IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

CRAIGSLIST INC.,

Plaintiff,

v.

3TAPS INC. ET AL.,

Defendants.
_____/

No. CV 12-03816 CRB

ORDER DENYING MOTION TO DISMISS CAUSES OF ACTION 13 AND 14 IN PLAINTIFF'S FIRST AMENDED COMPLAINT

Defendant 3taps, Inc. ("3Taps") has moved to dismiss Plaintiff craigslist, Inc.'s ("Craigslist") claims under the Computer Fraud and Abuse Act (CFAA) and its state-law counterpart, California Penal Code section 502. The CFAA imposes civil and criminal liability on "whoever . . . intentionally accesses a computer without authorization . . . and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(c).

The dispute here is limited to whether 3Taps accessed Craigslist's computers "without authorization." 3Taps asks this Court to hold that an owner of a publicly accessible website has no power to revoke the authorization of a specific user to access that website. However compelling 3Taps' policy arguments, this Court cannot graft an exception on to the statute with no basis in the law's language or this circuit's interpretive precedent. Accordingly, the Court DENIES 3Taps' motion.

//

I. BACKGROUND

Craigslist operates a well-known and widely-used website that allows users to submit and browse classified advertisements. First Am. Compl. (dkt. 35) ¶¶ 1, 25, 28-34. According to the First Amended Complaint ("FAC"), "[m]ore than 60 million Americans visit craigslist each month, and they collectively post several hundred million classified ads each year." Id. ¶ 25. Craigslist's service is organized by geographic area, and within each given area by types of products and services. Id. ¶ 29. Craigslist provides ancillary features, such as anonymous email forwarding, to support its classified ad service. E.g., id. ¶ 34.

Defendant 3Taps aggregates and republishes ads from Craigslist. Id. ¶¶ 63, 65, 99, 104, 112. Craigslist alleges that 3Taps copies (or "scrapes") all content posted to Craigslist in real time, directly from the Craigslist website. Id. ¶¶ 3, 78-80. 3Taps markets a "Craigslist API"[1] to allow third parties to access large amounts of content from Craigslist, id. ¶¶ 3, 5, 64, and also operates the website craiggers.com, which "essentially replicated the entire craigslist website," id. ¶ 65, including "all of craigslist's posts," id. ¶ 68.

After learning about 3Taps' scraping activities, Craigslist took two relevant steps to stop it. First, it sent a cease and desist letter to 3Taps, informing it that "[t]his letter notifies you that you and your agents, employees, affiliates, and/or anyone acting on your behalf are no longer authorized to access, and are prohibited from accessing craigslist's website or services for any reason." FAC ¶ 132; Hennessy Letter, Kao Decl. Ex. A (dkt. 60-2) at 3. Second, Craigslist configured its website to block access from IP addresses[2] associated with 3Taps. FAC ¶¶ 80-81. 3Taps bypassed that technological barrier by using different IP addresses and proxy servers to conceal its identity, and continued scraping data. FAC ¶¶ 82-84.

Craigslist sued 3Taps (and other defendants not relevant to this motion), alleging in relevant part that 3Taps' scraping activities violated the CFAA and its state-law analogue,

[1] An Application Programming Interface (API) is a set of programming instructions and standards to allow third parties to develop software that draws information from, or otherwise interacts with, a website, program, or database.

[2] An IP address is an identification number for a device that accesses the internet.

Cal. Penal Code § 502. 3Taps moved to dismiss those claims, and this Court concluded that Craigslist's allegations that 3Taps ignored the cease-and-desist letter and circumvented Craigslist's IP blocking efforts stated a claim under the CFAA. Id. at 5-8.[3]

The Court also noted that "[t]he parties have not addressed a threshold question of whether the CFAA applies where the owner of an otherwise publicly available website takes steps to restrict access by specific entities." Order at 7 n.8. 3Taps requested that the Court accept supplemental briefing on that legal issue from both sides. See Joint Case Mgmt. Statement, dkt. 78, at 9-10. The Court granted 3Taps' request and, with the benefit of further briefing from 3Taps, Craigslist, and amici curiae, now turns to the merits of that narrow statutory interpretation question.

