UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTIAN W. SANDVIG, et al., **Plaintiffs,** **v.** **WILLIAM P. BARR,[1] in his official capacity as Attorney General of the United States,** **Defendant.**	**Civil Action No. 16-1368 (JDB)**

MEMORANDUM OPINION

Plaintiffs are academic researchers who intend to test whether employment websites discriminate based on race and gender. In order to do so, they plan to provide false information to target websites, in violation of these websites' terms of service. Plaintiffs bring a pre-enforcement challenge, alleging that the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, as applied to their intended conduct of violating websites' terms of service, chills their First Amendment right to free speech. Without reaching this constitutional question, the Court concludes that the CFAA does not criminalize mere terms-of-service violations on consumer websites and, thus, that plaintiffs' proposed research plans are not criminal under the CFAA. The Court will therefore deny the parties' cross-motions for summary judgment and dismiss the case as moot.

[1] Pursuant to Fed. R. Civ. P. 25(d), William P. Barr, the current Attorney General of the United States, is automatically substituted as the defendant in this matter.

BACKGROUND

A. Research Plans

Christopher Wilson and Alan Mislove are professors of computer science at Northeastern University. Decl. of Pl. Christopher "Christo" Wilson ("First Wilson Decl.") [ECF No. 48-1] ¶ 1; Decl. of Pl. Alan Mislove ("First Mislove Decl.") [ECF No. 48-2] ¶ 1. For their research, Wilson and Mislove "intend to access or visit certain online hiring websites for the purposes of conducting academic research regarding potential online discrimination." Pls.' Statement of Undisputed Material Facts ("SMF") [ECF No. 47-2] ¶ 61. Their plans include "audit testing" to examine whether various hiring websites' proprietary algorithms discriminate against online users "based on characteristics, such as race or gender, that constitute a protected class status under civil rights laws." Id. ¶¶ 64, 66. To conduct these audit tests, plaintiffs "will create profiles for fictitious job seekers, post fictitious job opportunities, and compare their fictitious users' rankings in a list of candidates for the fictitious jobs" in order to see "whether [the] ranking is influenced by race, gender, age, or other attributes." Id. ¶ 71.

Wilson and Mislove state that they will take steps to minimize the impact of their research both on the targeted websites' servers and on other users of those websites. Id. at ¶¶ 75–78. For instance, they will make it apparent to real job seekers and employers that their postings are fake by "stat[ing] in any fictitious job posting, or in any fictitious job seeker profile, that the job or the job seeker is not real." Id. at ¶¶ 75–78. Both researchers also intend to "comply with the payment requirement" of certain employment websites. Decl. of Pl. Christopher "Christo" Wilson ("Second Wilson Decl.") [ECF No. 65-1] ¶ 5; Decl. of Pl. Alan Mislove ("Second Mislove Decl.") [ECF No. 65-2] ¶ 5. But Wilson and Mislove acknowledge that their research plan will violate the target websites' terms of service prohibiting the provision of false information and/or creating fake

accounts. SMF ¶ 86.

B. Procedural History

In June 2016, Wilson and Mislove, as well as two other researchers (Christian W. Sandvig and Kyratso Karahalios) and the nonprofit journalism group First Look Media Works, Inc., brought a pre-enforcement constitutional challenge to a provision of the CFAA. Compl. [ECF No. 1] ¶¶ 180–202. The provision at issue, 18 U.S.C. § 1030(a)(2)(C), or the "Access Provision," makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." Plaintiffs argue that this provision violates the First and Fifth Amendments. Compl. ¶¶ 180–202. Specifically, they claim that the Access Provision (1) is overbroad and chills their First Amendment right to freedom of speech; (2) as applied to their research activities, unconstitutionally restricts their protected speech; (3) interferes with their ability to enforce their rights and therefore violates the Petition Clause; (4) is void for vagueness under the Fifth Amendment Due Process Clause; and (5) unconstitutionally delegates lawmaking authority to private actors in violation of the Fifth Amendment Due Process Clause. See id. On March 30, 2018, this Court partially granted the government's motion to dismiss. See Sandvig v. Sessions, 315 F. Supp. 3d 1, 34 (D.D.C. 2018). The Court dismissed all but the as-applied First Amendment free speech claim brought by Wilson and Mislove. Id.

Now before the Court are the parties' cross-motions for summary judgment. Wilson and Mislove renew their pre-enforcement challenge to the Access Provision of the CFAA, alleging that it unconstitutionally restricts their First Amendment rights to free speech by criminalizing their research plans and journalistic activities that involve violating websites' terms of service. Pls.' Mem. P. & A. in Supp. of Mot. for Summ. J. ("Pls.' Mem.") [ECF No. 48] at 1. The government, for its part, argues that plaintiffs have failed to establish standing and that the First Amendment's

protections do not shield plaintiffs from private websites' choices about whom to exclude from their servers. Def.'s Mem. in Supp. of Cross-Mot. for Summ. J. & in Opp'n to Pls.' Mot. for Summ. J. ("Gov't's Opp'n") [ECF No. 50-1] at 1–4. The Court held a motions hearing on November 15, 2019, and subsequently ordered another round of briefing to clarify plaintiffs' specific research plans and both parties' understanding of particular terms within the CFAA. See November 26, 2019 Order [ECF No. 63] at 1–2. The parties each responded, see Def.'s Resp. to Court's Order for Clarification ("Def.'s Resp. for Clarification") [ECF No. 64]; Pls.' Mem. in Resp. to Court's Order [ECF No. 65], and the matter is now ripe for consideration.

LEGAL STANDARD

Summary judgment is appropriate when "the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The party seeking summary judgment "bears the initial responsibility of informing the district court of the basis for its motion, and identifying those portions of [the record] . . . demonstrat[ing] the absence of a genuine issue of material fact." Celotex Corp. v. Cartrett, 477 U.S. 317, 323 (1986); see Fed. R. Civ. P. 56(c)(1)(A) (explaining that a moving party may demonstrate that a fact is undisputed or not by citing "depositions, documents, electronically stored information, affidavits or declarations, stipulations . . . , admissions, interrogatory answers, or other materials").

