UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTIAN W. SANDVIG, et al.,

Plaintiffs,

v.

JEFFERSON B. SESSIONS III, in his official capacity as Attorney General of the United States,

Defendant.

Civil Action No. 16-1368 (JDB)

MEMORANDUM OPINION

It's a dangerous business, reading the fine print. Nearly every website we visit features Terms of Service ("ToS"), those endless lists of dos and don'ts conjured up by lawyers to govern our conduct in cyberspace. They normally remain a perpetual click away at the bottom of every web page, or quickly scrolled past as we check the box stating that we agree to them. But to knowingly violate some of those terms, the Department of Justice tells us, could get one thrown in jail. This reading of federal law is a boon to prosecutors hoping to deter cybercrime. Yet it also creates a dilemma for those with more benign intentions. Plaintiffs in this case, for instance, are researchers who wish to find out whether websites engage in discrimination, but who have to violate certain ToS to do so. They have challenged the statute that they allege criminalizes their conduct, saying that it violates their free speech, petition, and due process rights. First, however, they must show that they have a sufficient injury to make it through the courthouse door, and that their suit is plausible enough to continue. For the following reasons, the Court finds that plaintiffs have standing, and that they can bring one (but not the rest) of their claims.

I. BACKGROUND

This case centers on a few sections of the Computer Fraud and Abuse Act (CFAA), a law dedicated to "deterring the criminal element from abusing computer technology." H.R. Rep. No. 98–894, at 4 (1984). Plaintiffs directly challenge one section, referred to here as the Access Provision, which sweeps in the greatest amount of conduct. The Access Provision states that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section." 18 U.S.C. § 1030(a)(2)(C). The CFAA defines "protected computer" to mean, among other things, "a computer . . . which is used in or affecting interstate or foreign commerce or communication." Id. § 1030(e)(2)(B). This definition encompasses just about all computers hooked up to the Internet—including computers that house website servers. See, e.g., United States v. Nosal, 676 F.3d 854, 859 (9th Cir. 2012). The statute also defines "exceeds authorized access" as "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). Thus, the Access Provision applies to anyone who purposely accesses an Internet-connected computer without authorization, or uses a legitimate authorization to receive or change information that they are not supposed to, and thereby obtains information from the computer.

The CFAA provides for a fine and/or imprisonment for up to one year upon a first violation of the Access Provision, or up to ten years for any further offenses. Id. § 1030(c)(2)(A), (C). However, the punishment for an initial violation rises to a sentence of up to five years' imprisonment if the offense (1) "was committed for purposes of commercial advantage or private financial gain," (2) was "in furtherance of any criminal or tortious act in violation of the

Constitution" or state or federal law, or (3) involved obtaining information valued at more than $5,000. Id. § 1030(c)(2)(B). Thus, meeting one of these three conditions makes a first violation a felony; if none are met, the first violation is a misdemeanor.

Plaintiffs in this case are four professors and a media organization: Christian W. Sandvig of the University of Michigan; Kyratso "Karrie" Karahalios of the University of Illinois; Alan Mislove of Northeastern University; Christopher "Christo" Wilson of Northeastern University; and First Look Media Works, Inc. ("Media Works"), which publishes the online news platform The Intercept. Compl. [ECF No. 1] ¶¶ 13–14, 16–17, 19. Plaintiffs are conducting studies to respond to new trends in real estate, finance, and employment transactions, which increasingly have been initiated on the Internet. Id. ¶¶ 15, 18, 55. Data brokers assemble consumers' information from myriad sources and place consumers into models that include racial, ethnic, socioeconomic, gender, and religious inferences about them. Id. ¶¶ 56–57. After brokers create consumer profiles, those profiles follow consumers around online through tracking technologies such as cookies. Id. ¶¶ 58–59. Tracking allows websites and advertisers to display content targeted at particular groups, based on consumers' inferred characteristics or the sorts of websites they visit. Id. ¶¶ 59–60. But plaintiffs are concerned, "[g]iven the . . . history of racial discrimination in housing and employment," that this technology may be "harnessed for discriminatory purposes." Id. ¶ 61. They are also concerned that, "when algorithms automate decisions, there is a very real risk that those decisions will unintentionally have a prohibited discriminatory effect." Id. ¶ 62.

One way to determine whether members of protected classes are being discriminated against is to engage in "outcomes-based audit testing." Id. ¶ 67. Such testing commonly involves accessing a website or other network service repeatedly, generally by creating false or artificial user profiles, to see how websites respond to users who display characteristics attributed to certain

races, genders, or other classes. Id. ¶ 70. This method is similar to classical paired testing procedures, in which multiple people—identical but for one legally protected trait—apply for the same house or job. Such procedures are often used to uncover violations of housing and employment discrimination laws in the physical world. Id. ¶¶ 41, 50, 52.

Plaintiffs plan to engage, and are engaging, in such audit testing. Sandvig and Karahalios are investigating whether computer programs that decide what to display on real estate websites discriminate against users based on race or other factors. Id. ¶ 82. They are writing a computer program that will create bots—automated agents that will each browse the Internet and interact with websites as a human user might. Id. ¶ 88. Each bot will create a number of distinct user profiles, each of which is called a "sock puppet." Id. ¶ 89. Sandvig and Karahalios will program the bots to visit real estate websites and search for properties, while also engaging in behaviors correlated with members of a particular race. Id. ¶¶ 90–91. Sandvig and Karahalios will use an automatic data recording technique known as scraping to record the properties that each bot sees on the real estate sites. Id. ¶¶ 90, 92. They can then examine their data to determine whether race-associated behaviors caused the sock puppets to see different sets of properties. Id. ¶ 93.

Similarly, Mislove and Wilson plan to conduct a study to see whether hiring websites' algorithms end up discriminating against job seekers based on protected statuses like race or gender. Id. ¶ 107. They will first use bots to crawl the profiles of a random selection of job-seekers to obtain baseline demographic data, then create fake employer profiles so that they can search for candidates and record how the algorithms rank those candidates.[1] Id. ¶¶ 114–17. They will also create fictitious sock-puppet job seeker profiles, and have the fictitious seekers—who

[1] This second step involves both crawling the profiles of ranked candidates to determine their demographic data and scraping to record the overall rankings. Compl. ¶¶ 114–16.

will vary along different demographic axes—apply for fictitious jobs, to examine how the algorithms rank the candidates. Id. ¶¶ 118–19, 121–22. Mislove and Wilson will prevent real people from applying for the false jobs by giving them titles that say "[t]his is not a real job, do not apply," and will delete the fictitious accounts and jobs when they finish. Id. ¶ 120.

Media Works and its journalists seek to investigate online companies, websites, and platforms, including by examining any discriminatory effects of their use of algorithms. Id. ¶ 130.

Mislove and Wilson plan to publish their findings in academic papers, and to bring the results of their research to the public. Id. ¶ 123. Media Works intends to use the results of its journalistic investigations to inform the public about online business practices. Id. ¶ 132. Sandvig and Karahalios do not explicitly claim that they will publish their work, but state that their findings "would produce important new scientific knowledge about the operation of computer systems, discrimination, and cumulative disadvantage." Id. ¶ 94.

Plaintiffs are all aware that their activities will violate certain website ToS. Id. ¶¶ 95, 124, 131. All intend to use scraping to record data, which is banned by many of the websites plaintiffs seek to study. Id.; see id. ¶¶ 70–71. Many of the housing websites that Sandvig and Karahalios will study prohibit the use of bots. Id. ¶¶ 71, 95. All of the hiring websites that Mislove and Wilson will study prohibit the use of sock puppets, and most prohibit crawling. Id. ¶¶ 71, 124. Additionally, some websites control when and how visitors may speak about any information gained through the site—even in other forums—by including non-disparagement clauses in their ToS. Id. ¶ 72. Some sites also have ToS that require advance permission before using the sites for research purposes, which, plaintiffs allege, creates the possibility of viewpoint-discriminatory permission schemes. Id. ¶ 73. Aside from their ToS violations, plaintiffs' experiments will have at most a minimal impact on the operations of the target websites. Id. ¶¶ 96, 125. All plaintiffs

but Media Works have already begun some of the activities involved in their research plans, including activities that require violating websites' TOS. Id. ¶¶ 98, 126.

