A's fan. Going further, they definitely cannot broadcast the game then criminalize the A's fan for watching it on TV after the Giants tell him not too. But that is exactly what craigslist is doing. craigslist wants all the attendant benefits that come with using the Internet's public network but wants to deny its competitors those same benefits. Moreover, each of the harms craigslist outlines in its hypotheticals, including broadcasting a radio play, touching the artwork, etc., are *other torts*, not trespass.

E. craigslist Has Not Restricted 3taps' "Access" By Blocking IP Addresses

craigslist's argument that 3taps' access is unauthorized because 3taps "circumvented technological barriers" is a red herring in the context of a website that remains configured to grant access to the public. Even after craigslist blocks an IP address (analogous to sending a cease-and-desist-letter), the user-generated ads on craigslist are still available on a public website and, therefore, access to them remains authorized.

Assume, for example, that NBC blocks an Internet user from using his home IP address to log on to nbc.com to watch the latest episode of Saturday Night Live and tells the user he is no longer allowed to watch SNL because he criticizes the sketches on a blog. Later, the user goes to his friend's house and watches SNL with his friend, using his friend's IP address. The user has not circumvented technological barriers to "access" because nbc.com remains configured to be accessible by the public at large – *i.e.* it is not configured to protect the information on the website. *See Snow*, 450 F.3d at 1321-22 (plaintiff must demonstrate that information is not readily accessible by general public).

craigslist's argument that its blocking of IP addresses constitutes a technological barrier to access makes no sense in the context of a publicly available website. This is because IP addresses have nothing to do with the public configuration of a website itself.[11] Moreover, an IP address is *not* even a person, so blocking an IP address does not block a person's access at all. An IP address is an arbitrary number used by an Internet user for a short time and most Internet users employ many different IP addresses daily.[12] IP addresses are therefore comparable to a million roads

[11] For these reasons, the court in *Facebook, Inc. v. Power Ventures, Inc.*, 844 F. Supp. 2d 1025, 1038 (N.D. Cal. 2012), wrongly held that the defendant circumvented technological barriers to access by using multiple IP addresses to access Facebook. That decision also is distinguishable, as this Court recognized, because it did not involve access to public information. (Order Granting in Part and Denying in Part Mots. to Dismiss at 8 n.8 (N.D. Cal. Apr. 30, 2013, Dkt. 74).)

[12] Physical locations used to have static IP addresses. Today, that is no longer true. IP addresses change frequently in a single location. People also have different IP addresses for their home, their work, their cell phone, at the coffee shop, etc. In fact, there are currently more computer devices in the world than IP addresses and Internet users share IP addresses constantly depending on who in the world is connected to the Internet at any given time. *See* Rolf H. Weber & Ulrike I. Heinrich, *Anonymization* 11-12 (2012). Moreover, businesses that rely on other company's servers (the "cloud") can be assigned thousands of IP addresses at any given time, depending on their immediate server needs. *See* Bradley Morgan, *Wireless Security Attacks and Defenses*, http://www.windowsecurity.com/white papers/WirelessSecurity/Wireless-Security-Attacks-

(cont'd)

leading into a city. Just because a road is blocked does not mean a traveler does not have "access" to the city via a different road. Because an Internet user is not beholden to a specific IP address, and given the constant changing of IP addresses, blocking IP addresses is not a barrier to access.

For a technological barrier to revoke authorization to information on the *Internet*, the barrier must be used to keep information *private*. *See Gines-Perez*, 214 F. Supp. 2d at 225. craigslist admits that it blocks 3taps' IP addresses to keep 3taps away, not to keep information private. Taking the travel metaphor further, if craigslist wants to create a true technological barrier to access under the CFAA, it must erect a "wall" around its city, in the form of a code-based restriction, and make information on its website private.

III. Applying The Legal Analysis In *Nosal*, This Court Should Adopt 3taps' Interpretation

Even if the Court disagrees with 3taps' position that it has authorization to view craigslist's website, the term "without authorization" is at the very least ambiguous in this context, and, as in *Nosal*, the Court should adopt 3taps' narrower interpretation of the term.

