ALLEN RUBY (Bar No. 47109)
JACK P. DICANIO (Bar No. 138782)
ABRAHAM TABAIE (Bar No. 260727)
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
Abraham.Tabaie@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 SUPPLEMENTAL BRIEFING 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
Fascimile: (917) 777-3000
James.Keyte@skadden.com
Michael.Menitove@skadden.com
Marissa.Troiano@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 Materials

SUMMARY OF ARGUMENT

This Court should dismiss Plaintiff craigslist, Inc.'s Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and California Comprehensive Computer Access and Fraud Act, Cal. Penal Code § 502, claims alleged in the First Amended Complaint. By definition, an Internet user who accesses public data on a publicly available website *ipso facto* has authorized access to view the website. *See Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011). By making its user-generated classified ads publicly available on its public website, craigslist has authorized anyone to access the public information. craigslist's interpretation of the CFAA empowers private persons or entities to criminalize another's access to public data on a public website—precisely contrary to the principles the Ninth Circuit articulated in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012).

Even if this Court finds that Defendant 3taps' and craigslist's interpretation of the CFAA are both at the very least plausible, making the definition of "without authorization" ambiguous in the specific factual situation at hand, this Court should adopt 3taps' interpretation because: (i) of the rule of lenity; (ii) legislative history confirms that Congress never intended to restrict access to publicly available websites; (iii) 3taps' interpretation avoids constitutional vagueness concerns; and (iv) craigslist's attempt to create a permission-based "public" website is against public policy.

In support of its motion to dismiss the claims of Plaintiff craigslist, Inc. ("craigslist") in its First Amended Complaint ("FAC") alleging violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, and California's counterpart, the Comprehensive Computer Access and Fraud Act, Cal. Penal Code section 502 ("§ 502"), Defendant 3taps, Inc. ("3taps") submits this supplemental brief regarding whether liability under those statutory provisions may be imposed for accessing a publicly available website to view publicly available information.[1]

PRELIMINARY STATEMENT

Each month, more than sixty million Americans visit craigslist's website (craigslist.org) to view hundreds of millions of classified postings, which makes craigslist.org the world's largest online forum for local classified advertising and community discussions. (FAC ¶¶ 1, 24-25.) In terms of "web traffic," craigslist.org is the most viewed website in the United States behind Facebook and Google, with billions of webpage views annually. (*Id.* ¶ 25.)

To view the public information on craigslist.org, *no* passwords or other security clearance is needed, thereby making it a "publicly available website."[2] Yet, notwithstanding that the public exchange information on its website is readily accessible to the public, craigslist alleges that 3taps did not have "permission" to access such information and therefore violated the CFAA and § 502, both of which provide for civil and criminal remedies. Specifically, craigslist alleges that 3taps has violated these statutes because 3taps: (i) ignored a cease-and-desist letter stating that 3taps is "no longer authorized to access, and [is] prohibited from accessing craigslist's website" for any reason;[3] and (ii) used different Internet Protocol ("IP") addresses, and then "anonymous proxies,"

[1] craigslist did not assert CFAA and § 502 claims against Defendant Discover Home Network, Inc., d/b/a/ Lovely. (*Compare* FAC ¶¶ 212-29 (stating that the CFAA and § 502 claims are "as to Defendants 3Taps and Niessen"), *with id.* ¶¶ 208-11 (stating that the California Unfair Competition Claim is "as to all Defendants.").)

[2] *See* www.craiglist.org (allowing any person with an Internet connection to freely access the site); (Order Granting in Part and Denying in Part Mots. to Dismiss at 7 & n.8 (N.D. Cal. Apr. 30, 2013, Dkt. 74) [hereinafter "Apr. 30 Order"].)