Plaintiffs claim that they must either refrain from conducting research, testing, and investigations that (they argue) constitute protected speech or expressive activity, or else expose themselves to the risk of prosecution under the Access Provision of the CFAA. Id. ¶ 137. Plaintiffs therefore filed this suit against the Attorney General, raising four causes of action: (1) a facial overbreadth and as-applied challenge under the Free Speech and Free Press Clauses of the First Amendment, id. ¶¶ 180–86; (2) a First Amendment Petition Clause challenge, ¶¶ 187–93; (3) a vagueness claim under the Fifth Amendment's Due Process Clause, id. ¶¶ 194–98; and (4) a claim of unconstitutional delegation to private parties under the Fifth Amendment, id. ¶¶ 199–202. The government has moved to dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) for lack of standing and failure to state a claim. See Mot. to Dismiss [ECF No. 10].

II. DISCUSSION

We begin with the familiar standards that govern Rule 12(b) analysis. When facing a Rule 12(b)(1) motion to dismiss for lack of subject-matter jurisdiction, a plaintiff "bears the burden of showing that he has standing." Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009). Just because a plaintiff makes it through the courthouse doors on one claim does not mean that other claims can tag along; rather, a plaintiff "must demonstrate standing for each claim he seeks to press and for each form of relief that is sought." Town of Chester v. Laroe Estates, Inc., 137 S. Ct. 1645, 1650 (2017) (citation omitted). On a motion to dismiss, plaintiffs must plead facts that, taken as true, raise a plausible standing claim. See Humane Soc'y of the U.S. v. Vilsack, 797 F.3d 4, 8 (D.C. Cir. 2015). The Court must take all facts alleged in the complaint as true and make all reasonable inferences in plaintiffs' favor. See Gulf Coast Mar. Supply, Inc. v. United States, 867

F.3d 123, 128 (D.C. Cir. 2017). However, the Court "may consider materials outside the pleadings in deciding whether to grant a motion to dismiss for lack of jurisdiction." Id.

To survive a motion to dismiss for failure to state a claim under Rule 12(b)(6), a complaint must "contain 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, 570 (2007)). Plausibility does not mean certainty, or that a claim is more likely to succeed than not, but rather that the claim at issue rises "above the speculative level." Twombly, 550 U.S. at 555. In other words: if what plaintiffs lay out in the complaint actually happened, is it more than merely possible that the law has been violated? Plaintiffs cannot meet this standard through "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements." Iqbal, 556 U.S. at 678. Likewise, a court need not accept a plaintiff's legal conclusions, even if they are dressed up as factual allegations. See Sickle v. Torres Advanced Enter. Sols., LLC, 884 F.3d 338, 345 (D.C. Cir. 2018). However, courts must accept as true all facts stated in the complaint, making all reasonable inferences in plaintiffs' favor. Id.

A. THE INTERNET AS PUBLIC FORUM

At the outset, it is necessary to answer a question that affects both the standing and the merits inquiries in this case: what is the First Amendment status of the Internet? And, more particularly, what powers does the government possess to regulate activity on individual websites?

The government bases much of its argument that plaintiffs do not have standing, and that they have not alleged a First Amendment violation, on the premise that this case is about "a private actor's abridgment of free expression in a private forum." Reply in Supp. of Def.'s Mot. to Dismiss ("Def.'s Reply") [ECF No. 15] at 2; see Mem. of P. & A. in Supp. of Def.'s Mot. to Dismiss ("Def.'s Mem.") [ECF No. 10-1] at 10–13, 22–24. This argument finds some support in Supreme

Court case law, which has rejected the First Amendment claims of individuals who wished to distribute handbills or advertise a strike in shopping centers against the wishes of the property owners. See Hudgens v. NLRB, 424 U.S. 507, 520 (1976); Lloyd Corp. v. Tanner, 407 U.S. 551, 567–68 (1972). Private property, the Court determined, does not "lose its private character merely because the public is generally invited to use it for designated purposes." Lloyd, 407 U.S. at 569. Why, then, would it violate the First Amendment to arrest those who engage in expressive activity on a privately owned website against the owner's wishes?

The answer is that, quite simply, the Internet is different. The Internet is a "dynamic, multifaceted category of communication" that "includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue." Reno v. Am. Civil Liberties Union, 521 U.S. 844, 870 (1997). Indeed, "the content on the Internet is as diverse as human thought." Id. (citation omitted). Only last Term, the Supreme Court emphatically declared the Internet a primary location for First Amendment activity: "While in the past there may have been difficulty in identifying the most important places (in a spatial sense) for the exchange of views, today the answer is clear. It is cyberspace . . . ." Packingham v. North Carolina, 137 S. Ct. 1730, 1735 (2017) (citation omitted).

With this special status comes special First Amendment protection. The Packingham Court applied public forum analysis to a North Carolina law that banned former sex offenders from using social media websites, employing intermediate scrutiny because the law was content-neutral. See id. at 1736. The fact that the statute restricted access to particular websites, run by private companies, did not change the calculus. Consider: on one of the sites the Court treated as an exemplar of social media, LinkedIn, "users can look for work, advertise for employees, or review tips on entrepreneurship," id. at 1735—the same activities in which Mislove and Wilson wish to

engage for their research. As the Court warned, the judiciary "must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in [the modern Internet]." Id. at 1736. The government's proposed public/private ownership distinction cannot account for the Court's determination in Packingham that privately-owned sites like Facebook, LinkedIn, and Twitter are part of a public forum, government regulation of which is subject to heightened First Amendment scrutiny. The Internet "is a forum more in a metaphysical than in a spatial or geographic sense, but the same principles are applicable." Rosenberger v. Rector & Visitors of Univ. of Virginia, 515 U.S. 819, 830 (1995).

An analogy to the real world, while necessarily imperfect, may help illustrate the point. Stroll out onto the National Mall on any day with decent weather and you will discover a phalanx of food trucks lining the streets. Those food trucks are privately owned businesses. Customers interact with them for the private purpose of buying a meal. If they were a brick-and-mortar store on private property, they would encounter no First Amendment barrier to removing a patron who created a ruckus. Yet if a customer standing on a public sidewalk tastes her food and then yells at those in line behind her that they should avail themselves of the myriad other culinary options nearby, the truck could not call the police to arrest her for her comments. She is in a public forum, and her speech remains protected even when she interacts with a private business located within that forum.

It makes good sense to treat the Internet in this manner. "Each medium of expression . . . must be assessed for First Amendment purposes by standards suited to it, for each may present its own problems." Se. Promotions, Ltd. v. Conrad, 420 U.S. 546, 557 (1975). Regulation of the Internet presents serious line-drawing problems that the public/private distinction in physical space does not. The decisions in Lloyd and Hudgens concerned "property privately owned and used

nondiscriminatorily for private purposes only." Lloyd, 407 U.S. at 568. It is difficult to argue that most websites readily meet this description. As the Supreme Court has recognized, the Internet "provides relatively unlimited, low-cost capacity for communication of all kinds." Reno, 521 U.S. at 870. Much of this communication takes place on websites that, in the physical world, would be seen solely as private, commercial spaces. Take Amazon.com. As a "popular retail website," Amazon undoubtedly has a private use "as a seller of products." Packingham, 137 S. Ct. at 1741 (Alito, J., concurring in the judgment). Yet the site also "facilitates the social introduction of people for the purpose of information exchanges," since it "allows a user to create a personal profile" and, "[w]hen someone purchases a product on Amazon, the purchaser can review the product and upload photographs, and other buyers can then respond to the review." Id. Conversely, Facebook—to which the Court pointed in Packingham as a quintessential site for protected First Amendment activity—allows users to buy and sell products in its Marketplace, and, like many social media sites, sells ads to make revenue.[2] Simply put: the public Internet is too heavily suffused with First Amendment activity, and what might otherwise be deemed private spaces are too blurred with expressive spaces, to sustain a direct parallel to the physical world.

At the same time, however, it would be ill-advised to "equate the entirety of the [I]nternet with public streets and parks." Id. at 1738 (emphasis added). To do so would "gloss[] over the dual public and private nature of digital arenas," and subject to heightened scrutiny regulations on even the Internet's most secluded nooks and crannies. Note, First Amendment-Freedom of Speech-Public Forum Doctrine-Packingham v. North Carolina, 131 Harv. L. Rev. 233, 238 (2017). Rifling through a business's confidential files is no less a trespass merely because those files are located in the cloud. A hacker cannot legally break into a Gmail account and copy the account-

[2] See Facebook, Facebook Ads, https://www.facebook.com/business/products/ads; Facebook, Marketplace, https://www.facebook.com/marketplace/learn-more.

holder's emails, just as a busybody cannot legally reach into someone else's mailbox and open her mail. The First Amendment does not give someone the right to breach a paywall on a news website any more than it gives someone the right to steal a newspaper.