II. LEGAL STANDARD

A motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of the claims alleged in a complaint. Ileto v. Glock, Inc., 349 F.3d 1191, 1199-1200 (9th Cir. 2003). "Detailed factual allegations" are not required, but the Rule does call for sufficient factual matter, accepted as true, to "state a claim to relief that is plausible on its face." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. In determining facial plausibility, whether a complaint states a plausible claim is a "context-specific task that requires the reviewing court to draw on its judicial experience and common sense." Id. at 679. Allegations of material fact are taken as true and construed in the light most favorable to the non-moving party. Cahill v. Liberty Mut. Ins. Co., 80 F.3d 336, 337-38 (9th Cir. 1996).

//

//

//

[3]The Court rejected Craigslist's argument that 3Taps' alleged violation of Craigslist's "Terms of Use" stated a claim under the CFAA, and this Order does not revisit that conclusion.

III. DISCUSSION

A. The Plain Language of the Statute

The CFAA[4] imposes criminal penalties on any person who, among other prohibitions, "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). A "protected computer" is a computer "used in or affecting interstate or foreign commerce or communication." Id. § 1030(e)(2). "Any person who suffers damage or loss by reason of a violation of [the CFAA] may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief," provided that certain factors, not in dispute for the purpose of this motion, are satisfied. Id. § 1030(g).[5]

The parties agree that 3Taps intentionally accessed Craigslist's protected computer and obtained information from it. The only dispute is whether 3Taps did so "without authorization." 3Taps' argument starts out on firm statutory ground: "[B]y making the classified ads on its website publicly available, craigslist has 'authorized' the world, including 3Taps, to access craigslist.org." Supp. Br. at 4; Reply at 4; see also Pulte Homes, Inc. v. Laborer's Intern'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (public presumptively authorized to access "unprotected website"). That makes sense.

But it does not answer the question here, which is whether Craigslist had the power to revoke, on a case-by-case basis, the general permission it granted to the public to access the information on its website.[6] Craigslist certainly thought it had such authority, and sought to

---

[4]The parties agree that the CFAA provision at issue here and California Penal Code § 502 are identical for purposes of this motion. See 3Taps MTD at 12 (citing Multiven, Inc. v. Cisco Sys., Inc., 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010)); Opp'n to 3Taps MTD at 10 n.2 (same).

[5]Although this is a civil case, the rule of lenity applies here because conduct that triggers civil penalties under the relevant provision of the CFAA would also be a criminal violation. See United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (en banc); United States v. Thompson/Center Arms Co., 504 U.S. 505, 517-18 & n.10 (1992) (plurality) (citing Crandon v. United States, 494 U.S. 152, 168 (1990)); United States v. Santos, 553 U.S. 507, 523 (plurality) (2008) (citing Thompson/Center).

[6]At oral argument on this motion, counsel for 3Taps relied heavily on Pulte, arguing that it conclusively resolved the issue presented here. In Pulte however, the plaintiff never argued that it had revoked the defendant's authorization to access its computers. See 648 F.3d at 304 ("[Plaintiff] does not even allege that one or several calls or e-mails would have been unauthorized. Its complaint thus

exercise it through its cease-and-desist letter and IP blocking measures. 3Taps says that Craigslist had no power to "de-authorize" anyone, but it cannot point to any language in the statute supporting that conclusion.

In fact, the statutory context and the Ninth Circuit's interpretation of the phrase "without authorization" both cut against 3Taps' argument. One way to accomplish the result that 3Taps urges–prohibiting computer owners from revoking "authorization" to access public websites–would be to restrict the kind of information protected by the CFAA. For example, Congress might have written § 1030(a)(2) to protect only "nonpublic" information. A neighboring provision in the CFAA includes that very modifier, and prohibits access without authorization to "nonpublic" government computers. See 18 U.S.C. § 1030(a)(3). Another adjacent provision applies only to certain kinds of financial information. See § 1030(a)(2)(A). Congress apparently knew how to restrict the reach of the CFAA to only certain kinds of information, and it appreciated the public vs. nonpublic distinction–but § 1030(a)(2)(c) contains no such restrictions or modifiers.

Congress also included in a similar statute a restriction like the one 3Taps proposes here. The Stored Communications Act includes a provision that 3Taps describes as "almost identical" to the CFAA. See 18 U.S.C. § 2701(a) ("[W]hoever–intentionally accesses without authorization a facility through which an electronic communication service is provided; . . . ."). 3Taps cites an Eleventh Circuit case interpreting that provision, Snow v. DirecTV, Inc., 450 F.3d 1314 (11th Cir. 2006), and argues that the reasoning from Snow applies here. Reply at 5-6. But 3Taps does not mention that Congress included in the SCA language stating that "[i]t shall not be unlawful under this [law] for any person-(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the

---

amounts–at most–to an allegation that [the defendant] exceeded its authorized access.") Thus, when the Pulte court observed in dicta that the public was authorized to access an unprotected website, it was not reaching the follow-up issue never argued by the plaintiff in that case: whether the computer owner could revoke that general authorization on a case by case basis, making further access by a banned entity "without authorization."

general public." 18 U.S.C. § 2511(2)(g) (emphasis added). No such language appears in the CFAA provision at issue here.