[3] (Dkt. 60, Ex. A. to Dec. of Christopher Kao, at 2; *see also* FAC ¶ 132.)

to avoid craigslist's attempts to deny 3taps' access to craigslist.org.[4] (FAC ¶¶ 82-84.) craigslist seeks to bar 3taps from viewing craigslist.org to prevent 3taps from "scraping" (i.e., electronicly copying) the user-generated ads posted on the site. (*See id.* ¶ 77.)[5]

As described below, both as a matter of law and policy, the CFAA does not create a permission-based regime for access to the public data on publicly viewable portions of websites. The courts that have addressed the issue confirm that an unprotected website—e.g., one not requiring a password or code-based restriction to access private or confidential information—by definition grants access to the entire world. The courts implicitly recognize that—irrespective of whether a website owner has attempted to "restrict" a particular user's access to the website—it would make no sense to hold that user civilly or criminally liable under the CFAA for accessing the publicly available content on the website. After all, the website owner permits that very access.

Here, craigslist asks this Court to adopt an approach to the CFAA that Congress never contemplated and that courts have rejected, in an attempt to foster a permission-based Internet *for public websites*. In such a world, owners of public websites can arbitrarily determine *who* can view publicly available information rather than merely prevent access to private or confidential information on a protected website. Whether such privately enforced "de-authorizing" from public websites is directed at competitors, journalists (as in this Court's example (*see* Apr. 30 Order at 8 n.8)), or just those with different points of view, any interpretation of the CFAA that empowers private persons or entities to criminalize another's access to public data on a public website is precisely contrary to the principles the Ninth Circuit articulated in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). Accordingly, this Court should dismiss craigslist's CFAA and § 502 claims.

Even if the Court finds that 3taps' and craigslist's interpretations of the CFAA are both at

[4] Craigslist also argued that 3taps violated the CFAA and § 502 because it accessed craigslist.org in violation of craigslist's terms of use. This Court rejected that argument. (*See* Apr. 30 Order at 5-7.)

[5] Notably, prior to August 2012, 3taps obtained user-generated posts on craigslist via caches maintained by Google, a general purpose website. As alleged in 3taps' counterclaim for violations of the federal antitrust laws, craigslist has caused that content to be unavailable for scraping. (3taps' First Amended Counterclaim ¶¶ 137-46 (Dec. 21, 2012, Dkt. 47).)

the very least plausible, making "without authorization" ambiguous in the specific factual situation at hand, this Court should adopt 3taps' interpretation because: (i) of the rule of lenity; (ii) legislative history confirms that Congress never intended to restrict access to publicly available websites; (iii) 3taps' interpretation avoids constitutional vagueness concerns; and (iv) craigslist's attempt to create a permission-based "public" website is against public policy.

ARGUMENT

I. Settled Law Confirms That the CFAA Does Not Apply to Public Websites

A. Courts Have Rejected the CFAA's Application to Public Websites

As relevant here, the CFAA imposes criminal and/or civil liability on "whoever . . . intentionally *accesses a computer without authorization* or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(c) (emphasis added), (b) (providing for criminal liability), (g) (providing a civil remedy). Congress did not define "without authorization" and therefore the Ninth Circuit has given the term its "'ordinary, contemporary, common meaning.'" *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132-33 (9th Cir. 2009) (citation omitted); *see also United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991).

Specifically, the Ninth Circuit has defined "[a]uthorization . . . as 'permission or power granted by an authority.'" *Brekka*, 581 F.3d at 1133 (holding that "a person who uses a computer 'without authorization' has *no rights, limited or otherwise*, to access the computer in question") (emphasis added) (citing *Random House Unabridged Dictionary* 139 (2001); *Webster's Third International Dictionary* 146 (2002) (further defining authorization as "the state of being authorized" and "authorize" as "to endorse, empower, justify, permit by or as if by some recognized or proper authority"). The issue, then, is whether by making the classified ads on its website publicly available, craigslist has "authorized" the world, including 3taps, to access craigslist.org.

A person who views publicly available information on a publicly available website is no more a criminal under the CFAA than a person "viewing a shop window from a public street." *See* Orin S. Kerr, C*ybercrime's Scope: Interpreting "Access" and "Authorization" in Computer*

Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1620 (2003). craigslist has determined that, because it is a public website providing for the exchange of goods and services, it must keep its window "curtains" open for the public to have access to its public exchange space—without any password or code-based restriction meant to screen users not entitled to private or confidential information. In the parlance of the CFAA, craigslist has given everyone "permission" to access its information simply by virtue of making the user-generated classified ads openly available on craigslist.org.