What separates these examples from the social media sites in Packingham is that the owners of the information at issue have taken real steps to limit who can access it. But simply placing contractual conditions on accounts that anyone can create, as social media and many other sites do, does not remove a website from the First Amendment protections of the public Internet. If it did, then Packingham—which examined a law that limited access to websites that require user accounts for full functionality—would have come out the other way. 137 S. Ct. at 1737; see also Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1658 (2003) ("Applying a contract-based theory of authorization in a criminal context . . . may be constitutionally overbroad, criminalizing a great deal beyond core criminal conduct, including acts protected by the First Amendment."). Rather, only code-based restrictions, which "carve[] out a virtual private space within the website or service that requires proper authentication to gain access," remove those protected portions of a site from the public forum. Orin S. Kerr, Essay, Norms of Computer Trespass, 116 Colum. L. Rev. 1143, 1171 (2016). Stealing another's credentials, or breaching a site's security to evade a code-based restriction, therefore remains unprotected by the First Amendment.

To return to the National Mall example, suppose that a food truck remains stationed on the Mall but boards up for the night, and the owner returns home. By shutting the food in a truck, perhaps along with her cooking instructions, the owner has placed a barrier between that property and the public forum outside. Thus, while the police could not arrest a customer for telling others in line that the food tastes terrible, or for reading the menu on the truck's exterior, they could arrest

that customer for breaking into the boarded-up truck seeking confidential culinary information. This is true even if the customer claimed she was doing so in order to broadcast to the world the truck's substandard ingredients and ill-conceived recipes. While the First Amendment has free rein on the Mall generally, it does not protect those who circumvent barriers that demarcate private areas, even if those private areas are surrounded by an otherwise public forum. This distinction guides the Court's analysis here.

B. STANDING

Before reaching the merits of plaintiffs' claims, the Court must assure itself that they have standing—a sufficient stake to transform this dispute into one of the "Cases" or "Controversies" on which federal courts may pass judgment. U.S. Const. art. III, § 2. "The 'irreducible constitutional minimum of standing contains three elements': (1) injury-in-fact, (2) causation, and (3) redressability." Rainbow/PUSH Coal. v. FCC, 330 F.3d 539, 542 (D.C. Cir. 2003) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). Plaintiffs must plead or prove each element of standing "with the manner and degree of evidence required at the successive stages of the litigation." Lujan, 504 U.S. at 561. Here, therefore, "general factual allegations of injury resulting from the defendant's conduct may suffice" to allege standing, "for on a motion to dismiss we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" Id. (alteration in original) (citation omitted). For any given claim or form of relief, "the presence of one party with standing is sufficient" to reach the issue. Rumsfeld v. Forum for Acad. & Institutional Rights, Inc., 547 U.S. 47, 53 n.2 (2006).

Because this is a pre-enforcement challenge, plaintiffs must meet more specific conditions to satisfy the injury-in-fact requirement. They must plausibly allege "an intention to engage in a course of conduct [1] arguably affected with a constitutional interest, but [2] proscribed by a

statute, and [3] [that] there exists a credible threat of prosecution thereunder." Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2342 (2014) (quoting Babbitt v. United Farm Workers Nat'l Union, 442 U.S. 289, 298 (1979)). The government argues that plaintiffs cannot meet this test. See Def.'s Mem. at 8–19. Plaintiffs contend that they do intend to engage in constitutionally protected speech, and that they have pled a credible threat of prosecution. See Pls.' Mem. of P. & A. in Opp'n to Def.'s Mot. to Dismiss ("Pls.' Mem.") [ECF No. 13] at 18–30. It is clear that any injury to plaintiffs is caused by the government's criminalization of websites' ToS, and that the declaratory and injunctive relief plaintiffs seek, see Compl. at 46–47, would redress the injury. Therefore, the question is whether plaintiffs allege a sufficient injury in the first place.

Generally speaking, a court's standing analysis must be "especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." Raines v. Byrd, 521 U.S. 811, 819–20 (1997). However, the D.C. Circuit has interpreted the Supreme Court's pre-enforcement standing doctrine broadly in the First Amendment sphere. Indeed, "the courts have shown special solicitude to pre-enforcement challenges brought under the First Amendment." N.Y. Republican State Comm. v. SEC, 799 F.3d 1126, 1135 (D.C. Cir. 2015). Therefore, the Circuit has found, "the courts' willingness to permit pre-enforcement review is 'at its peak' when claims are rooted in the First Amendment." Id. at 1135 (citation omitted). "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) (quoting Driehaus, 134 S. Ct. at 2345), reh'g en banc denied, 855 F.3d 381 (D.C. Cir.), cert. docketed, No. 17-504 (U.S. Oct. 3, 2017). Nor need they show that they are likely to be prosecuted. Rather, "[s]tanding '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. (quoting Act Now to Stop War & End Racism Coal. v. District of Columbia (ANSWER I), 589 F.3d 433, 435 (D.C. Cir. 2009)).

1. "Arguably Affected With a Constitutional Interest"

Plaintiffs assert that their conduct falls within three categories of First Amendment-protected activity. Scraping data from their target websites, they allege, is subject to the First Amendment right to record or preserve information. Pls.' Mem. at 10–14. Moreover, employing bots and sock puppets and creating false user accounts constitute harmless false speech. Id. at 14–17. And their planned post-research activities are protected by the right to publish. Id. at 17–18. All of these claims are sufficiently plausible to conclude that plaintiffs' proposed conduct is "arguably affected with a constitutional interest." Driehaus, 134 S. Ct. at 2342.

First, scraping plausibly falls within the ambit of the First Amendment. "[T]he First Amendment goes beyond protection of the press and the self-expression of individuals to prohibit government from limiting the stock of information from which members of the public may draw." First Nat. Bank of Boston v. Bellotti, 435 U.S. 765, 783 (1978). The Supreme Court has made a number of recent statements that give full First Amendment application to the gathering and creation of information.[3] Additionally, six courts of appeals have found that individuals have a First Amendment right to record at least some matters of public interest, in order to preserve and

[3] See Packingham, 137 S. Ct. at 1737 (holding that banning people from "gain[ing] access to information," "knowing current events," and "checking ads for employment" through social media inhibits "the legitimate exercise of First Amendment rights"); Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011) ("This Court has held that the creation and dissemination of information are speech within the meaning of the First Amendment. Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs." (citations omitted)); Brown v. Entm't Merchants Ass'n, 564 U.S. 786, 792 n.1 (2011) ("Whether government regulation applies to creating, distributing, or consuming speech makes no difference."); Citizens United v. FEC, 558 U.S. 310, 340 (2010) ("Laws enacted to control or suppress speech may operate at different points in the speech process . . . .").

disseminate ideas.[4] That plaintiffs wish to scrape data from websites rather than manually record information does not change the analysis. Scraping is merely a technological advance that makes information collection easier; it is not meaningfully different from using a tape recorder instead of taking written notes, or using the panorama function on a smartphone instead of taking a series of photos from different positions. And, as already discussed, the information plaintiffs seek is located in a public forum. Hence, plaintiffs' attempts to record the contents of public websites for research purposes are arguably affected with a First Amendment interest.