A. "Without Authorization" Arguably Can Be Read in at Least Two Ways

As craigslist admits, the Ninth Circuit has defined "[a]uthorization . . . as 'permission or power granted by an authority'" and the term "'without authorization'" as "no rights, limited or otherwise, to access the computer in question." *See LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). Just as the Ninth Circuit held that the definition of "exceeds authorized access" could "be read either of two ways," so can the definitions of "authorization" and "without authorization." *See Nosal*, 676 F.3d at 856. As explained by 3taps (Brief 8), the term could be interpreted to mean that once public information is made available on a public website, everyone has authorization to access it. Or, conversely, as craigslist suggests, it could allow the subjective intent of a website owner to selectively determine authorization notwithstanding the fact that the information is publicly available.

(cont'd from previous page)
Defenses.html (last visited 7/12/2013) (describing a "corporate environment where thousands of IP addresses are leased throughout the day").

B. As In *Nosal*, The Rule of Lenity Applies

craigslist only argues that the rule of lenity does not apply because the phrase "without authorization" is unambiguous. craigslist does *not* argue that if the phrase is ambiguous it should be interpreted in its favor. (Opp'n 18-19.) But as in *Nosal*, the phrase is ambiguous *in the present circumstance* and, therefore, 3taps' narrower interpretation must be adopted. 676 F.3d at 863-64.

Under the Ninth Circuit's definition of "authorization" and "without authorization," it is at least arguable that 3taps has "rights, limited or otherwise" to visit craigslist.org. First, the statute is unclear as to whether craigslist has the "authority" to selectively deny access once it publishes information on a public website. (Brief 8.) Second, 3taps has "rights" to access craigslist when all 3taps has to do is use an IP address that craigslist has not blocked to access the website. (Brief 12.)

In *Nosal*, the court held that Congress did not mean "to criminalize conduct beyond that which is inherently wrongful, such as breaking into a computer." 676 F.3d at 859. Similarly, here, 3taps does nothing inherently wrongful in copying non-copyrightable public information disseminated over the Internet. Because there is significant doubt about whether Congress intended the CFAA "to prohibit the conduct in which [3taps] engaged, [this Court should] choose the interpretation least likely to impose penalties unintended by Congress." *See id.* at 863.

C. As in *Nosal*, This Court Should Reject an "As Applied" Interpretation of "Without Authorization" and Consider its Application to Other Internet Users

craigslist demands that the Court interpret the term "without authorization" "as applied to 3taps and the conduct in which it is engaged" and ignore how its interpretation would affect other Internet users. (Opp'n 17.) But, "[i]t is not possible to define authorization narrowly for some CFAA violations and broadly for others." *See Advanced Micro Devices, Inc. v. Feldstein*, No. 13-40007-TSH, 2013 WL 2666746, at *4 (D. Mass. June 10, 2013). As in *Nosal*, the Court must consider how its interpretation would affect all Internet users – who likely would be appalled to learn that it is a federal crime to access an unprotected, public website if the owner tells them not to. If Congress desires to criminalize accessing public websites against their owners' wishes,

"Congress should have spoken in language that is [more] clear and definite." *Nosal*, 676 F.3d at 863 (citation and internet quotation marks omitted).[13]

D. As in *Nosal*, the Court Is Not Legislating from the Bench by Interpreting an Ambiguous Statute

The Court would not be "legislating from the bench" by adopting 3taps' interpretation of "without authorization," as craigslist contends.[14] (Opp'n 22.) Courts have a duty to interpret statutes susceptible to multiple readings. *See Nosal*, 676 F.3d at 862-63. Congress drafted the CFAA to address "in a single statute the problem of computer crime, rather than identifying and amending every potential applicable statute affected by advances in computer technology." S. REP. NO. 104-357, at 5. Use of this broad standard "implicitly recognized the necessary involvement of the courts to interpret the scope of the statute in the context of case by case decision-making." Winn, 62 Bus. Law at 1403-04. Just as there was nothing improper with the Ninth Circuit's narrow interpretation of the CFAA in *Nosal*, there would be nothing improper with this Court narrowly interpreting "without authorization" here.