Case law confirms this. For example, in *Pulte Homes, Inc. v. Laborer's International Union of North America*, 648 F.3d 295 (6th Cir. 2011), the Sixth Circuit held that a home builder, Pulte, had not sufficiently pled an "access without authorization" claim under the CFAA where the defendant union's members bombarded Pulte with calls and emails, clogging its phone lines and overloading Pulte's servers and email system. *Id.* at 299. Pulte's general counsel sent a cease-and-desist letter to the union demanding that it stop encouraging members to contact Pulte and its officers. *Id.* The calls and e-mails continued and Pulte filed suit. *Id.*

The Sixth Circuit adopted *Brekka*'s definition of "without authorization" to mean a person who "uses [the] computer [that] . . . *has no rights, limited or otherwise*, to access the computer in question." *Id.* at 304 (quoting *Brekka*, 591 F.3d at 1133 (emphasis added)). It then held that the union members had the right to call and email Pulte's offices and personnel because "[the union] used unprotected public communication systems." *Id.* That fact alone—the use of a public communications systems—meant that Pulte's allegations failed because "*like an unprotected website*, Pulte's phone and e-mail systems [were] open to the public, so [the union] was authorized to use [them]." *Id.* (internal quotations, original alterations and citations omitted). The court reasoned that because no password or code was necessary to email or call Pulte, the union members did not access Pulte's computers "without authorization." *See id.*

Pulte Homes is dispositive here. Just as the union members accessed the home builder's computers through unprotected public communications systems, 3taps accessed an unprotected public website and obtained information available to anyone with Internet access. And, just as Pulte's cease-and-desist letter did not further its "without authorization" claim, the cease-and-desist

letter craigslist sent to 3taps *cannot* change the fact that craigslist.org was and remains publicly available to anyone with Internet access.

Other district courts also have dismissed CFAA claims against defendants that accessed and used publicly available information on a website, in apparent violation of the website's terms of use. *See Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 933-34 (E.D. Va. 2010); *Koch Indus., Inc. v. Does*, No. 2:10CV1275DAK, 2011 WL 1775765, at *8-9 (D. Utah May 9, 2011). For example, in *Cvent*, the court dismissed a CFAA claim where a publicly available website owner alleged that a competitor hired a third party to "scrape" data from its website. 739 F. Supp. 2d at 930. The website owner argued, similar to craigslist here, that because its terms of use prohibited competitors from *accessing* its website or information, the competitor's access was "without authorization." *Id.* at 932. The court rejected that argument, holding that the scraping did not constitute hacking under the CFAA because the information was on a publicly available website, and therefore the "scraper" had authorized access to it. *Id.* at 933. The court explained that because "anyone, including competitors . . . may access and search information [on the website] at will," and because the website owner did not meaningfully protect its information through password protection, for example, the competitor was not "without authorization" and could scrape data from the site without violating the CFAA. *Id.* at 932-34.

Similarly, in *Koch Industries*, the court dismissed a CFAA claim alleging that a climate change group engaged in "unauthorized access" of a public website. 2011 WL 1775765, at *9. The group created a website with content similar to that on the plaintiff's site, as well as a link to the actual website. *Id.* at *1. The court held, in part, that alleging unwarranted use of publicly available information was insufficient to state a claim under the CFAA where the website owner required no "individualized grant of access," such as a login or password for that information. *Id.* at *8 (quoting *Cvent*, 739 F. Supp. 2d at 932). The court further noted that adopting the website owner's theory of liability—"that is, any use of its website's content of which [the owner did] not approve" in its terms of use or otherwise—"could expose a political critic to criminal prosecution," which would be a result "clearly beyond Congress' intent in passing the CFAA." *Id.* at *9; *see also*

Loud Records LLC v. Minervini, 621 F. Supp. 2d 672, 678 (W.D. Wis. 2009) ("[B]ecause the files that plaintiffs allegedly accessed were accessible by the public, any allegation that the computer should be considered protected or that plaintiffs acted without authorization is tenuous at best.").