In determining whether a genuine issue of material fact exists, the Court must "view the facts and draw reasonable inferences in the light most favorable to the party opposing the motion." Scott v. Harris, 550 U.S. 372, 378 (2007) (internal quotation marks and alteration omitted). But a non-moving party must establish more than the "mere existence of a scintilla of evidence" in support of its position. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 252 (1986). To avoid summary judgment, "there must be evidence on which the jury could reasonably find for the [non-moving

party]." Id.

ANALYSIS

I. Jurisdictional Standing

To have Article III standing, a "plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992)). This Court previously concluded that plaintiffs had plausibly alleged standing on their First Amendment claims at the motion-to-dismiss stage, Sandvig, 315 F. Supp. 3d at 16–22, but plaintiffs must now demonstrate standing "with specific facts set out by affidavit or other admissible evidence," In re Navy Chaplaincy, 323 F. Supp. 3d 25, 39 (D.D.C. 2018) (internal quotation marks omitted).

There are two ways in which litigants like plaintiffs here may establish the requisite ongoing injury when seeking to enjoin a statute alleged to violate the First Amendment. First, plaintiffs may show that they intend "to engage in a course of conduct arguably affected with a constitutional interest, but proscribed by a statute, and there exists a credible threat of prosecution thereunder." Susan B. Anthony List v. Driehaus, 573 U.S. 149, 159 (2014) (quoting Babbitt v. United Farm Workers Nat. Union, 442 U.S. 289, 298 (1979)). Second, they may refrain from exposing themselves to sanctions under the statute, making a sufficient showing of self-censorship—i.e., they may establish a chilling effect on their free expression. See Laird v. Tatum, 408 U.S. 1, 11–14 (1972). In either case, a constitutionally affected interest and a credible threat of enforcement are required; without them, plaintiffs can establish neither a realistic threat of legal sanction for engaging in protected speech nor an objectively good reason for self-censoring by not conducting their planned research. Here, plaintiffs take the first path and argue that they intend to engage in conduct

"arguably" proscribed by statute.

The government responds that plaintiffs lack standing for three reasons. First, regardless of whether the Department of Justice would prosecute their conduct, plaintiffs "lack any concrete plans for conducting future research covered by their as-applied claim, i.e., involving fake or misleading accounts." Gov't's Opp'n at 10. Second, assuming concrete research plans, "[p]laintiffs have not demonstrated a credible threat of prosecution for . . . such research." Id. And third, plaintiffs' "claims are too abstract to be evaluated and therefore are not ripe." Id. The government does not appear to dispute that, if plaintiffs can satisfy the injury-in-fact requirements, they can also meet the causation and redressability tests to establish standing. See Spokeo, 136 S. Ct. at 1547.

A. Concrete Plans

The government first argues that plaintiffs have failed to establish the existence of "any concrete plans for conducting further research covered by their as-applied claim." See Gov't's Opp'n at 10–11. To support this argument, the government quotes testimony from Wilson and Mislove that they have no "concrete plans" for research involving the provision of false information or the creation of fake accounts in violation of websites' terms of service. Id.

This framing—and selective quotation—of plaintiffs' testimony mischaracterizes the extent of their plans. "Pre-enforcement review, particularly in the First Amendment context, does not require plaintiffs to allege that they will in fact violate the regulation in order to demonstrate an injury." U.S. Telecom Ass'n v. FCC, 825 F.3d 674, 739 (D.C. Cir. 2016) (internal quotation marks omitted). "Standing to challenge laws burdening expressive rights requires only a credible statement by the plaintiff of intent to commit violative acts and a conventional background expectation that the government will enforce the law." Id. (emphasis added) (internal quotation marks omitted).

Plaintiffs here satisfy this standard. Wilson later clarified that, when he said he did not have

concrete plans, "what [he] meant was [they] don't have software, [they] don't have a timeframe. There [are] no students assigned to it." Oral Depo. of Christopher Wilson ("Wilson Depo.") [ECF No. 54-3] at 215:25–216:4. But Wilson has already "applied and received . . . funding" and approval from the Institutional Review Board ("IRB") for such projects. Id. at 217:15–18. Likewise, Mislove testified that he has "specific research plans [and] specific platforms that [his lab is] studying . . . in the sense that this is an area of [his] research that [he] intend[s] to conduct work[] in." Oral Depo. of Alan E. Mislove ("Mislove Depo.") [ECF No. 52-3] at 47:4–8. In response to the government's interrogatory asking for "any and all platforms and/or websites that Plaintiffs intend to access in the future for purposes" of research, plaintiffs identified specific websites, including LinkedIn, Monster, Glassdoor, and Entelo, and noted that they intended to conduct research that might violate these sites' terms of service by "creating accounts using false information and/or providing false or misleading information." Pls.' Third Suppl. Resps. & Objs. to Def.'s First Set of Interrogs. Nos. 2–3 [ECF No. 52-6] at 3–4.

The government argues in response that "'some day' intentions—without any description of concrete plans, or indeed even any specification of when the some day will be—do not support a finding of the actual or imminent injury." Gov't's Opp'n at 10–11 (quoting Defs. of Wildlife, 504 U.S. at 564). But unlike the amorphous "'some day' intentions" to visit endangered species on another continent at issue in Defenders of Wildlife, see 504 U.S. at 564, these researchers' plans are already in motion, even if the specifics of their study are still being developed. The fact that plaintiffs have secured funding and IRB clearance to engage in conduct covered by their as-applied challenge evinces a sufficient demonstration of injury in fact. Cf. Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc., 528 U.S. 167, 183–84 (2000) (concluding that organizational plaintiffs' members suffered an injury in fact because they had "reasonable concerns" rising above the level of

"speculative some day intentions" that the discharge of pollutants would "directly affect[]" their "recreational, aesthetic, and economic interests" (internal quotation marks omitted)).