Second, plaintiffs have a First Amendment interest in harmlessly misrepresenting their identities to target websites. The complaint alleges that plaintiffs' research requires them to create false employer and job-seeker profiles on employment websites, and to use sock puppets to make it appear to a number of housing and employment sites that multiple people are accessing the information they have made available. Compl. ¶¶ 88–93, 114–21. Because "some false statements are inevitable if there is to be an open and vigorous expression of views in public and private conversation," and because "[t]he Government has not demonstrated that false statements generally should constitute a new category of unprotected speech," false claims that are not "made to effect a fraud or secure moneys or other valuable considerations" fall within First Amendment protection. United States v. Alvarez, 567 U.S. 709, 718, 722–23 (2012). Plaintiffs allege that their conduct will cause minimal, if any, harm to the targeted websites, and that they will take steps to avoid affecting third-party users of the website (such as informing job seekers that their fake

[4] See Gericke v. Begin, 753 F.3d 1, 7 (1st Cir. 2014); Fields v. City of Philadelphia, 862 F.3d 353, 359 (3d Cir. 2017); Turner v. Lieutenant Driver, 848 F.3d 678, 688–89 (5th Cir. 2017); ACLU of Ill. v. Alvarez, 679 F.3d 583, 595 (7th Cir. 2012); Animal Legal Def. Fund v. Wasden, 878 F.3d 1184, 1203 (9th Cir. 2018); W. Watersheds Project v. Michael, 869 F.3d 1189, 1195–97 (10th Cir. 2017); Smith v. City of Cumming, 212 F.3d 1332, 1333 (11th Cir. 2000); see also Rideout v. Gardner, 838 F.3d 65, 75 (1st Cir. 2016), cert. denied, 137 S. Ct. 1435 (2017) (stating that "[t]here are strong First Amendment interests" in photographically recording one's own completed ballot, because the "'use of illustrations or pictures . . . serves important communicative functions'" (citation omitted)).

positions are fake). Compl. ¶¶ 96, 120, 125. Thus, plaintiffs' harmless false or misleading speech to website owners is arguably affected with a constitutional interest.[5]

Third, plaintiffs contend that they have the right, and the desire, to publish the results of their research, and that some sites' ToS prohibit them from doing so without prior permission or else employ anti-disparagement clauses. Pls.' Mem. at 17. The Supreme Court has made very clear that the right to publish falls within the core of the First Amendment's protections. See, e.g., Bartnicki v. Vopper, 532 U.S. 514, 527 (2001) ("As a general matter, 'state action to punish the publication of truthful information seldom can satisfy constitutional standards.'" (quoting Smith v. Daily Mail Publishing Co., 443 U.S. 97, 102 (1979)). Applying criminal sanctions for publishing original material that uses publicly available information, or for making negative statements about a website, triggers First Amendment scrutiny.

The government raises two overarching objections to all of these alleged rights. It initially claims that the First Amendment does not regulate the decisions that private entities make about how to control access to their private websites—in other words, that there is no state action here. See Def.'s Mem. at 21–24; Def.'s Reply at 6–12; see also Columbia Broad. Sys., Inc. v. Democratic Nat. Comm., 412 U.S. 94, 114 (1973) ("[The First Amendment] is a restraint on government action, not that of private persons."). However, private speech prohibitions can still implicate the First Amendment when given the imprimatur of state protection through civil or criminal law. See, e.g., New York Times Co. v. Sullivan, 376 U.S. 254, 265 (1964). Moreover, plaintiffs claim injury from a potential criminal action against them—and "a criminal prosecution under the CFAA would undoubtedly constitute state action" because the government itself is

[5] The government counters that Alvarez and the cases that follow it do not "address facially neutral statutes of general applicability, such as the CFAA." Def.'s Reply at 10. However, that goes to the standard of review on the merits rather than to whether plaintiffs' activities are imbued with any First Amendment interest at all.

policing website ToS violations. hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099, 1114 n.12 (N.D. Cal. Aug. 14, 2017), appeal docketed, No. 17-16783 (9th Cir. Sept. 6, 2017).

The government also claims that the First Amendment does not protect plaintiffs' conduct because, under Zemel v. Rusk, 381 U.S. 1, 16–17 (1965), and Houchins v. KQED, Inc., 438 U.S. 1, 10–11 (1978) (plurality opinion), the First Amendment does not create a right to acquire information in whatever manner one desires. Def.'s Mem. at 10–12. In Zemel, the Court held that the government did not implicate any First Amendment rights by refusing to issue the plaintiff a passport to visit Cuba, which the plaintiff claimed interfered with his ability to acquaint himself with the effects of the government's policies in relation to Cuba. 381 U.S. at 16. The Court rejected the claim, stating that "[t]he right to speak and publish does not carry with it the unrestrained right to gather information." Id. at 17. Then, in Houchins, the Court held that journalists had no special First Amendment right to access inmates in a jail just because they sought to write stories about the jail; the Court rejected the "notion that the First Amendment confers a right of access to news sources." 438 U.S. at 11. However, the Court did note that "[t]he right to receive ideas and information is not the issue in this case," and that "[t]he issue is a claimed special privilege of access." Id. at 12. Thus, "[t]here is an undoubted right to gather news 'from any source by means within the law,'" but the First Amendment does not "compel[] others—private persons or governments—to supply information." Id. at 11.

Here, plaintiffs are not asking the Court to force private websites to provide them with information that others cannot get. Instead, they seek only to prevent the government from prosecuting them for obtaining or using information that the general public can access—though they wish to do so in a manner that could have private consequences, such as a website banning them or deleting their accounts. See Compl. ¶ 4 ("[Plaintiffs] have no intent . . . to access any data

or information that is not made available to the public."). Because plaintiffs neither want a special privilege of access nor seek to force websites to give them otherwise unobtainable information, the Zemel and Houchins line of cases is inapposite here. Plaintiffs therefore plausibly allege that their conduct is arguably affected with a constitutional interest.

2. "Proscribed by a Statute"

Under D.C. Circuit precedent, "at the motion to dismiss stage, a plaintiff's non-frivolous contention regarding the meaning of a statute must be taken as correct for purposes of standing." Info. Handling Servs., Inc. v. Def. Automated Printing Servs., 338 F.3d 1024, 1030 (D.C. Cir. 2003). Because plaintiffs' reading of the statute to encompass all ToS violations is not frivolous, and because plaintiffs allege that their conduct would violate websites' ToS, it is clear for standing purposes that their intended actions would violate the statute.

The government contests this conclusion in only one instance. In two sentences in its reply brief, the government claims that plaintiffs lack standing for any injuries relating to their ability to publish. As the government sees it, "[t]he Complaint contains no allegation that any website on which plaintiffs intend to conduct their activity contains" a restriction on future publication, "and plaintiffs lack standing to assert claims based on hypothetical circumstances." Def.'s Reply at 12.

This argument is unavailing. True, plaintiffs do not explicitly allege that their target websites restrict subsequent publication. But the complaint does allege that "[p]laintiffs wish to . . . report on their findings to the public," and that "[t]he research, testing, and investigative methods they have designed would, if carried out, violate the [Access] Provision, because they all require violating the [ToS] of the targeted website." Compl. ¶¶ 134–35 (emphasis added); see also id. ¶ 160 ("Plaintiffs wish to have the option of publishing the results of their research, including any findings of discrimination, even if a target website's ToS prohibit doing so."). "[O]n a motion

to dismiss we presum[e] that general allegations embrace those specific facts that are necessary to support the claim." Food & Water Watch, Inc. v. Vilsack, 808 F.3d 905, 913 (D.C. Cir. 2015) (second alteration in original) (citation omitted). Plaintiffs' allegations allow for the presumption that reporting on their research findings would violate some targeted websites' ToS. While far from the degree of proof necessary for summary judgment, see Lujan, 504 U.S. at 561, at this early stage plaintiffs have plausibly alleged that the CFAA prevents all of their conduct.

3. "Credible Threat of Prosecution"

Even if plaintiffs' intended conduct is arguably affected with a constitutional interest, and is prohibited by the CFAA, plaintiffs still must show that there is a credible threat of prosecution for that conduct under the statute. See Driehaus, 134 S. Ct. at 2342. The government asserts that plaintiffs cannot meet this test, because "plaintiffs make no allegation that the government has threatened them with CFAA enforcement," plaintiffs "cite no instances in which the government has enforced the challenged provision for harmless [ToS] violations," and DOJ "has expressly stated that it has no intention of prosecuting harmless [ToS] violations that are not in furtherance of other criminal activity or tortious conduct." Def.'s Reply at 13. The government is, for the most part, correct on the facts. The complaint does not allege that plaintiffs have actually been threatened with prosecution. The two cases plaintiffs cite to show that prosecutors have used the Access Provision to punish ToS violations did, in fact, involve harmful conduct. And DOJ's guidance to federal prosecutors does discourage them—though somewhat tepidly—from bringing CFAA cases based solely on harmless ToS violations. See U.S. Att'y Gen., Intake and Charging Policy for Computer Crimes Matters ("Charging Policy") (Sept. 11, 2014) [ECF No. 15–1] at 5.