These cases confirm that by making its user-generated classified ads publicly available on its website, craigslist has authorized anyone to access them even though it has purported to selectively "de-authorize" access. This Court should follow these decisions and hold that, by definition, an Internet user who accesses a publicly available website with no password or code-based restrictions *ipso facto* has authorized access to view the website.

B. The Principles Outlined in *Nosal* Dictate That Public Data on Publicly Available Websites Are Beyond the Scope of the CFAA

The underlying logic of the Ninth Circuit's analysis in *Nosal* strongly suggests that the CFAA does not apply to public data on public websites.[6]

First, the Ninth Circuit rejected the government's interpretation of the CFAA because it "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." *Nosal*, 676 F.3d at 857. The court explained that the CFAA was intended to target computer hacking and "[i]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions – which may well include everyone who uses a computer – we would expect it to use language better suited to that purpose." *Id*.

Second, in cautioning against broadly interpreting the CFAA, the court held that "[b]asing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." *Id*. at 860. In fact, a broad interpretation is more dangerous in the CFAA context because a website owner retains the right to change its terms at any time without notice.[7] *Id.* at 862.

[6] This Court noted that *Nosal* "did not seize on th[e] opportunity to highlight a possible distinction between public and non-public information." (Apr. 30 Order at 8 n.8.) But the *Nosal* Court did not have that opportunity because the defendant was accused of accessing confidential, proprietary information. *See Nosal*, 676 F.3d at 856.

[7] Lest one think this is a hypothetical proposition, here, craigslist relied on a change in its Terms of Use to claim that it is the exclusive licensee of all its users' posts. (Apr. 30 Order at 11-12.)

craigslist's attempt to impose CFAA liability on 3taps raises these same concerns. craigslist's interpretation would subject any and all Internet users to potential criminal liability for merely receiving data transmitted over the Internet when it violates privately created access restrictions. *See id.* at 861 (expressing concern that access to public information could be criminalized by a company). Under the CFAA, no substantive distinction exists between a public website owner selectively restricting access to a site completely and restricting use of a site for a certain purpose.[8]

C. craigslist's Attempt to Revoke 3taps' Access Is a Use Prohibition Masquerading as an Access Ban

Nosal noted that appropriate interpretations of the CFAA "maintain [the CFAA's] focus on hacking rather than turning it into a sweeping Internet-policing mandate." 676 F.3d at 858. The court therefore held that "the CFAA does not extend to violations of use restrictions." *Id.* at 863.

Because craigslist.org is a public website, craigslist, by definition, cannot be concerned with mere access to its site; in fact, its business model requires such access to make its public exchange space successful. Faced with the dilemma of having a public website that allows users to exchange goods and services, but wanting to restrict "access" to certain users, craigslist does the predictable: attempt to block those whose *use* it finds objectionable under the guise of denying "access." "But simply denominating limitations as 'access restrictions' does not convert what is otherwise a use policy into an access restriction." *Wentworth-Douglass Hosp. v. Young & Novis Prof'l Ass'n*, No. 10–cv–120–SM, 2012 WL 2522963, at *4 (D.N.H. June 29, 2012).

[8] Indeed, such distinctions lead to arbitrary and absurd results. For example, as this Court noted, a news outlet could merely send letters purporting to restrict access by any other news outlet's employees and block their IP addresses. If an employee of a competitor were to view the news outlet's website, he could face criminal liability under craigslist's interpretation. (*See* Apr. 30 Order at 8 n.8.) Similarly, the Democratic National Committee could send an email restricting access by every registered Republican. If a registered Republican visited http://www.democrats.org, he could face criminal liability under craigslist's interpretation. *See Koch Indus.*, 2011 WL 1775765, at *9. Lastly, if someone received an email from a friend that a new website, www.dontvisitme.com, has some beautiful pictures posted, but the website's homepage clearly and unambiguously states that no one is allowed to click on the links to view the pictures, that person could face criminal liability for viewing the pictures. *See* Orin S. Kerr, *Investigating and Prosecuting 21st Century Cyber Threats*, United States House of Representatives Subcommittee on Crime, Terrorism, Homeland Security and Investigations (Mar. 13, 2013).