The government also argues that plaintiffs' two declarations, clarifying the meaning of their earlier statements about "concrete plans," must be disregarded under the so-called "sham affidavit rule." Gov't's Opp'n at 11–12; see also First Wilson Decl.; First Mislove Decl. This argument fails, however, because these affidavits' descriptions of plaintiffs' research plans merely clarify plaintiffs' prior answers and contextualize their use of the term "concrete." See Galvin v. Eli Lilly & Co., 488 F.3d 1026, 1030 (D.C. Cir. 2007). Mislove and Wilson said they have no "concrete" plans in order to explain that they are not currently implementing any of those research plans, notwithstanding their intent to do so in the future. Moreover, there is no indication that plaintiffs, in their earlier statements, intended to use the term "concrete plans" in its specific meaning as a legal term of art.

Finally, in its reply brief, the government states that the clearest examples of concrete steps taken by Wilson actually concern a different research project than the proposed discrimination project at issue in this case. Def.'s Reply Mem. in Supp. of Cross-Mot. for Summ. J. ("Gov't's Reply") [ECF No. 56] at 4 n.1. The government does not clearly articulate the distinction between the different research projects, however, and this Court has already recognized that Wilson and Mislove intend both to "create fake employer profiles" and to "create fictitious sock-puppet job seeker profiles" as part of the research at issue in this case. Sandvig, 315 F. Supp. 3d at 9–10.

B. Credible Threat

Under their theory of standing, plaintiffs must show that they intend to engage in conduct arguably both protected by the First Amendment and proscribed by the statute they challenge, and that there is a "credible threat" that the statute will be enforced against them when they do so. See Driehaus, 573 U.S. at 158–63. The government argues that plaintiffs fail to establish a credible threat

of prosecution under the CFAA, contending that (1) plaintiffs' testimony shows that they do not fear prosecution (and, indeed, already have engaged in such research); (2) past CFAA prosecutions do not establish a credible threat that plaintiffs' proposed conduct will be prosecuted; and (3) the government's charging policies and public statements undercut plaintiffs' attempt to establish a credible threat of prosecution. Gov't's Opp'n at 12–18.

"Standing to challenge laws burdening expressive rights requires only a credible statement by the plaintiff of intent to commit violative acts and a conventional background expectation that the government will enforce the law" U.S. Telecom Ass'n, 825 F.3d at 739 (internal quotation marks omitted). As previously noted, plaintiffs satisfy the first half of this test; the question thus becomes whether the "conventional background expectation" of criminal enforcement holds here. Id. Again, plaintiffs have the stronger arguments.

First, plaintiffs' testimony that they do not subjectively fear prosecution under this statute—and that they have even engaged in the allegedly "chilled" conduct previously—does not undermine their legal claim. The question is whether there exists "a credible threat," which is an objective, rather than subjective, inquiry. See id. Mislove also testifies that he does subjectively fear facing criminal consequences for his future research. See, e.g., Mislove Depo. at 147:12–19 ("[I]t really weigh[s] heavily on my mind . . . [that I am] exposing my students to criminal—to potential criminal prosecution or the risk.").

Second, even assuming the absence of prior prosecutions, but see Sandvig, 314 F. Supp. 3d at 19–20 (discussing two previous prosecutions under the Access Provision), plaintiffs still are not precluded from bringing this pre-enforcement action. When constitutionally protected conduct falls within the scope of a criminal statute, and the government "has not disavowed any intention of invoking the criminal penalty provision," plaintiffs are "not without some reason in fearing

prosecution" and have standing to bring the suit. Babbitt, 442 U.S. at 302. Indeed, at the pleadings stage, the Court already rejected the contention that the lack of similar past CFAA prosecutions undermines a credible threat of prosecution now. See Sandvig, 315 F. Supp. 3d at 18–21.

Third, the government points to guidance from the Attorney General that "expressly cautions against prosecutions based on [terms-of-service] violations," as well as statements to Congress by Department of Justice officials, as evidence that plaintiffs face no credible threat of prosecution. Gov't's Opp'n at 16–17. But the absence of a specific disavowal of prosecution by the Department undermines much of the government's argument. See Babbitt, 442 U.S. at 302. The government insists that it is not a defendant's burden to "come forward with proof of a non-existent threat of prosecution." Gov't's Opp'n at 17. But while the burden of demonstrating standing remains on the plaintiffs, this Court has previously ruled that in the absence of an "explicit statement" disavowing prosecution, these various advisory and non-binding statements and Department of Justice policies do not eliminate the reasonable fear of prosecution. Sandvig, 315 F. Supp. 3d at 20–21. Furthermore, as noted above the government has brought similar Access Provision prosecutions in the past and thus created a credible threat of prosecution. Id. at 19–20.

Discovery has not helped the government's position. John T. Lynch, Jr., the Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of the Department of Justice, testified at his deposition that it was not "impossible for the Department to bring a CFAA prosecution based on [similar] facts and de minimis harm." Dep. of John T. Lynch, Jr. [ECF No. 48-4] at 154:3–7. Although Lynch has also stated that he does not "expect" the Department to do so, Aff. of John T. Lynch, Jr. [ECF No. 21-1] ¶ 9, "[t]he Constitution 'does not leave us at the mercy of noblesse oblige,'" Sandvig, 315 F. Supp. 3d at 21 (quoting United States v. Stevens, 559 U.S. 460, 480 (2010)). Absent a specific disavowal or a clear indication that plaintiffs' conduct falls outside

the scope of the criminal provisions, plaintiffs adequately demonstrate a credible threat for standing purposes.

C. Ripeness

The government also argues that plaintiffs' claims are not ripe for adjudication. "Plaintiffs have not yet identified the specific websites that they intend to access for their research," the government says, and hence it is "impossible to know what those websites' [terms of service] will be at the time of Plaintiffs' research"—or whether any violation of the terms of service will run afoul of the Court's narrow construction of the CFAA. Gov't's Opp'n at 18. Because plaintiffs do not know what their research will entail, the government argues, the Court cannot evaluate the potential harms caused by their hypothetical research. Id. at 18–19. Hence, according to the government, the Court cannot meaningfully examine plaintiffs' First Amendment claim on the merits and fashion a proper injunction under Rule 65 because it cannot "describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required." Id. at 19 (quoting Fed. R. Civ. P. 65(d)(1)(B), (C)).