However, both Supreme Court and D.C. Circuit precedent create a low standing bar in cases like this one. Because plaintiffs "challenge [a] law[] burdening expressive rights," and

because their complaint provides "a credible statement . . . of intent to commit violative acts," plaintiffs may rely on the "conventional background expectation that the government will enforce the law." U.S. Telecom Ass'n, 825 F.3d at 739 (citation omitted); accord Act Now to Stop War & End Racism Coal. v. District of Columbia (ANSWER II), 846 F.3d 391, 401–02 (D.C. Cir. 2017), cert. denied, 138 S. Ct. 334 (2017) (mem.). Indeed, the D.C. Circuit has occasionally found standing without inquiring into whether the government has actually enforced the challenged restriction. See U.S. Telecom Ass'n, 825 F.3d at 739–40.

Here, there are sufficient indications of a credible threat to enforce the Access Provision, both in general and as applied to plaintiffs' activities. To begin with, the parties have sparred over whether DOJ has enforced the Access Provision specifically against harmless ToS violations. See Compl. ¶ 31; Def.'s Mem. at 14–17; Pls.' Mem. at 3–4, 25. Yet a number of cases have looked to whether the statutory provision as a whole—or at least the particular term being challenged—has been enforced through prosecutions, without asking whether the facts were similar to those the plaintiffs alleged. See, e.g., Holder v. Humanitarian Law Project, 561 U.S. 1, 16 (2010); Babbitt, 442 U.S. at 302; N. Carolina Right to Life, Inc. v. Bartlett, 168 F.3d 705, 710 (4th Cir. 1999). If one need only find a history of enforcement of the Access Provision generally, or enforcement of the "exceeds authorized access" language in particular, plaintiffs would have no trouble showing that there is a significant history. Indeed, the Supreme Court decided a case just two years ago that involved a prosecution under the Access Provision, in part for exceeding authorized access. Musacchio v. United States, 136 S. Ct. 709, 713 & n.1 (2016).[6]

[6] For some other recent examples, see United States v. Batti, 631 F.3d 371, 372 (6th Cir. 2011); United States v. Willis, 476 F.3d 1121, 1124 (10th Cir. 2007); United States v. Cave, No. 8:12CR417, 2013 WL 3766550, at *1 (D. Neb. July 16, 2013); United States v. Roque, No. CRIM. 12-540 KM, 2013 WL 2474686, at *1 (D.N.J. June 6, 2013); United States v. Auernheimer, No. 11-CR-470 SDW, 2012 WL 5389142, at *1 (D.N.J. Oct. 26, 2012), rev'd, 748 F.3d 525 (3d Cir. 2014); United States v. Aleynikov, 737 F. Supp. 2d 173, 190 (S.D.N.Y. 2010).

Even looking more closely at similar factual scenarios, plaintiffs have shown that prosecutions have stemmed from close enough facts that it would be credible to fear a future prosecution for their own activities. Plaintiffs cite two cases in which individuals were prosecuted under the Access Provision for violating ToS agreements: United States v. Lowson, No. 10-cr-114 (KSH), 2010 WL 9552416 (D.N.J. Oct. 12, 2010), and United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009). Compl. ¶ 31. Lowson, as the government points out, did not solely involve violations of website ToS; it also involved ticket scalpers' attempts "to defeat code-based security restrictions" on Ticketmaster's website. 2010 WL 9552416, at *5. However, the indictment alleged "both contract- and code-based violations," id. at *6, and laid out the websites' prohibitions that the defendants allegedly violated, see Superseding Indictment at 5–9, Lowson, 2010 WL 9552416 (No. 10-cr-114), ECF No. 10-2. More directly on point is Drew, in which the government prosecuted a woman for lying about her age and creating a false account on Myspace in order to cyberbully her daughter's teenage classmate—thus violating Myspace's ToS in order to commit the tort of intentional infliction of emotional distress. 259 F.R.D. at 452. Prosecutors included both a felony count under the Access Provision—because the violation was in furtherance of a tortious act—and a misdemeanor count for the standalone ToS violations. Id. at 451. The jury acquitted Drew on the felony count, id.; the court then dismissed the misdemeanor conviction, as coverage of ToS violations rendered the Access Provision unconstitutionally vague, id. at 467.

That the government brought the Drew case without enough evidence to ultimately prove the added harm required for a felony conviction, and chose to include a misdemeanor count for harmless ToS violations, lends some credibility to plaintiffs' fears of prosecution. The government also does not know whether prosecutors may have employed the Access Provision to obtain plea agreements in which defendants admitted to harmless ToS violations. See Tr. of Mot. Hr'g [ECF

No. 20] at 17:15–18:13.[7] These prior prosecutions, whether under the Access Provision generally or under related factual circumstances, provide "somewhat more than the 'conventional background expectation that the government will enforce the law.'" ANSWER I, 589 F.3d at 435 (citation omitted). Thus, even if more were necessary, plaintiffs have provided it.

Finally, the government has not expressly disavowed any intent to prosecute plaintiffs, which would defeat the normal expectation of enforcement. The government points to a 2014 memorandum that the Attorney General sent to United States Attorneys regarding charging policy under the CFAA, which the government claims is the current "binding guidance" on this issue. Def.'s Reply at 14. According to the government, plaintiffs' fear of prosecution is "implausible" because (1) the charging policy focuses on several factors that would not apply to harmless ToS violations, (2) prosecutions based solely on such violations are discouraged, and (3) attorneys must consult with the Criminal Division of DOJ before making CFAA charging decisions. Id. However, to disprove an otherwise credible threat of prosecution, courts have normally required an explicit statement "that plaintiffs will not be prosecuted if they do what they say they wish to do." Humanitarian Law Project, 561 U.S. at 16. The government has not made such a declaration. DOJ's charging policy states that, "if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or [ToS] with an Internet service provider or website, federal prosecution may not be warranted." Charging Policy at 5 (emphasis added). This is a far cry from the sort of disavowal required by case law.[8]

[7] It also matters that the CFAA is a civil as well as a criminal statute. The possibility of administrative or private civil actions, even without a threat of criminal prosecution, may buttress—or perhaps independently provide—standing for pre-enforcement challenges. See, e.g., Babbitt, 442 U.S. at 302 n.13; Chamber of Commerce v. FEC, 69 F.3d 600, 603 (D.C. Cir. 1995).

[8] The government also offers the statement of the Deputy Assistant Attorney General for the Criminal Division before a congressional subcommittee in 2015, in which the DAAG stated that DOJ "has no interest in prosecuting harmless violations of use restrictions" and suggested amending the CFAA so that it would essentially only apply to the acts that currently give rise to a felony under the Access Provision. Statement of David M. Bitkower, Deputy Ass't Att'y Gen., Crim. Div., Dep't of Justice, Before the Subcomm. On Crime and Terrorism, S. Comm. on

In an attempt to provide such a disavowal, and at the Court's suggestion, the government filed an affidavit from John T. Lynch, Jr., Chief of the Computer Crime and Intellectual Property Section of the Criminal Division of DOJ. Aff. of John T. Lynch, Jr. [ECF No. 21-1]. He points to the charging factors mentioned above, id. at 2–3, and states that he "do[es] not expect that the Department would bring a CFAA prosecution based on such facts and de minimis harm," id. at 3. But many things that we do not expect in fact come to pass. An official's prognostication does not substitute for a declaration of non-prosecution. Moreover, even explicit disavowals are most valuable when they are made "on the basis of the Government's own interpretation of the statute and its rejection of plaintiffs' interpretation as unreasonable." Blum v. Holder, 744 F.3d 790, 798 (1st Cir. 2014). Here, the government has implicitly—and in past prosecutions, explicitly—read the Access Provision to include ToS violations. See Charging Policy at 4–5. "[T]o rely upon prosecutorial discretion to narrow the otherwise wide-ranging scope of a criminal statute's highly abstract general statutory language places great power in the hands of the prosecutor." Marinello v. United States, No. 16-1144, 2018 WL 1402426, at *6 (U.S. Mar. 21, 2018). The Constitution "does not leave us at the mercy of noblesse oblige," United States v. Stevens, 559 U.S. 460, 480 (2010), which is all the government ultimately offers.