IV. craigslist Embraces the Negative Consequences Resulting from Its Interpretation

In its Brief, 3taps lists a series of troubling consequences that would result from craigslist's interpretation of the CFAA to show why craigslist's interpretation must be rejected. (Brief 14 n.13.) Instead of shying away from these consequences, craigslist embraces them, stating: "there

---

[13] craigslist also seems to misunderstand 3taps' void-for-vagueness argument. (Opp'n 17.) First, 3taps' argument is a statutory construction argument regarding why the statute must be narrowly interpreted – to avoid vagueness concerns. Second, the statute is void-for-vagueness as applied to 3taps because the term "without authorization" (1) does not give 3taps notice that owners of public websites can selectively order Internet users not to access their websites and (2) could lead to the arbitrary and discriminatory enforcement at issue here.

[14] craigslist misleadingly quotes the Amici's academic work in arguing that their literature confirms its position. (Opp'n 22.) Although the Amici have rightly advocated for amendments to the CFAA to make it *less ambiguous*, and to curb expansive interpretations never contemplated by Congress, they have each also called on courts to interpret the CFAA narrowly so as to eliminate such expansive interpretations. *See, e.g.*, Jennifer Granick, *Toward Learning From Losing Aaron Swartz*, cyberlaw.stanford.edu/blog/2013/01/towards-learning-losing-aaron-swartz ("One area for advocacy could be in the Supreme Court, should the issue ever get there. . . . Alternatively, there could be a statutory fix.") (last visited 7/12/2013); 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 (2004) ("[T]he CFAA was never designed to protect information contained on publicly accessible websites.").

is nothing wrong with empowering a computer owner to restrict access to its computers." (Opp'n 16.) craigslist admits, then, that under its CFAA interpretation, owners of cnn.com can send cease-and-desist letters to every journalist, or the DNC can block every registered Republican's IP address, and, if those people access the respective websites, they become criminals.[15]

craigslist also completely fails to address the serious public policy concerns noted by the Court and the Amici. (*See* Brief 13-14; Amici Brief 9-11.) By using criminal law to stifle competition and innovation, craigslist is trying to create dangerous precedent that could threaten the continued openness of the Internet by closing off public non-copyrightable information to Internet users whenever a website owner deems their use of the information undesirable.[16] As noted by 3taps and Amici, the truly unsettling consequences that would result from adopting craigslist's interpretation of the CFAA are even more reason for this Court to adopt 3taps' position.

CONCLUSION

For the foregoing reasons, the Court should dismiss craigslist's CFAA and § 502 claims.[17]

DATED: July 12, 2013

SKADDEN, ARPS, SLATE, MEAGHER & FLOM, LLP

By: /s/ Jack P. DiCanio
Jack P. DiCanio
Attorneys for Defendants
3TAPS, INC. and DISCOVER HOME NETWORK, INC. d/b/a LOVELY

[15] Internet users also could engage in much mischief if craigslist's interpretation were adopted. For example, someone could defame another on his personal website, order the defamed person not to view the website (and block his IP address), thereby creating a CFAA counter claim to a defamation suit. 3taps' narrow interpretation must be adopted to prevent such tactics, especially when felony criminal liability is involved.

[16] As one author has put it, "[t]he Internet is littered with digital carcasses that once built on top [of craigslist]. Their pixelated tombstones are inscribed with one-liners that Craigslist killed access . . . or they were sent a cease-and-desist letter by [craigslist's lawyers] . . . ." Nick Bilton, *Disruptions: Innovations Snuffed Out by Craigslist*, Bits: The Business of Technology, N.Y. Times (July 29, 2012), bits.blogs.nytimes.com/2012/07/29/when-craigslist-blocks-innovations-disruptions/?_r=0 (last visited 7/12/2013).

[17] Factual issues remain only if the Court rules, as a matter of law, that obtaining public information from a public website when the website owner disapproves, violates the CFAA. If the Court were to reach that conclusion, discovery on the CFAA issues would proceed regarding whether 3taps "accesses" craigslist's computers, whether – based on craigslist's prior conduct – it authorized 3taps to scrape information, and whether craigslist experienced actual harm.