And, the Ninth Circuit's interpretation of the CFAA's phrase "without authorization" confirms that computer owners have the power to revoke the authorizations they grant. In LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009), an employee logged into his work computer with valid credentials provided by his employer and e-mailed valuable documents from the employer's computer to the employee's personal e-mail address for use in his own competing business. Id. at 1129-30, 1134.

Turning first to the "plain language" of the statute, the court approvingly cited the Second Circuit's conclusion that the phrase "without authorization" has an unambiguous, plain meaning. Id. at 1132-33 (citing United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991)). The "ordinary, contemporary, common meaning" of the word "authorization" is "permission or power granted by an authority." Id. at 1133. The court also distinguished access "without authorization" from use that "exceeds authorized access," which is a separate provision in the CFAA. Id. "A person who uses a computer 'without authorization' has no rights, limited or otherwise, to access the computer in question." Id.

The court rejected the employer's invitation to read into the word "authorization" a requirement that the employee be acting as an agent of the employer at the time of access. The employer's argument was that the basis of the employee's authorization was his status as an agent, and a breach of the duty of loyalty under common law agency principles terminated the agency relationship. Id. at 1134.

Noting that the CFAA was a criminal statute and that the rule of lenity applied, the court emphasized that the CFAA made no mention of state law duties of loyalty, and "[t]he plain language of the statute . . . indicates that 'authorization' depends on actions taken by the employer." Id. at 1135 (emphasis added). Accordingly, "a person uses a computer 'without authorization' under [the CFAA] when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer

without any permission) or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway." Id. (emphasis added).

Here, under the plain language of the statute, 3Taps was "without authorization" when it continued to pull data off of Craigslist's website after Craigslist revoked its authorization to access the website. As the "ordinary, contemporary, common meaning" of the word indicates, and as Brekka expressly held, "authorization" turns on the decision of the "authority" that grants–or prohibits–access. In Brekka, the authority was the employer. Here, it is Craigslist. Craigslist gave the world permission (i.e., "authorization") to access the public information on its public website. Then, just as Brekka instructed that an "authority" can do, it rescinded that permission for 3Taps. Further access by 3Taps after that rescission was "without authorization."

B. The Ninth Circuit's Access vs. Use Distinction

3Taps tries to muddy the waters by plucking a few stray quotes from a more recent Ninth Circuit case, United States v. Nosal, 676 F.3d 854 (9th Cir. 2012), and arguing that the Ninth Circuit has significantly narrowed the reach of the CFAA's broad language. In Nosal, the government brought criminal charges under the CFAA against David Nosal for encouraging corporate employees to access confidential information on their employer's computer system and to transfer the information to Nosal. Id. at 856. The employees were authorized to access the information but violated a corporate policy by disclosing it to Nosal. Id. The Ninth Circuit held that the phrase "'exceeds authorized access' in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its use." Id. at 863-64.

The Ninth Circuit's thoughtful discussion of the dangers of criminalizing violations of private use policies adds little here because in Nosal the court was considering scenarios where a computer user has some legitimate access to the protected computer in the first place. In that context, criminalizing violations of private use policies "that most people are only dimly aware of and virtually no one reads or understands"–and that are subject to

change at any time–presents serious notice concerns and also threatens to "transform whole categories of otherwise innocuous behavior into federal crimes." Id. at 860-61.

The calculus is different where a user is altogether banned from accessing a website. The banned user has to follow only one, clear rule: do not access the website. The notice issue becomes limited to how clearly the website owner communicates the banning. Here, Craigslist affirmatively communicated its decision to revoke 3Taps' access through its cease-and-desist letter and IP blocking efforts. 3Taps never suggests that those measures did not put 3Taps on notice that Craigslist had banned 3Taps; indeed, 3Taps had to circumvent Craigslist's IP blocking measures to continue scraping, so it indisputably knew that Craigslist did not want it accessing the website at all.