One final point. Until now, this standing analysis has focused on plaintiffs' First Amendment challenge. But plaintiffs also bring due process claims. In Seegars v. Gonzales, 396 F.3d 1248 (D.C. Cir. 2005), the D.C. Circuit applied a more rigorous "imminence" standard for non-First-Amendment constitutional claims. But the court took pains to point out that it was forced to follow circuit precedent that conflicted with the Supreme Court's and the D.C. Circuit's own

the Judiciary (July 8, 2015) [ECF No. 10-3] at 6. However, this is no stronger a disavowal than is DOJ's statement in its charging policy. Moreover, Congress never adopted DOJ's proposed amendments.

laxer standing test for First Amendment pre-enforcement challenges. See id. at 1252–54. Subsequent cases have confirmed that the "more demanding standard" required by Seegars does not apply when challenging "laws burdening expressive rights." ANSWER I, 589 F.3d at 435. Here, plaintiffs' Fifth Amendment claims allege an injury-in-fact essentially identical to that alleged for their First Amendment claims. Pls.' Mem. at 23 n.2. Both the Supreme Court and the D.C. Circuit have upheld standing for dual First- and Fifth-Amendment pre-enforcement challenges, under a less rigorous imminence standard, without distinguishing between the two amendments for standing purposes. See Humanitarian Law Project, 561 U.S. at 11–12, 15–16; ANSWER II, 846 F.3d at 396, 401–02; ANSWER I, 589 F.3d at 434–35. Plaintiffs therefore have standing to bring their Fifth Amendment claims along with their First Amendment ones.

For the foregoing reasons, plaintiffs have plausibly pled standing at the motion to dismiss stage, and the government's Rule 12(b)(1) motion will be denied.

C. INTERPRETING THE STATUTE

Plaintiffs allege only constitutional claims in this case. Likely because they are bringing a pre-enforcement challenge, they are not claiming that the statute, properly read, does not apply to them. However, nearly all of their claims require the Court to determine the reach of the Access Provision before deciding the constitutional question. Since the Court does not accept plaintiffs' legal conclusions as true for purposes of a motion to dismiss under Rule 12(b)(6), see Doe v. Rumsfeld, 683 F.3d 390, 391 (D.C. Cir. 2012), plaintiffs' reading of the statute to cover their conduct does not control. Instead, the Court must interpret the law.

Courts are split as to how to read the relevant provisions. The CFAA defines the phrase "exceeds authorized access" as "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). The Second, Fourth, and Ninth Circuits have held that this language prohibits only unauthorized access to information. See United States v. Valle, 807 F.3d 508, 523–28 (2d Cir. 2015); WEC Carolina Ener. Solutions LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012); Nosal, 676 F.3d at 863; see also Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295, 304 (6th Cir. 2011) (stating, based on Ninth Circuit precedent, that "an individual who is authorized to use a computer for certain purposes but goes beyond those limitations . . . has 'exceed[ed] authorized access'" (citation omitted) (alteration in original)). Meanwhile, the First, Fifth, and Eleventh Circuits have held that it also covers (at least in some instances) unauthorized use of information that a defendant was authorized to access only for specific purposes. See EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583 (1st Cir. 2001); United States v. John, 597 F.3d 263, 271 (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010); see also Int'l Airport Centers, LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (holding that an employee who deleted his employer's files in violation of his employment contract had terminated the agency relationship that authorized him to access the information). Courts have also split over whether violating a website's ToS exceeds authorized access for purposes of the CFAA.[9] The D.C. Circuit has never opined on either question. Several district judges in this

[9] Compare Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) ("[A] violation of the terms of use of a website—without more—cannot establish liability under the CFAA."), cert. denied 138 S. Ct. 313 (2017) (mem.); Valle, 807 F.3d at 528 (rejecting unauthorized use reading of "exceeds authorized access" because "the government's interpretation of 'exceeds authorized access' makes every violation of a private computer use policy a federal crime"); WEC Carolina, 687 F.3d at 206 (noting that the unauthorized use reading "would impute liability to an employee who with commendable intentions disregards his employer's policy against downloading information to a personal computer so that he can work at home"), with EarthCam, Inc. v. OxBlue Corp., 703 Fed. App'x 803, 808 & n.2 (11th Cir. 2017) (stating that "one of the lessons from [circuit precedent] may be that a person exceeds authorized access if he or she uses the access in a way that contravenes any policy or term of use governing the computer in question," and noting the dissenting views of other circuits); CollegeSource, Inc. v. AcademyOne, Inc., 597 Fed. App'x 116, 130 (3d Cir. 2015) (suggesting that defendants can be prosecuted under the CFAA if they "breach[ed] any technological barrier or contractual term of use"); EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. 2003) ("A lack of authorization could be established by an explicit statement on the website restricting access. . . . Many webpages contain lengthy limiting conditions, including limitations on the use of scrapers.").

Circuit, however, have held that the provision only applies to unauthorized access to information, not to unauthorized use of properly accessed material. See Hedgeye Risk Mgmt., LLC v. Heldman, 271 F. Supp. 3d 181, 194–95 (D.D.C. 2017) (collecting cases).

At one point in their briefing, plaintiffs suggest a different dividing line: a limiting construction that carves out harmless ToS violations from the statute. Pls.' Mem. at 31–33, 35. However, "[t]he text will not bear such a reading." INS v. Yueh-Shaio Yang, 519 U.S. 26, 30 (1996). It is one thing to carve out such violations by determining that the statute is unconstitutional as applied, but the text of the statute itself—"exceeds authorized access"—and its statutory definition do not appear to allow for such a surgical slicing off of conduct. How does the text differentiate between ToS violations and violations of employers' computer use policies, for instance? And how does the text distinguish between "[ToS] violations alone," Pls.' Mem. at 35, and ToS violations that cause damage or involve fraud, which plaintiffs admit are covered by §§ 1030(a)(4) and (a)(5), id. at 31–32? One can just as easily "use [authorized] access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter," § 1030(e)(6), whether it is a website or some other entity that is doing the authorizing, and whether the violation is harmful or harmless.

The question thus remains whether "exceeds authorized access" refers to access alone or to access, use, and other violations. The Court finds the narrow interpretation adopted by the Second, Fourth, and Ninth Circuits—and by numerous other district judges in this Circuit—to be the best reading of the statute. First, the text itself more naturally reads as limited to violations of the spatial scope of one's permitted access. To "exceed[] authorized access," one must have permission to access the computer at issue, and must "use such access"—i.e., one's authorized presence on the computer—"to obtain or alter information in the computer." Id. Thus, unlike the

phrase "unauthorized access" used alongside it in several CFAA provisions, the phrase "exceeds authorized access" refers not to an outside attack but rather to an inside job. See, e.g., Nosal, 676 F.3d at 858. The rest of the definition requires that the information at issue be information "that the accesser is not entitled so to obtain or alter." Id. The key word here is "entitled." "And, in context, the most 'sensible reading of "entitled" is as a synonym for "authorized."'" Hedgeye, 271 F. Supp. 3d at 194 (quoting Nosal, 676 F.3d at 857). The focus is thus on whether someone is allowed to access a computer at all, in the case of "unauthorized access," or on whether someone is authorized to obtain or alter particular information, in the case of "exceeds authorized access." In neither instance does the statute focus on how the accesser plans to use the information.[10]

The statutory context buttresses this narrower reading of the text. Reading "exceeds authorized access" to turn on the accesser's purpose in seeking out the information would eliminate a major difference between the Access Provision—which has no purpose requirement—and other provisions that require intent to defraud. E.g., 18 U.S.C. § 1030(a)(4). It would also water down the difference between the misdemeanor penalty provisions and the felony provisions that enhance sentences for violations committed for fraud or financial gain. Id. § 1030(c)(2); see also S. Rep. No. 104-357, at 8 (1996) ("[T]he statutory penalties are structured to provide that obtaining information of minimal value is only a misdemeanor, but obtaining valuable information, or misusing information in other more serious ways, is a felony." (emphasis added)). After all, just about any attempt to use proprietary information to defraud or for personal or commercial gain would likely violate a computer use policy or website ToS. See Nosal, 676 F.3d at 858 n.4.

[10] Nor does the word "so," which has inspired a good deal of exegesis in prior opinions, see WEC Carolina, 687 F.3d at 205–06; Nosal, 676 F.3d at 857–58, meaningfully change this focus. Read in the context of the phrase "so to obtain or alter," "so" most naturally refers back to the earlier phrase "such access," emphasizing that the accesser must not have been entitled to obtain or alter that particular information through the particular authorization used—even if, theoretically, there were another way in which the accesser might legally obtain or alter the information.

Congress knew how to draft a specific intent requirement, and did so in these other sections of the CFAA. It would be rather odd, then, for Congress to also smuggle a specific intent factor into its definition of the actus reus of the offense. While this context is certainly not dispositive—Congress often drafts overlapping or even redundant provisions—it is best to avoid readings that "would render superfluous another part of the same statutory scheme." Marx v. Gen. Revenue Corp., 568 U.S. 371, 386 (2013).