Here, craigslist is only blocking 3taps, its competitor, because of the way 3taps intends to *use* information, which *Nosal* held is not a violation of the CFAA. (*See, e.g.*, FAC ¶¶ 1-8.) Indeed, *Nosal*'s distinction between "use" and "access" restrictions would be superfluous if craigslist could blacklist those engaging in a use it finds objectionable by not allowing "access" to its public site.

II. At Minimum, the Phrase "Without Authorization" Is Ambiguous As Applied to a Publicly Available Website, And Must Be Interpreted Narrowly

At the least, 3taps' interpretation of access "without authorization" is plausible. In the same way that the Ninth Circuit found the definition of "exceeds authorized access" ambiguous, *see Nosal*, 676 F.3d at 856-57, as applied here, "access[] . . . without authorization" is likewise ambiguous. *See EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir. 2001) (meaning of "without authorization" "proven to be elusive"), *superseded by statute on other grounds as recognized in Cenveo Corp. v. CelumSolutions Software GMBH & Co KG*, 504 F. Supp. 2d 574, 581 n.6 (D. Minn. 2007).[9]

Here, accessing craigslist.org "without authorization" could be interpreted in at least two ways. *First*, as 3taps contends, it had authorization to access craigslist.org because, by making available public data on a publicly available website, craigslist gave access to everyone and has no authority to selectively choose who looks at its website. *Second*, under craigslist's interpretation, it has the authority to single out users and prohibit access to public portions of its site. Under these facts, if the Court determines that both interpretations of the CFAA are at the very least plausible, the definition of "without authorization" would therefore be ambiguous.

[9] *See also* Kerr, 78 N.Y.U. L. Rev. at 1623-24 ("[W]ho and what determines whether access is authorized, and under what circumstances? Can a computer owner set the scope of authorization by contractual language? Or do these standards derive from the social norms of Internet users? The statute[ ] [is] silent on these questions. . . ."). Indeed, courts define the term "without authorization . . . based upon analogizing the concept . . . as to computers to a more familiar and mundane predicate presented in or suggested by the specific factual situation at hand." *United States v. Drew*, 259 F.R.D. 449, 460 (C.D. Cal. 2009).

A. The Rule of Lenity Requires Adoption of 3taps' Interpretation of "Without Authorization"

"The rule of lenity requires penal laws [like the CFAA] to be construed strictly." *Nosal*, 676 F.3d at 863 (internal quotation marks and citations omitted). "'[W]hen [a] choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before [the Court] choose[s] the harsher alternative, to require that Congress should have spoken in language that is clear and definite.'" *Id.* (first alteration in original) (quoting *Jones v. United States*, 529 U.S. 848, 858 (2000)). "If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [defendant] engaged, then [the court] must choose the interpretation least likely to impose penalties unintended by Congress." *Id.* (first alteration in original) (internal quotation marks and citation omitted).

As the "unauthorized access" language in the CFAA is currently drafted, Internet users, including the sixty million monthly craigslist.org users, do not have fair notice that Congress intended to criminalize viewing a public website in the event the website's owner instructs a person not to view it. This is because the plain language of the CFAA does not clearly create liability in such a circumstance. *See id.* Therefore, to avoid sweeping liability, the rule of lenity requires the Court to interpret the CFAA to mean that Internet users always have "authorized access" to public information on a publicly available website. *See id.* at 862-63.

B. Congress Did Not Intend for the CFAA to Apply to Public Information on Publicly Available Websites

The CFAA's lengthy legislative history confirms that Congress was interested in protecting *private* and *confidential* information, not public information on publicly available websites. Recognizing the explosion of computer use and its implications for the public, private, governmental, and personal sectors, Congress believed computers "brought a great many benefits . . . to all of our lives," but also posed a great risk to our privacy and confidentiality. S. Rep. No. 99-432, at 1-2 (1986); *see also* H.R. Rep. No. 98-894, at 10 (1984). In passing the first iteration of the CFAA in 1984, Congress noted that the potential for privacy abuse by a specific

subset of computer users—"hackers"—threatened the viability of computer systems in daily life. H.R. Rep. No. 98-894, at 10.