Nor does prohibiting people from accessing websites they have been banned from threaten to criminalize large swaths of ordinary behavior. It is uncommon to navigate contemporary life without purportedly agreeing to some cryptic private use policy governing an employer's computers or governing access to a computer connected to the internet. In contrast, the average person does not use "anonymous proxies" to bypass an IP block set up to enforce a banning communicated via personally-addressed cease-and-desist letter. See Compl. ¶ 84. Thus, a meaningful distinction exists between restricting uses of a website for a certain purpose and selectively restricting access to a website altogether.

3Taps says that Craigslist's purported "de-authorization" was really just a creatively-labeled use restriction, because Craigslist banned 3Taps based on Craigslist's disapproval of how 3Taps was using the information from Craigslist's website. It is true that "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). Thus, purported "de-authorizations" buried in a website's terms of service may turn out to be use restrictions in disguise, and would present the same problems identified by the Nosal court. See Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932-34 (E.D. Va. 2010); Koch

Indus., Inc. v. Does, No. 2:10CV1275DAK, 2011 WL 1775765, at *8-9 (D. Utah May 9, 2011).

But that is not this case. Here, it is possible to distinguish the kind of restriction in place from Craigslist's motivation for imposing that restriction. Craigslist made a complete access restriction when it told 3Taps that it could not access Craigslist's website "for any reason," and then put in place a technological barrier designed to completely cut off 3Taps' ability to view the site. That it did so because of how 3Taps used Craigslist's information is true, but beside the point, because as discussed above, true access restrictions do not present the same notice and breadth issues that come with the criminalization of use policies.

C. Other Statutory Interpretation Tools

3Taps' remaining arguments all rest to some degree on the premise that the CFAA is ambiguous and could be reasonably interpreted as prohibiting computer owners from selectively revoking authorization to access public information on a public website. As discussed above, the plain language of the statute, as interpreted by the Ninth Circuit in Brekka, admits of no such interpretation, and so these points carry little weight with this Court.

Rule of Lenity: Where a criminal statute suffers from a "grievous ambiguity," the law should be interpreted to avoid imposing unintended penalties. Muscarello v. United States, 524 U.S. 125, 138 (1998); Nosal, 676 F.3d at 863. As the Supreme Court has recognized, however, most statutes are technically ambiguous, and "[t]he mere possibility of articulating a narrower construction does not by itself make the rule of lenity applicable." Muscarello, 524 U.S. at 138. The rule does not create ambiguity where, as here, the plain meaning of the statute indicates that a penalty applies.

Constitutional Avoidance and Vagueness: Similarly, where two "plausible" interpretations of a statute present themselves, and one presents serious constitutional doubts as to the validity of the statute, the constitutional avoidance canon says that a court should select the interpretation that avoids the constitutional problem. E.g., Milavetz, Gallop & Milavetz, P.A. v. United States, 559 U.S. 229, 239 (2010). Here, 3Taps cannot invoke that

cannon for two reasons: First, for the reasons already stated, its alternative interpretation is not plausible.

Second, no serious constitutional doubts accompany the Court's interpretation of the CFAA. 3Taps says that if the CFAA assigns criminal penalties to a computer owner's selective restriction on access to an otherwise public website, the statute becomes "so vague and sweeping that it [does] not provide an ordinary person with sufficient notice as to what conduct is prohibited." Supp. Br. at 12. Supposedly, that is because "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 code-based restrictions to protect private or confidential information." Id.

The relevant question is whether the 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." Holder v. Humanitarian Law Project, 130 S. Ct. 2718-19 (2010) (internal quotation marks omitted). Here, 3-Taps (1) received a personally-addressed cease-and-desist letter stating that it could not access Craigslist's website "for any reason"; (2) discovered that it could no longer access the website at all from its IP addresses; and (3) was sued for continuing to access that website after circumventing the IP restrictions. A person of ordinary intelligence would understand Craigslist's actions to be a revocation of authorization to access the website,[7] and thus have fair notice that further access was "without authorization."[8]

To be sure, later cases may confront difficult questions concerning the precise contours of an effective "revocation" of authorization to access a generally public website.

---

[7]Accordingly, the Court finds little significance in 3Taps' point that an IP address is not a person. See Reply at 3. IP blocking may be an imperfect barrier to screening out a human being who can change his IP address, but it is a real barrier, and a clear signal from the computer owner to the person using the IP address that he is no longer authorized to access the website.