Plaintiffs respond first that, because terms of service are always subject to change, it will always be impossible to know what a website's exact terms of service will be in the future, or whether research violating those terms will implicate the Access Provision. Pls.' Mem. in Opp'n to Def.'s Mot. for Summ. J. & Reply in Supp. of Pls.' Mot. for Summ. J. ("Pls.' Reply") [ECF No. 54] at 10–11. Accordingly, "[p]laintiffs would have to actually undertake the research—taking note of the [terms of service] actually in effect at the time and exposing themselves to criminal liability—in order to challenge the Access Provision's application to them," a drastic and risky step that plaintiffs argue is not required by the First Amendment. Id. at 11. Next, plaintiffs say that how exactly they plan to carry out their research—for instance, the number of fictitious accounts or postings that will

be necessary or how long each account or posting will exist—is irrelevant to the First Amendment question. Id. Finally, plaintiffs argue that their complaint and declarations clarify in detail the research goals, methodologies, and precautions that will be taken to mitigate potential harm. Id. at 11–12.

The question of ripeness presents a closer call than the previous two standing issues. For instance, if this Court were to reach the First Amendment analysis urged by plaintiffs and evaluate the Access Provision under intermediate scrutiny, it would have to determine whether the government has "show[n] 'a close fit between ends and means'" such "that the regulation 'promotes a substantial government interest that would be achieved less effectively absent the regulation,'" and does "not 'burden substantially more speech than is necessary to further the government's legitimate interests.'" A.N.S.W.E.R. Coal. v. Basham, 845 F.3d 1199, 1213–14 (D.C. Cir. 2017) (citations omitted); see also Sandvig, 315 F. Supp. 3d at 30. Absent specific direction from plaintiffs, it will be difficult to engage in this analysis. The Court is not well placed, for instance, to forecast what technological or security risks might be generated by permitting such research.

Still, based on the record before it, the Court concludes that the present dispute is ripe. Plaintiffs listed several websites—LinkedIn, Monster, Glassdoor, and Entelo—that they plan to visit, and they described intending to violate these sites' terms of service by "creating accounts using false information and/or providing false or misleading information." Pls.' Third Suppl. Resps. & Objs. to Def.'s First Set of Interrogs. No. 3, at 3–4. Wilson and Mislove also both testified that their research plans were designed to have, at most, a de minimis effect on the targeted websites, further demonstrating that specific concrete steps have been taken in their research. First Wilson Decl. ¶ 46; First Mislove Decl. ¶ 43. The governments' own exhibits make clear the extent to which websites, like LinkedIn, both prohibit and attempt to eliminate false accounts. See, e.g., Decl. of Paul Rockwell

("LinkedIn Decl.") [ECF No. 52-11] at 3–12; Decl. of Thomas O'Brien ("GlassDoor Decl.") [ECF No. 52-13] at 5–6; Affirmation of Leonard Kardon ("Monster Aff.") [ECF No. 52-14] at 1–2. These various pieces of evidence reveal a ripe dispute over whether criminally prosecuting plaintiffs under the CFAA for violations of public websites' terms of service runs afoul of the First Amendment.

* * *

Finally, the Court turns to the question of whether plaintiffs' "intended future conduct is 'arguably . . . proscribed by'" the CFAA. Driehaus, 573 U.S. at 162 (quoting Babbitt, 442 U.S. at 298). The government does not appear to question that plaintiffs plan to engage in proscribed conduct, but the Court has "an independent obligation to assure that standing exists." Summers v. Earth Island Inst., 555 U.S. 488, 499 (2009). The Court is also mindful that its ultimate interpretation of the CFAA, see infra, at 15–28, excludes plaintiffs' conduct from criminal liability and, at minimum, moots their First Amendment claim. Still, the question remains whether the Court's ultimate determination that the CFAA does not criminalize plaintiffs' intended conduct eliminates plaintiffs' injury-in-fact, see Driehaus, 573 U.S. 158–59, or merely moots the First Amendment dispute, see Powell v. McCormack, 395 U.S. 486, 496 (1969) ("[A] case is moot when the issues presented are no longer 'live' . . . .").

The resolution to this question turns on the meaning of Driehaus's holding that plaintiffs' intended conduct must be "arguably . . . proscribed by statute," Driehaus, 573 U.S. at 159; see also Woodhull Freedom Found. v. United States, 948 F.3d 363, 371 (D.C. Cir. 2020) (holding that courts should look to Driehaus's test for determining whether a plaintiff faces an "imminent threat" of prosecution in a pre-enforcement action). The Second Circuit has taken this standard to mean that, as long as plaintiffs propose a reasonable interpretation of the statute under which they credibly fear prosecution, then they satisfy the standing requirement. See Knife Rights, Inc. v. Vance, 802 F.3d

377, 384–86 (2d Cir. 2015) (holding that plaintiff had standing where, despite believing its knife design was not proscribed, plaintiff could not "confidently determine which such knives defendants will deem proscribed gravity knives"). This "reasonable interpretation" approach stems from a line of pre-Driehaus cases in which the Second Circuit was interpreting Babbitt, from which Driehaus borrowed the "arguably proscribed" standard. See Vt. Right to Life Comm., Inc. v. Sorrell, 221 F.3d 376, 382 (2d Cir. 2000). The Second Circuit understood Babbitt to require only that an interpretation proscribing plaintiffs' intended conduct be "reasonable enough that [they] may legitimately fear that [they] will face enforcement of the statute." Id. at 383.

The D.C. Circuit's recent decision in Woodhull Freedom Foundation suggests a slightly different approach. Although not as explicit as the Second Circuit in stating how plausible an interpretation needs to be to satisfy plaintiffs' standing requirements, the court engaged in considerable statutory construction before deciding that plaintiffs did, in fact, have standing. See Woodhull Freedom Found., 948 F.3d at 371–73. As Judge Katsas suggested in concurrence, a district court is first to decide the statute's meaning and then to decide if, arguably, the plaintiffs' conduct falls within its "[p]roperly construed" bounds. Id. at 375 (Katsas, J., concurring).