Thereafter, the CFAA has grown in scope, but not in its purpose to subvert unauthorized activity breaching *privacy* and *confidentiality* that results in harms such as damaged information or the transmission of viruses. *See* H.R. Rep. No. 98-894, at 9 (realizing that "criminals possess the capability to access and control high technology processes vital to our everyday lives which has spurred the recent alarm over computer-related crime"); 142 Cong. Rec. S10,889, 10,890 (1996) ("The . . . Act would close these loopholes[,] outside hackers . . . and malicious insiders face criminal liability for intentionally damaging a computer."). Glaringly absent from this legislative history is any indication that the CFAA was meant to apply to one's access to public data on publicly available websites.

Indeed, when a website is publicly accessible—and especially when the information at issue is otherwise publicly available—then privacy and confidentiality concerns are not at issue, and the CFAA is not applicable. Congress has compared violations of the CFAA to the physical crime of "'breaking and entering.'" H.R. Rep. No. 98-894, at 12. But Congress never suggested that the CFAA should apply to Internet users (or publicly available information) because public data on public websites, by nature of being public, require no access authorization, or "breaking and entering." *See* S. Rep. No. 99-432, at 9 ("the offender obtains . . . information as to how to break into that computer system"); S. Rep. No. 104-357, at 9 (1996) (explaining that insiders who are authorized to access a computer face criminal liability only for intentionally inflicted damage whereas outside hackers may be punished for causing damage).

Expanding the CFAA to apply to the public information on public websites flies in the face of its legislative history. The statute essentially would then apply to all forms of information and every website and make the CFAA limitless in scope and application. The legislative history warns against this interpretation. When Congress amended the CFAA in 1996, Senator Leahy specifically articulated that the statute's premise "is privacy protection." 142 Cong. Rec. S10,889. And this premise has been reiterated time and again. *See* S. Rep. No. 104-357, at 7 ("[T]he

premise of this subsection is privacy protection.") (citation omitted).[10]

When congressional intent is lacking, the CFAA should not be applied to curtail the very benefits that it was enacted to protect. *See Nosal*, 676 F.3d at 858 n.5. In passing the CFAA, Congress sought to protect the many benefits that computer systems offer to our lives. S. Rep. No. 99-432, at 2. One such benefit is the vast amount of publicly available data on public websites that allow users to innovate and create new technologies and ideas. Absent from the CFAA's legislative history is any indication that the statute should apply to the dissemination of public information on a publicly available website.

C. To Avoid Constitutional Infirmity, This Court Must Adopt 3taps' Interpretation of "Without Authorization"

Assuming that craigslist's and 3taps' interpretations of the CFAA in the context of public data on publicly available websites are both "fairly possible," this Court must choose the interpretation that does not "raise serious constitutional problems." *See INS v. St. Cyr.*, 533 U.S. 289, 299-300 (2001). Here, that requires the Court to choose 3taps' interpretation because applying the CFAA to persons who access publicly available websites would render the CFAA unconstitutionally vague, in violation of a criminal defendant's due process rights.

As the Ninth Circuit recognized, the CFAA must be interpreted consistently in the criminal and civil contexts, which necessarily requires this Court to interpret the CFAA in a way that does not run afoul of a criminal defendant's due process rights. *See Brekka*, 581 F.3d at 1134. To ensure that the CFAA does not raise due process concerns, it must be interpreted: (1) to "provide the kind of notice that will enable ordinary people to understand what conduct it prohibits" and (2) so that it does not authorize or "even encourage arbitrary and discriminatory enforcement." *City of Chicago v. Morales*, 527 U.S. 41, 56 (1999) (citation omitted).