[8]3Taps also makes a passing suggestion in the "public policy" section of its brief that application of the statute's plain language "raises serious First Amendment implications." Supp. Br. at 14. But it cites no authority even remotely on point, and does not respond to Craigslist's observation that criminal enforcement of limits on the use of private property is common and not a presumptive violation of the First Amendment. See, e.g., Lloyd Corp., v. Tanner, 407 U.S. 569-70 (1972).

This Court cannot and does not wade into that thicket, except to say that under the facts here, which include the use of a technological barrier to ban all access, 3Taps' deliberate decision to bypass that barrier and continue accessing the website constituted access "without authorization" under the CFAA.

Legislative History: 3Taps says that the legislative history indicates that the CFAA was an "anti-hacking" statute designed to protect private information–not information voluntarily exposed to the world on a public website. Supp. Br. at 9-11. The lengthy legislative history includes statements referring to the protection of private information. See S. Rep. No. 99-432, at 1-2 (1986); H.R. Rep. No. 98-894, at 9-12 (1984); 142 Cong. Rec. S10,889, 10,890 (1996); S. Rep. No. 104-357, at 9 (1996). In other places, it says that the statute was modeled on common law trespass, see S. Rep. No. 104-357, at 7-11 (1996); S. Rep. No. 99-432, at 7 (1986); 131 Cong. Rec. S11,872 (daily ed. Sept. 20, 1985); H.R. Rep. No. 98-894, at 10, 20 (1984), where criminal enforcement of selective exclusion decisions by private parties is the norm.

This Court has no grounds for favoring one set of vague statements over the other–nor does it make much sense to try, where the statements were not addressed to the facts at issue in this case, which Congress probably could not have foreseen if it tried. In any event, as with the rule of lenity and the constitutional avoidance doctrines, courts "do not resort to legislative history to cloud a statutory text that is clear." Ratzlaf v. United States, 510 U.S. 135, 147-48 (1994).

Public Policy: Without any language in the statute to support its arguments, 3Taps lets the cat out of the bag in the concluding section of its brief and urges consideration of "serious policy concerns" raised by straightforward application of the CFAA's broad language. There, and sprinkled throughout its earlier, ostensibly text-based, arguments, 3Taps posits outlandish scenarios where, for example, someone is criminally prosecuted for visiting a hypothetical website www.dontvisitme.com after a "friend"–apparently not a very good one–says the site has beautiful pictures but the homepage says that no one is allowed to click on the links to view the pictures. See Supp. Br. 7 n.8. Needless to say, the Court's decision

concerning 3Taps' persistent scraping efforts undertaken after (1) receiving a cease-and-desist letter and (2) employing IP rotation technology to mask its identity and overcome Craigslist's technological barriers does not speak to whether the CFAA would apply to other sets of facts where an unsuspecting individual somehow stumbles on to an unauthorized site.

3Taps also invites this Court to make all manner of legislative judgments turning on, for example, the "culture" of the internet, the Court's view of whether accessing a website is more like window shopping from a public sidewalk or actually entering a store, and whether "a permission-based regime for public websites could implode the basic functioning of the internet itself." Id. at 13-14. 3Taps opines that "the 'socially prudent' benefits of finding an implied license [to access public website data] far outweigh any social utility derived from allowing a website owner to selectively block access to publicly available information, including by competitors." Reply at 10.

Maybe, or maybe not–but it is certainly not for this Court to impose its views on those matters on unambiguous statutory language. 3Taps and amici have articulated alternative, intuitive ways that Congress might draw the relevant statutory lines. For example, the statute might only protect "non-public information protected by a password, firewall, or similar restriction." Reply at 5. Currently, however, the statute protects all information on any protected computer accessed "without authorization," and nothing in that language prohibits a computer owner from selectively revoking authorization to access its website.

3Taps implies that this result borders on absurd, but this Court disagrees. The law of trespass on private property provides a useful, if imperfect, analogy. Store owners open their doors to the public, but occasionally find it necessary to ban disruptive individuals from the premises. That trespass law has enforced those bans with criminal penalties has not, in the brick and mortar context, resulted in the doomsday scenarios predicted by 3Taps in the internet context. The current broad reach of the CFAA may well have impacts on innovation, competition, and the general "openness" of the internet, see Reply at 15, but it is for Congress to weigh the significance of those consequences and decide whether amendment would be prudent.

IV. CONCLUSION

For the foregoing reasons, the Court DENIES 3Taps' renewed motion to dismiss the CFAA claim and the § 502 claim.

IT IS SO ORDERED.

Dated: August 16, 2013

CHARLES R. BREYER
UNITED STATES DISTRICT JUDGE