Unlike in Woodhull Freedom Foundation, which concerned a plain-meaning interpretation relying on dictionaries and precedent, see id. at 372–73, Wilson and Mislove challenge an ambiguous statute that this Court has already deemed may apply to their conduct, see Sandvig, 315 F. Supp. 3d at 18. As will be discussed below, substantive canons of interpretation, like the rule of lenity and constitutional avoidance, guide this Court's ultimate decision. Under such circumstances, the Court concludes that plaintiffs' intended conduct is "arguably . . . proscribed by statute," Driehaus, 573 U.S. at 159. To rule otherwise, and decide this complicated statutory matter under the rubric of standing, would risk converting the "arguably . . . proscribed by statute" standard of Babbitt and

Driehaus into one of certainty. Cf. Hedges v. Obama, 724 F.3d 170, 199 (2d Cir. 2013) (noting an unease with "allowing a preenforcement standing inquiry to become the vehicle by which a court addresses" important and complex matters of statutory interpretation).

II. Interpreting the CFAA

Assuming, then, that plaintiffs have satisfied the injury-in-fact requirement, the Court nevertheless concludes that their First Amendment claim is moot. As will be discussed below, courts have disagreed as to the breadth of the CFAA's Access Provision. If this Court determines that the Access Provision does not actually criminalize plaintiffs' proposed conduct—namely, violating consumer websites' terms of service—then the Court need not dive, and judicial economy would advise against diving, into the First Amendment issue. See Bond v. United States, 572 U.S. 844, 855 (2014) ("[I]t is a well-established principle governing the prudent exercise of this Court's jurisdiction that normally the Court will not decide a constitutional question if there is some other ground upon which to dispose of the case." (internal quotation marks omitted)). Rather, the Court concludes that the First Amendment claims plaintiffs "presented are no longer 'live'" and will dismiss the case as moot. Powell, 395 U.S. at 496.

a. Accessing Without Authorization

The CFAA prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2). The term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication," Id. § 1030(e)(2)(B), and no party disputes that the servers and other computers associated with the websites in question here, like LinkedIn, constitute "protected computer[s]."

Although the CFAA does not define "authorization," courts have found the term "clear" and

given it a "straightforward meaning." United States v. Nosal ("Nosal II"), 844 F.3d 1024, 1035 (9th Cir. 2016). The Ninth Circuit, for instance, has consistently interpreted "authorization" to mean "permission or power granted by an authority." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); see also hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 1000 (9th Cir. 2019) ("Authorization is an affirmative notion, indicating that access is restricted to those specially recognized or admitted." (internal quotation marks omitted)); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] defendant can run afoul of the CFAA when he or she has no permission to access a computer or when such permission has been revoked explicitly."); Nosal II, 844 F.3d at 1033 ("Not surprisingly, there has been no division among the circuits on the straightforward 'without authorization' prong of [§ 1030(a)]."). At least the Second, Fourth, and Sixth Circuits have come to the same conclusion. See, e.g., United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015) ("[C]ommon usage of 'authorization' suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all."); WEC Carolina Energy Sols. v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) ("[B]ased on the ordinary, contemporary, common meaning of 'authorization,' . . . an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer."); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 303–04 (6th Cir. 2011) ("Commonly understood, . . . a defendant who accesses a computer 'without authorization' does so without sanction or permission.").

The statutory text is less clear, however, when it comes to the entire phrase "accesses a computer without authorization." The CFAA does not define this phrase, but "the wording of the statute, forbidding 'access[] . . . without authorization,' . . . suggests a baseline in which access is not generally available and so permission is ordinarily required." hiQ Labs, 938 F.3d at 1000. This

wording thus contemplates a view of the internet as divided into at least two realms—public websites (or portions of websites) where no authorization is required and private websites (or portions of websites) where permission must be granted for access. Because many websites on the internet are open to public inspection, a website or portion of a website becomes "private" only if it is "delineated as private through use of a permission requirement of some sort." Id. at 1001.[2]

Most courts agree with the hiQ Labs court's interpretation of "accesses . . . without authorization" as contemplating a "two-realm internet." See, e.g., WEC Carolina Energy Sols., 687 F.3d at 204 ("[A user] accesses a computer 'without authorization' when he gains admission to a computer without approval." (emphasis added)); United States v. Nosal ("Nosal I"), 676 F.3d 854, 858 (9th Cir. 2012) (en banc) ("'[W]ithout authorization' would apply to outside hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."). Courts have interpreted this provision to involve transitioning from a public area of the internet to a private, permission-restricted area, often requiring some form

[2] The hiQ Labs court faced the additional wrinkle of whether sending a cease-and-desist letter to specific users, who were allegedly violating LinkedIn's terms of service, was enough to revoke authorization even for otherwise "public" parts of the website. See 938 F.3d at 999 ("The pivotal CFAA question here is whether once hiQ received LinkedIn's cease-and-desist letter, any further scraping and use of LinkedIn's data was 'without authorization' within the meaning of the CFAA and thus a violation of the statute."); see also Craigslist Inc. v. 3Taps Inc., 964 F. Supp. 2d 1178, 1182 (N.D. Cal. 2013) (describing "the question here" as "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"). Because no such letters have been sent in this case, the Court need not decide whether they would constitute a revocation of authorization and thereby make any further visits by the recipients to the otherwise public portions of LinkedIn a CFAA violation. See also Pet. for Writ of Cert. at 25, LinkedIn Corp. v. hiQ Labs, Inc., No. 19-1116 (U.S. Mar. 9, 2020) ("Where a website owner sets up technical measures to deny a third-party scraper access to its website or sends a cease-and-desist letter, thereby putting the scraper indisputably on notice that access is not authorized, any further efforts to access that website are 'without authorization.'").