Legislative history also points to an access-based, rather than an intended-use-based, reading of "exceeds authorized access." The Second Circuit has already canvassed in great detail the congressional intent and history behind the definition of "exceeds authorized access," see Valle, 807 F.3d at 525–26, and this Court will not repeat it here. This Court agrees with the Second Circuit, however, that "the legislative history consistently characterizes the evil to be remedied—computer crime—as 'trespass' into computer systems or data, and correspondingly describes 'authorization' in terms of the portion of the computer's data to which one's access rights extend." Id. at 525. Congress thus viewed exceeding authorized access as the digital equivalent of being allowed into a house but entering a room within it that the owner has declared to be off-limits. A sensible conception, particularly considering that the language at issue was written in 1986—before the World Wide Web or websites existed. See Kerr, Norms of Computer Trespass, supra, at 1161.

The amendment history of the definition supports this reading. The initial language of the CFAA applied to anyone who, knowingly "having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend, and thereby obtains information." Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, tit. II, ch. 21, § 2102(a), 98 Stat. 1837, 2190–91 (emphasis added).

In 1986, however, in a section entitled "Modification of Authorized Access Aspect of Offenses," Congress replaced this language with the phrase "exceeds authorized access," and, in a section entitled "Conforming Amendments to Definitions Provision," added the current definition of that phrase. See Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2(c), (g)(4), 100 Stat. 1213, 1215. It is not clear that Congress intended this language change to be substantive. See S. Rep. No. 99-432, at 9 (1986) ("The Committee intends this change to simplify the language in 18 U.S.C. 1030(a)(1) and (2), and the phrase 'exceeds authorized access' is defined separately in Section (2)(g) of the bill."); 132 Cong. Rec. 28,821 (1986) (statement of Rep. Hughes) (stating, as the chairman of the drafting subcommittee just before final passage, that "the basic thrust of this bill remains its three new offenses with some minor changes in the existing law"). Yet it is notable that Congress did not simply transpose the existing, purpose-oriented language into the definition section—which still would have simplified the language of § 1030(a), as desired—but instead replaced it with new language that focuses on authorization to access particular information. Indeed, if Congress did not think it was making a substantive change, the legislative history suggests that this was because Congress thought the initial language also was limited to access, since "when Congress referenced the user's 'purposes,' it spoke in terms of the particular computer files or data to which the user's access rights extended." Valle, 807 F.3d at 526.

Finally, plaintiffs raise numerous First and Fifth Amendment concerns with the Access Provision that would arise out of reading "exceeds authorized access" to include the purpose or use restrictions that appear in many ToS. When a court is "deciding which of two plausible statutory constructions to adopt," and when "one of them would raise a multitude of constitutional problems, the other should prevail." Clark v. Martinez, 543 U.S. 371, 380–81 (2005). This maxim holds doubly true for criminal statutes. See Marinello, 2018 WL 1402426, at *4 ("[Courts] have

traditionally exercised restraint in assessing the reach of a federal criminal statute, both out of deference to the prerogatives of Congress and out of concern that 'a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed.'" (citation omitted)). While the CFAA's text and legislative history point strongly toward an access-only interpretation of "exceeds authorized access," a broader reading is not entirely implausible; therefore, constitutional avoidance applies. Cf. Jennings v. Rodriguez, 138 S. Ct. 830, 842 (2018). In interpreting the statutory text, the Court need not determine whether plaintiffs' constitutional arguments would actually win the day. Rather, the Court undertakes "a narrow inquiry" into whether one reading "presents a significant risk that [constitutional provisions] will be infringed." NLRB v. Catholic Bishop of Chicago, 440 U.S. 490, 533 (1979).

Here, significant risks abound. By providing for both civil and criminal enforcement of websites' limitless ToS—including enforcement by the same entities that write the ToS—a broader reading of the CFAA "would appear to criminalize a broad range of day-to-day activity" and "subject individuals to the risk of arbitrary or discriminatory prosecution and conviction," raising Fifth Amendment concerns. United States v. Kozminski, 487 U.S. 931, 949 (1988); see Valle, 807 F.3d at 527–28; Nosal, 676 F.3d at 862. By incorporating ToS that purport to prohibit the purposes for which one accesses a website or the uses to which one can put information obtained there, the CFAA threatens to burden a great deal of expressive activity, even on publicly accessible websites—which brings the First Amendment into play. See Packingham, 137 S. Ct. at 1736. If "exceeds authorized access" is read broadly, plaintiffs claim, the Access Provision could even run afoul of the Fifth Amendment by delegating power to private parties to define restrictions "limitless in time and space," which can then operate as petty civil and criminal codes. Pls.' Mem. at 10; see Ass'n of Am. R.Rs. v. U.S. Dep't of Transp. (Ass'n of Am. R.Rs. II), 821 F.3d 19, 31

(D.C. Cir. 2016) ("[T]he Supreme Court has consistently concluded the delegation of coercive power to private parties can raise . . . due process concerns."); Note, The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation, 127 Harv. L. Rev. 751, 768–71 (2013) (arguing that a broadly-read CFAA violates the nondelegation doctrine). One need neither slay nor succumb to this Hydra-headed set of objections to acknowledge it as formidable.

All of these factors, therefore, lead the Court to adopt a narrow reading of the term "exceeds authorized access."[11] Just as an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval," an individual "'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access." WEC Carolina, 687 F.3d at 204.

This interpretation gets us far, but not all the way. At oral argument, both parties agreed that the Access Provision applies only to access restrictions. See Tr. of Mot. Hr'g at 19:17–20:3, 34:10–35:22. But they have very different ideas about what that means. The government treats this difference as a largely temporal one. It argues that "the moment the violation occurs is on access," so that subsequent usage of information lawfully obtained does not constitute a CFAA violation. Id. at 20:12–:18. But the government also claims that "it's appropriate to analyze the issue of whether access is authorized according to a broad context of background facts that could include limitations on the purpose for which information is accessed," such as "access restrictions that are contained in the [ToS] that the website itself has prepared." Id. at 19:21–20:2. Plaintiffs,

[11] A number of other courts have applied the rule of lenity to limit the scope of "exceeds authorized access." See Valle, 807 F.3d at 526; WEC Carolina, 687 F.3d at 204; Nosal, 676 F.3d at 363. The rule of lenity "requires ambiguous criminal laws to be interpreted in favor of the defendants subjected to them." DePierre v. United States, 564 U.S. 70, 88 (2011) (citation omitted). However, lenity is to be used "only 'at the end of the process of construing what Congress has expressed' when the ordinary canons of statutory construction have revealed no satisfactory construction." Lockhart v. United States, 136 S. Ct. 958, 968 (2016) (citation omitted). Text, context, legislative history, congressional intent, and constitutional avoidance all point in one direction here. Because these tools "allow [the Court] to make far more than 'a guess as to what Congress intended,' the rule of lenity does not apply." DePierre, 564 U.S. at 89. If the question were closer, however, lenity would undoubtedly come to plaintiffs' aid.

on the other hand, argue that the distinction between access and use turns on the conduct being prohibited, rather than whether the website attempts to cast the conduct as related to access rather than use. Id. at 61:17–:23. Plaintiffs' reading is the more natural one, and better reflects the constitutional avoidance concerns that support the Court's interpretation of the statute. Therefore, the Court must make an objective inquiry into the conduct alleged to violate websites' ToS. The focus is on what information plaintiffs plan to access, not on why they wish to access it, the manner in which they use their authorization to access it, or what they hope to do with it.

Applying this standard, it becomes clear that most of plaintiffs' proposed activities fall outside the CFAA's reach. Scraping or otherwise recording data from a site that is accessible to the public is merely a particular use of information that plaintiffs are entitled to see. The same goes for speaking about, or publishing documents using, publicly available data on the targeted websites. The use of bots or sock puppets is a more context-specific activity, but it is not covered in this case. Employing a bot to crawl a website or apply for jobs may run afoul of a website's ToS, but it does not constitute an access violation when the human who creates the bot is otherwise allowed to read and interact with that site. See Kerr, Norms of Computer Trespass, supra, at 1170. The website might purport to be limiting the identities of those entitled to enter the site, so that humans but not robots can get in. See Star Wars: Episode IV – A New Hope (Lucasfilm 1977) ("We don't serve their kind here! . . . Your droids. They'll have to wait outside."). But bots are simply technological tools for humans to more efficiently collect and process information that they could otherwise access manually. Cf. Star Wars: Episode II – Attack of the Clones (Lucasfilm 2002) ("[I]f droids could think, there'd be none of us here, would there?").