If the CFAA were interpreted to apply to persons obtaining information from publicly

[10] *See also* S. Rep. No. 99-432, at 6 ("The premise . . . will remain the protection, for privacy reasons, of computerized credit records and computerized information."); 142 Cong. Rec. S10,889 ("This legislation will help safeguard the privacy . . . of our national computer systems and networks.").

available websites, the phrase "without authorization" would be so vague and sweeping that it would not provide an ordinary person with sufficient notice as to what conduct is prohibited. As an initial matter, an ordinary Internet user would not understand what "without authorization" means in the context of a public website that does not require a password or impose a code-based restriction to protect private or confidential information. In fact, an ordinary person would not understand that he could be "without authorization," and thus engaging in criminal conduct, should a website merely load in his or her Internet browser—as a publicly available website would—upon the person entering a URL or clicking on a hyperlink. That an owner of a publicly available website tells a specific person or set of persons not to view the website, whether through a cease-and-desist letter or otherwise, does not bring any clarity to the phrase "without authorization." The problem is that notwithstanding the website owner's pronouncements, the user still can access the public data on the site. Indeed, but for the website owner transmitting the website's public information to the person's computer (i.e., granting authorization), the person would be unable to view the information. (*See* discussion *infra* p.13 n.12.)

Similarly, in blocking a person's IP address, a website owner is not "de-authorizing" access. Rather, the website owner has merely blocked access from a specific IP address.[11] Because the site remains available for that person to view from another computer or location with a different IP address, an ordinary person would not understand a blocked IP address to mean that he *personally* is "without authorization."

Thus, to save the CFAA from potential constitutional infirmities, the Court should interpret the phrase "without authorization" as not applying to the accessing of publicly available websites. An interpretation of the CFAA that empowers private entities to criminalize access to public data on a public website is precisely contrary to the principles articulated in *Nosal* and could create federal criminal liability for untold scores of unsuspecting Internet users. *See* 676 F.3d at 860.

[11] Internet users innocuously use multiple IP addresses for different devices and while connecting to different wireless networks. There is nothing improper or unlawful about switching IP addresses and thereby avoiding IP address blocking.

D. craigslist's Attempt to Create a Permission-Based "Public" Website Under the CFAA Raises Serious Policy Concerns

Policy considerations weigh heavily in favor of following those courts that have rejected the CFAA's application to public websites and adopting 3taps' interpretation of the CFAA. Since its inception, the Internet "has been premised on a culture of openness—*where access has been presumed to be the de facto rule*, with individual actors being given the choice of 'opting out' by *adopting bright-line* exclusionary techniques (such as encryption, passwords, authentication techniques and the like)." Shyamkrishna Balganesh, *Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass*, 12 Mich. Telecomm. & Tech. L. Rev. 265, 289-90 (2006) (emphasis added).

craigslist, however, would have this Court interpret the CFAA in a way that would render public information on public websites subject to selective private censorship based on *who* can and cannot access such information. In effect, craigslist seeks a CFAA that no longer is aimed at protecting against "hackers" but rather would enable website owners to criminalize viewing public information on public websites by anyone they decide to blacklist. But a legal standard that invites owners of public websites to selectively criminalize the behavior of potentially anyone who uses a computer is precisely what *Nosal* warned against. *See Nosal*, 676 F.3d at 859, 860-61 (A "broad construction of the CFAA" would affect "everyone . . . who uses a computer, smart-phone, iPad, Kindle, Nook, X-box, Blu–Ray player or any other Internet-enabled device" and potentially "millions of unsuspecting individuals would find that they are engaging in criminal conduct.").

Like public websites, a store window is either open or shut—there is no in between. craigslist, by choice, keeps the curtains to its storefront open at all times so that any passerby can look inside. Unwilling to exercise the power to close the curtains to the public, including 3taps, craigslist instead in effect polices the *public* sidewalk, which it certainly does not have the power to do under any law, including the CFAA.[12] *See Pulte Homes*, 648 F.3d at 304. Any contrary view of

[12] Although the "open window" metaphor is one way to conceptualize publicly available websites on the Internet as a physical "place," any cyberspace-as-a-place metaphor, including this one, is too restrictive because the way in which computers communicate when gathering information on a publicly available website cannot be analogized to space. When a user clicks on a link, the user's *(cont'd)*