At the same time, the fact that receipt of a cease-and-desist letter might render the recipient's future visits to an otherwise public website "unauthorized" does provide one possible distinction between § 1605(a)(2) and § 1605(a)(3) that helps to give meaning to the term "nonpublic" in the latter provision. Cf. 3Taps, 964 F. Supp. 2d at 1182–83 ("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.").

of authentication before a viewer is granted access. See, e.g., hiQ Labs, 938 F.3d at 1001 ("[A]uthorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information."); Valle, 807 F.3d at 524 ("'[W]ithout authorization' most naturally refers to a scenario where a user lacks permission to access the computer at all.").

The statutory and legislative history of the CFAA support this public-private reading of the provision. Originally part of the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92, the CFAA "has been substantially modified" over the intervening decades. See Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 1561, 1561 (2010). Throughout this history, however, Congress has consistently analogized violations of § 1030 to physical-world crimes. For example, "[t]he 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry." hiQ Labs, 938 F.3d at 1000. That Report notes that "[d]ifficulties in coping with computer abuse arise because much of the property involved does not fit well into categories of property subject to abuse or theft." H.R. Rep. No. 98-894, at *9 (1984) (emphasis added). Instead of focusing on what was stolen, the CFAA relied on "an 'unauthorized access' concept," wherein "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense." Id. at *20.

Likewise, when the CFAA was amended in 1996 to cover federal government computers and those in interstate commerce (i.e., "protected computers"), the Senate Report described the bill as "protect[ing] against the interstate or foreign theft of information by computer" (emphasis added), suggesting a comparison to the physical-world crime of theft. S. Rep. No. 104-357, at *7 (1996). This Report reveals that a central motivation behind these amendments was "to increase protection for the privacy and confidentiality of computer information," id., further suggesting that "access[ing]

a computer without authorization" involves "obtain[ing]" information from non-public websites, see 18 U.S.C. § 1030(a)(2).

This interpretation rooted in property norms also aligns with judicial readings of similar language in the Stored Communications Act. See 18 U.S.C. § 2701(a) (criminalizing "intentionally access[ing] without authorization a facility through which an electronic communication service is provided" or "intentionally exceed[ing] an authorization to access [such a] facility"); see also Wachovia Bank v. Schmidt, 546 U.S. 303, 305 (2006) ("[U]nder the in pari materia canon, statutes addressing the same subject matter generally should be read as if they were one law . . . ." (internal quotation marks omitted)). For example, interpreting the Act in light of the common law, the Ninth Circuit focused on "the essential nature" of the relationship between the computer owner and the accesser, and concluded that "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances." Theofel v. Farey-Jones, 359 F.3d 1066, 1073 (9th Cir. 2004) (emphasis added).

Likewise, in amending 18 U.S.C. § 2510, the Patriot Act defined "computer trespasser" as "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer." Pub. L. 107–56, 115 Stat. 272 (2001). That the Patriot Act cites § 1030 for the definition of "protected computer" makes the connection between these two statutes all the clearer: "access[ing] a computer without authorization" is the computer equivalent of trespassing in the physical world.

Adopting the formulation of the Ninth Circuit in hiQ Labs, this Court will call the barriers between the public internet and private authorization-based computers "permission requirements." 938 F.3d at 1001. Under this interpretation, the question becomes what sort of "permission

requirement" constitutes enough of a barrier to trigger criminal liability under § 1030(a)(2) if bypassed. The government suggests that such "permission requirements" can be minimal. See Tr. Mots. H'rg [ECF No. 62] at 54:15–56:17. An announcement on the homepage of a website that access to any further content is conditioned on agreeing to lengthy terms of service—or even one term of service—would, the government argues, constitute such a requirement. Id. at 54:22–24.

The Court concludes that agreeing to such contractual restrictions, although that may have consequences for civil liability under other federal and state laws, is not sufficient to trigger criminal liability under the CFAA. In other words, terms of service do not constitute "permission requirements" that, if violated, trigger criminal liability.

A number of considerations lead the Court to this conclusion. First, websites' terms of service provide inadequate notice for purposes of criminal liability. These protean contractual agreements are often long, dense, and subject to change. While some websites force a user to agree to the terms before access—so-called "clickwrap"—others simply provide a link at the bottom of the webpage, or place the terms, often in fine print, elsewhere on the page. "Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read." Nosal I, 676 F.3d at 860.

Second, although not a paradigmatic example of a "nondelegation" problem, enabling private website owners to define the scope of criminal liability does raise concerns for the Court. See The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation, 127 Harv. L. Rev. 751, 768–71 (2013). Previously, this Court determined that a narrow interpretation of the CFAA limited to "access restrictions" saved § 1030(a)(2) from becoming "a limitless, standardless delegation of power to individual websites to define crimes." Sandvig, 315 F. Supp. 3d at 33. The Court also concluded that merely "incorporat[ing] private parties' chosen restrictions, which are only

binding on those who interact with those parties' individual [websites]," did not necessarily constitute an improper delegation of legislative or regulatory authority. Id. at 33–34.

Upon further reflection, and now presented with additional evidence of the nature of the target websites' terms of service, the Court finds that it is necessary to answer another question: whether terms-of-service conditions, rather than authentication gates, constitute adequate "permission requirements" for criminal liability under the CFAA. Again, the Court concludes that the narrower interpretation is the wiser path. The government analogizes website owners to real property owners, who have historically been allowed to exclude whomever they choose from their private, non-commercial land, Gov't's Opp'n at 23–24, but the analogy between real property and the internet is not perfect. The internet is inherently open and public, see Reno v. Am. Civil Liberties Union, 521 U.S. 844, 880 (1997) (observing that "most Internet forums—including chat rooms, newsgroups, mail exploders, and the Web—are open to all comers"), and users constantly move from one website to another and navigate between various sections of a given website. Under such circumstances, the CFAA's prohibition on "access[ing] a computer without authorization," even though phrased "in the form of a general prohibition" that can often escape nondelegation worries, see Silverman v. Barry, 845 F.2d 1072, 1086 (D.C. Cir. 1988), becomes unworkable and standardless. Criminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature. Such an arrangement, wherein each website's terms of service "is a law unto itself," Emp't Div., Dep't of Human Res. of Or. v. Smith, 494 U.S. 872, 890 (1990), would raise serious problems. This concern, then, supports a narrow interpretation of the CFAA.

Third, both the rule of lenity and the avoidance canon weigh in favor of this narrow interpretation as well. "When interpreting a criminal statute, we do not play the part of a mindreader." United States v. Santos, 553 U.S. 507, 515 (2008). If "a reasonable doubt persists about a statute's

intended scope even after resort to the language and structure, legislative history, and motivating policies of the statute," Moskal v. United States, 498 U.S. 103, 108 (1990) (internal quotation marks omitted), courts must adopt the narrower interpretation. See Yates v. United States, 135 S. Ct. 1074, 1088 (2015) ("[I]f . . . recourse to traditional tools of statutory construction leaves any doubt about the meaning of [a statutory term] . . . , we would invoke the rule that ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." (internal quotation marks omitted)). Here, none of the traditional tools of statutory interpretation definitively resolves the question of what constitutes "access[ing] . . . without authorization," so the Court opts to interpret the provision narrowly and as not encompassing terms-of-service violations.

Likewise, constitutional avoidance weighs in favor of interpreting "accesses . . . without authorization" narrowly. If the Court were to conclude that plaintiffs' terms-of-service violations do violate the CFAA, then it would have to decide whether prosecuting them for such actions violates the First Amendment. As the Court previously observed, it "need not determine whether plaintiffs' constitutional arguments would actually win the day," but rather "whether one reading 'presents a significant risk that [constitutional provisions] will be infringed.'" Sandvig, 315 F. Supp. 3d at 25 (quoting NLRB v. Catholic Bishop of Chi., 440 U.S. 490, 502 (1979)). Plaintiffs' First Amendment challenge raises such risks, see Sandvig, 315 F. Supp. 3d at 28–30, and thus weighs in favor of a narrow interpretation under the avoidance canon.

Given all these concerns, a user should be deemed to have "accesse[d] a computer without authorization," 18 U.S.C. § 1030(a)(2), only when the user bypasses an authenticating permission requirement, or an "authentication gate," such as a password restriction that requires a user to demonstrate "that the user is the person who has access rights to the information accessed," Orin S. Kerr, Norms of Computer Trespass, 116 Colum. L. Rev. 1143, 1147, 1164 (2016) (hereinafter

"Norms"). Although bypassing code-based restrictions, like a social-security-number or credit-card requirement, are paradigmatic examples of an "authentication gate," see Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1664 (2003), "[t]he key point is not that some code was circumvented but rather that the computer owner conditioned access on authentication of the user and the access was outside the authentication," Norms at 1164.

Here, neither Wilson nor Mislove attempt to bypass an authentication gate. For websites requiring "login credentials—i.e., usernames and passwords"—Wilson and Mislove intend to provide the information that they "generated when [they] created tester accounts." Second Wilson Decl. ¶ 6; Second Mislove Decl. ¶ 6. And for websites that require payments, they intend to "comply with the payment requirement." Second Wilson Decl. ¶ 5; Second Mislove Decl. ¶ 5. None of their research plans, then, involve bypassing authenticating "permission requirements," and thus none of them when executed will constitute violations of the CFAA as interpreted herein.

The record does reflect that at least Wilson previously used borrowed business information for authentication purposes on CareerBuilder.com. See Wilson E-mails Regarding CareerBuilder Receipt, PID7243-46 (July 2016) [ECF No. 52-16] at 3. At the motions hearing, however, counsel for plaintiffs stated that "they only intend to access parts of a website that are otherwise open to the public or available to anyone who creates a [username] and password." Mots. Hr'g Tr. at 8:15–17. The Court asked for clarification, see Nov. 26, 2019 Order at 1–2, and declarations from both researchers now clarify that, although they may pay for access to some public employment websites, their future research plans entail no provision of "authenticating, real-world business information . . . , such as real-world business license information." Second Wilson Decl. ¶ 2; Second Mislove Decl. ¶ 2. The Court thus has no occasion to determine whether provision of either false or borrowed

real-world business information to access otherwise private portions of employment websites would violate the CFAA.

b. Exceeding Authorized Access

Turning to the second part of the Access Provision, the CFAA prohibits "exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer." The CFAA defines "the term 'exceeds authorized access' [to] mean[] to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C § 1030(e)(6).

This language suggests that an individual cannot "exceed[] authorized access" without first legitimately passing through a "permission requirement." After all, the violator must "use such [authorized] access" in order to "obtain or alter information" to which the violator "is not entitled," implying that barriers are passed through permissibly. Id. (emphasis added). This interpretation aligns with the Ninth Circuit's distinction between "accesses . . . without authorization" applying to "outside hackers" and "exceeds authorized access" applying to "inside hackers." Nosal I, 676 F.3d at 858.

If bypassing a "permission requirement" is not the action that triggers criminal liability, however, then the question remains what type of conduct does constitute a criminal act. In other words, what distinguishes information that an authorized accesser is "entitled to obtain or alter" from information to which he is not entitled? Does plaintiffs' anticipated provision of false information to their target websites, in violation of these websites' terms of services, cross that line and "exceed[] authorized access"?

The resolution of this question turns, in part, on the meaning of "entitled" in the statutory definition of "exceeds authorized access" at § 1030(e)(6). The government argues that "entitled"

means "to furnish with a right," and "supports [a] broader interpretation of the phrase 'exceeds authorized access' . . . , in which all relevant facts (including policies set by the computer owners) may be considered in determining the scope of a person's authorized access." Def.'s Resp. for Clarification at 5–6. By this approach, the meaning of "exceeds authorized access" is context-dependent: "Because the computer owner furnishes an individual with the right to access its systems and obtain information from them, explicit policies restricting that right determines when an individual 'exceeds authorized access.'" Id. at 6. According to the government, such "explicit policies" include employers' computer-use policies and the terms of service of public websites. See id. at 6; Gov't's Opp'n at 53–54.