"authorized" access to public websites would create a particularly dangerous "public" Internet environment policed by private website owners. A website owner could selectively "de-authorize"—backed by threatened criminal exposure—any person it did not wish to permit to view its public website. Such a permission-based regime for public websites could implode the basic functioning of the Internet itself, which is premised on the freedom of public search. Moreover, as a vehicle for targeting *who* may visit public websites, craigslist's permission-based view of authorization under the CFAA also raises serious First Amendment implications—e.g., private companies could use the CFAA to deter or limit free speech and assembly.[13] This certainly is not a policy *Nosal* or any other court encourages.[14]

(cont'd from previous page)
computer sends a request to the server on which the desired information resides. *See* Mark A. Lemley, *Place and Cyberspace*, 91 Cal. L. Rev. 521, 523-24, 529 (2003). "That computer decides whether or not to respond favorably to the query. It honors the request by sending a copy of the document to the user's computer . . . ." *See* Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 Berkeley Tech. L. J. 561, 568-69 (2001). Thus, analyzing this case, or similar cases, under an auspice that cyberspace is similar to a physical place will inevitably lead to unwanted legal implications, including inaccurately "creating [laws] of stunning breadth." Lemley, 91 Cal. L. Rev. at 529. Therefore, for publicly available websites, there is truly no "access," just two computers communicating. Thus, for public data on public websites, there can be no unauthorized access at all.

[13] If, for example, an owner of a publicly available news website sent cease-and-desist letters ordering a group of people who were critical of a journalist's article to stop using its website, and the group continued to criticize the author of the article on the website, those speakers could be subject to criminal liability under craigslist's interpretation of the CFAA. In this sense, where a vague statute "'abut(s) upon sensitive areas of basic First Amendment freedoms,' it 'operates to inhibit the exercise of (those) freedoms.'" *See Grayned v. City of Rockford*, 408 U.S. 104, 108-09 (1972) (citations omitted). Under even a more relaxed content-neutral standard, such a restriction must be shown to serve an important state interest, and the "incidental restriction on alleged First Amendment freedoms [must be] no greater than is essential to the furtherance of that interest." *United States v. O'Brien*, 391 U.S. 367, 377 (1968). Under this example, the CFAA would prohibit the group's ability to speak, and to use the website's comment board as a place to assemble. Because the news media's conduct "is not constitutionally entitled to protection," applying the CFAA broadly to such cases threatens to destabilize the balance struck by current First Amendment jurisprudence. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 Md. L. Rev. 320, 365 (2004).

[14] Enabling website owners to selectively deny access to publicly available websites is also bad policy from a competition perspective. As this Court itself observed, there is something troubling about imposing CFAA liability on a competitor accessing another competitor's public website in violation of the website owner's privately declared de-authorization of access (by cease-and-desist letter or otherwise). (Apr. 30 Order at 8 n.8.) As 3taps and Padmapper have alleged, such conduct by a competing website owner is overtly anticompetitive absent a legitimate concern *(cont'd)*

CONCLUSION

For the foregoing reasons, 3taps respectfully requests that the Court dismiss craigslist's CFAA and § 502 claims alleged in the First Amended Complaint.

DATED: June 7, 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

(cont'd from previous page)
regarding harm to its servers. *See* Galbraith, 63 Md. L. Rev. at 333 ("[I]t appears that these owners of publicly accessible websites may be less concerned with actual harm to their computer system and more interested in finding a way to protect themselves from increased competition."). Indeed, this Court's intuition highlights that craigslist's primary, if not sole, criterion for sending out numerous (if not hundreds or more) cease-and-desist letters is the use that the targeted person or company makes of publicly accessible, user-generated posts. In essence, invocation of the CFAA is part of craigslist's broader scheme to be to scare off potential innovators and competitors. *See* O'Rourke, 16 Berkeley Tech. L. J. at 607-08 ("The Internet may be one of the few, if not the only, contexts in which it may be a viable strategy for a monopolist to create a barrier to entry by controlling the flow of its own product and pricing information.").