Plaintiffs seem to have agreed with this interpretation for much of the litigation and assumed that such terms-of-service violations do fall afoul of the CFAA. See Pls.' Mem. at 2–3, 9–11. Rather than interpreting the statute narrowly, they argued that their actions are protected by the First Amendment. But plaintiffs now suggest that they would be satisfied with "declaratory and injunctive relief" barring prosecution under the CFAA for violations of websites' terms of service—in other words, with a narrow interpretation of the CFAA that it does not encompass terms-of-service violations. See Pls.' Mem. in Resp. to Court's Order at 1.

Courts have come to a range of views on the best interpretation of "exceeds authorized access," and the circuits are currently divided on whether, in the employment context, an employee's violation of company policy constitutes a CFAA violation. The First, Fifth, Seventh, and Eleventh Circuits have concluded that a person with access to a computer for business purposes exceeds authorized access when the accesser "obtain[s] . . . information for a nonbusiness reason." United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); see also United States v. John, 597 F.3d 263, 272 (5th Cir. 2010) (concluding that an employee's "access[ing] account information for

individuals whose accounts she did not manage, remov[ing] this highly sensitive and confidential information from [the employer's] premises, and ultimately us[ing] this information to perpetrate fraud on [the employer] and its customers" constituted a CFAA violation); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (similar); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–83 (1st Cir. 2001) (similar).[3] The Second and Fourth Circuits have come to the opposite conclusion. See Valle, 807 F.3d at 512–13, 528 (applying the rule of lenity and not imposing liability for accessing a government database of personal information for no law enforcement purpose); WEC Carolina Energy Sols., 687 F.3d at 205–07 (refusing to impose liability when employees violated company policy).

Far fewer courts have weighed in on the facts before this Court: namely, whether violating the terms of service of consumer websites constitutes a criminal CFAA violation. But the majority of courts that have examined this question has determined that there is no liability. See, e.g., Facebook, 844 F.3d at 1067 ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."); Bittman v. Fox, 107 F. Supp. 3d 896, 900–01 (N.D. Ill. 2015) (concluding that defendants did not "exceed[] authorized access" by creating "a fake social media account in violation of a social media company's terms of service"); United States v. Drew, 259 F.R.D. 449, 464–65 (C.D. Cal. 2009) (interpreting "exceeds authorized access" to exclude mere terms-of-service violations to avoid rendering the statute void for vagueness). But see United States v. Lowson, Crim. No. 10-114 (KSH), 2010 WL 9552416, at *5 (D.N.J. Oct. 12, 2010) (not dismissing

[3] The First Circuit later extended its holding in Explorica, which was based upon confidentiality agreements signed by former employees, to Zefer, a third-party website. See EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58 (1st Cir. 2003). Although the decision did suggest that terms of service may create CFAA liability by "say[ing] just what non-password protected access they purport to forbid," id. at 64, the First Circuit's holding relied upon the "relatively narrow grounds" that the injunction against Explorica applied to "anyone else with notice" and thus "precluded [Zefer] from acting to assist the enjoined party from violating the decree [and] from doing so on behalf of that party," id. at 61, 63.

a case wherein the defendants "implement[ed] 'hacks' and us[ed] 'backdoors' to enable automated programs to purchase tickets" from online vendors).

The Court agrees with the clear weight of relevant authority and adopts a narrow interpretation of "exceeds authorized access." Without weighing in on the circuit split over employers' computer-use policies, the Court concludes that violating public websites' terms of service, as Wilson and Mislove propose to do for their research, does not constitute a CFAA violation under the "exceeds authorized access" provision.

In coming to this determination, the Court is guided by many of the same reasons that led to a narrow interpretation of "accesses . . . without authorization" that excludes terms-of-service violations. See supra, at 20–22. First, consumer websites' terms of service do not provide adequate notice for purposes of criminal liability. See Drew, 259 F.R.D. at 464–66; see also United States v. Thomas, 877 F.3d 591, 596 (5th Cir. 2017) (recognizing that "a narrow reading of [§ 1030(a)(2)] avoids criminalizing common conduct—like violating contractual terms of service for computer use or using a work computer for personal reasons—that lies beyond the antihacking purpose of the access statutes"). Second, criminalizing violations of private websites' terms of service raises considerable nondelegation issues. See supra, at 20–21.

Third, the rule of lenity and the constitutional avoidance canon weigh against a broad interpretation of "exceeds authorized access" as encompassing terms-of-service violations. As noted above, courts have come to varying opinions on what type of conduct violates this provision. Compare Rodriguez, 628 F.3d at 1263; John, 597 F.3d at 272; Citrin, 440 F.3d at 420–21; Explorica, 274 F.3d at 582–83, with Valle, 807 F.3d at 512–13, 528; WEC Carolina Energy Sols., 687 F.3d at 205–07. Legislative history and statutory structure provide little guidance one way or the other. See, e.g., Valle, 807 F.3d at 526 (finding the legislative history inconclusive on whether a public employee

"exceed[ed] authorized access" in using government computers for personal ends). Because the traditional tools of statutory interpretation do not point definitively one way or the other for whether "exceeds authorized access" encompasses terms-of-service violations on public websites, the rule of lenity requires that the Court adopt the narrower construction. See id. at 526–28. And because this narrow interpretation obviates the need to engage with plaintiffs' thorny First Amendment concerns, constitutional avoidance, too, counsels in favor of this narrow reading. See Bond, 572 U.S. at 855.

Taken together, these considerations make clear that, even if reading "exceeds authorized access" to exclude terms-of-service violations on public websites is not the only reasonable interpretation, adopting the narrow approach is the wisest path forward. In agreement with the clear weight of relevant cases, then, the Court adopts this narrow interpretation of the CFAA and concludes that plaintiffs' proposed research plans do not violate either provision of § 1030(a)(2).

CONCLUSION

For the foregoing reasons, the Court concludes that plaintiffs' research plans do not violate the Access Provision of the CFAA. Because their actions are not criminal, the Court need not wade into the question whether plaintiffs' proposed conduct should receive First Amendment protection. Instead, the Court concludes that the parties' cross-motions for summary judgment are moot, and the case will be dismissed. A separate order will be issued on this date.

/s/
JOHN D. BATES
United States District Judge

Dated: March 27, 2020