Out of plaintiffs' proposed activities, then, only Mislove and Wilson's plan to create fictitious user accounts on employment sites would violate the CFAA. Unlike plaintiffs' other

conduct, which occurs on portions of websites that any visitor can view, creating false accounts allows Mislove and Wilson to access information on those sites that is both limited to those who meet the owners' chosen authentication requirements and targeted to the particular preferences of the user.[12] Creating false accounts and obtaining information through those accounts would therefore fall under the Access Provision. With that in mind, the Court must turn to the government's motion to dismiss plaintiffs' constitutional claims.

D. FREEDOM OF SPEECH AND FREEDOM OF THE PRESS

Plaintiffs first claim that the Access Provision violates the First Amendment's guarantees of freedom of speech and of the press.[13] They assert that the provision is both facially overbroad and unconstitutional as applied to their own conduct. The Court will analyze these claims in turn.

1. Facial Overbreadth

Plaintiffs allege that the Access Provision "creates virtually limitless restrictions on speech and expressive activity," such that the statute "is unconstitutionally overbroad on its face." Compl. ¶ 183. In a typical facial challenge, plaintiffs must show "'that no set of circumstances exists under which [the Access Provision] would be valid,' . . . or that the statute lacks any 'plainly legitimate sweep.'" Stevens, 559 U.S. at 472 (citations omitted). However, First Amendment cases allow for "'a second type of facial challenge,' whereby a law may be invalidated as overbroad if 'a substantial number of its applications are unconstitutional, judged in relation to the statute's plainly

[12] Professor Kerr argues that "a website that appears to require a username and password to access the contents of the site, but that actually grants access for any username and password combination," should not be seen as creating an access restriction, because it "would appear to a user to regulate by code, but would actually work more like a system of regulation by contract." Kerr, Cybercrime's Scope, supra, at 1646. The distinction between code-based and contract-based barriers matters for First Amendment analysis, see supra Part II.A, but it does not quite line up with the Court's reading of the CFAA. Social media sites like Facebook, for instance, grant access for any username and password combination, but they still allow those with accounts to access data that those who merely visit the site without signing up cannot. Hence, conditions placed on account creation can still be access restrictions.

[13] Courts normally subject free speech and free press claims to the same level of scrutiny. See, e.g., Citizens United, 558 U.S. at 352; McConnell v. FEC, 251 F. Supp. 2d 176, 234–35 (D.D.C.) (three-judge court) (per curiam), aff'd in part, rev'd in part, 540 U.S. 93 (2003). The Court will thus treat the speech claim as a proxy for both.

legitimate sweep.'" Id. at 473 (citation omitted). This second, lower bar is the one against which plaintiffs—and the Court—measure their challenge.

The government argues that plaintiffs have failed to state a plausible overbreadth claim. See Def.'s Reply at 18–19. The Court agrees. "The first step in overbreadth analysis is to construe the challenged statute; it is impossible to determine whether a statute reaches too far without first knowing what the statute covers." United States v. Williams, 553 U.S. 285, 293 (2008). The Court has now done so. Plaintiffs have operated under the assumption that the Access Provision covers all ToS violations; but, properly read, the Access Provision incorporates only those ToS that limit access to particular information. This fact alone is enough to dispose of plaintiffs' overbreadth claim. "Invalidation for overbreadth is strong medicine," id. (citation omitted), to be "employed . . . sparingly and only as a last resort," Broadrick v. Oklahoma, 413 U.S. 601, 613 (1973). A court should not invalidate a provision for overbreadth "when a limiting construction has been or could be placed on the challenged statute." Id.

Plaintiffs concede that a limiting construction would address their overbreadth concerns—though they contend that the Access Provision would need to be "construed not to reach [ToS] violations alone." Pls.' Mem. at 35. While the Court's reading of "exceeds authorized access" is not as narrow as the reading plaintiffs might prefer, it does eliminate many of the potentially unconstitutional applications of the Access Provisions. To be overbroad, a statute's unconstitutional scope must be "substantial, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep." Williams, 553 U.S. at 292. As purpose, use, or manner restrictions fall outside the Access Provision's reach, plaintiffs have not plausibly alleged that the provision's potentially unconstitutional applications are substantial relative to its legitimate ones. Moreover, plaintiffs also bring an as-applied claim, and facial challenges are disfavored when a

case "may be disposed of on narrower grounds." Texas v. Johnson, 491 U.S. 397, 403 n.3 (1989). Hence, Plaintiffs' overbreadth claim will be dismissed.

2. As-Applied Challenge

Plaintiffs allege that, "[a]s applied to the[m]," the Access Provision "unconstitutionally restricts their protected speech." Compl. ¶ 184. "[T]o prevail on an as-applied First Amendment challenge," plaintiffs "must show that the [Access Provision is] unconstitutional as applied to their particular speech activity." Edwards v. District of Columbia, 755 F.3d 996, 1001 (D.C. Cir. 2014). "'[T]he distinction between facial and as-applied challenges . . . goes to the breadth of the remedy employed by the Court, not what must be pleaded in a complaint.' . . . The substantive rule of law is the same for both challenges." Id. (citations omitted).

Aside from the overarching objections that the Court has already rejected, the government's primary response to plaintiffs' as-applied claim is that the Access Provision regulates conduct, rather than speech, and is therefore subject to limited scrutiny. See Def.'s Mem. at 21, 27. But even if a law "says nothing about speech on its face," it is "subject to First Amendment scrutiny" if "it restricts access to traditional public fora." McCullen v. Coakley, 134 S. Ct. 2518, 2529 (2014). As the Access Provision both limits access to and burdens speech in the public forum that is the public Internet, see supra Part II.A, heightened First Amendment scrutiny is appropriate. "In particular, the guiding First Amendment principle that the 'government has no power to restrict expression because of its message, its ideas, its subject matter, or its content' applies with full force in a traditional public forum." Id. (citation omitted). Content- or viewpoint-based restrictions receive strict scrutiny. See Reed v. Town of Gilbert, 135 S. Ct. 2218, 2226 (2015); Rosenberger, 515 U.S. at 829. On the other hand, if a statute is content-neutral and only "impose[s] reasonable restrictions on the time, place, or manner of protected speech," McCullen,

134 S. Ct. at 2529, it is subjected to intermediate scrutiny. "In order to survive intermediate scrutiny, a law must be 'narrowly tailored to serve a significant governmental interest,'" Packingham, 137 S. Ct. at 1736 (citation omitted), and must "leave open ample alternative channels for communication of the information," McCullen, 134 S. Ct. at 2529.[14]

Plaintiffs claim that the Access Provision allows websites to impose direct speech restrictions, including content-based restrictions, and that it is therefore subject to strict scrutiny. Pls.' Mem. at 34–35. However, the statute itself does not target speech, or impose content-based regulations, on its face. Nor have plaintiffs plausibly alleged that the government's purpose is to restrict speech based on its content or viewpoint. Indeed, while the government has not yet been able to proffer much evidence of the purposes behind the provision, the legislative history indicates that Congress was interested in passing the Access Provision to prevent the digital equivalent of theft. See S. Rep. 104–357, at 7 ("The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer. . . . This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected [sic]."). Therefore, strict scrutiny does not apply. See Pursuing America's Greatness v. FEC, 831 F.3d 500, 509 (D.C. Cir. 2016) (stating that courts must determine content neutrality based on text, and then purpose).

[14] The standard that governs expressive conduct prohibitions with "incidental limitations on First Amendment freedoms," see United States v. O'Brien, 391 U.S. 367, 376 (1968), is inapposite to this as-applied claim. "The law here may be described as directed at conduct, . . . but as applied to plaintiffs the conduct triggering coverage under the statute consists of communicating a message." Humanitarian Law Project, 561 U.S. at 28. Plaintiffs are informing the websites of who they are, and claiming to be employers, much in the same way that the defendant in Alvarez had claimed to be a decorated war veteran, or the plaintiffs in Humanitarian Law Project had sought to train terrorists to engage in peaceful activity. All of these forms of conduct communicate messages to the recipients. Moreover, it is the content of plaintiffs' speech to the targeted websites—that they represent their identities falsely or misleadingly instead of truthfully—that triggers the sites' ToS and, thereby, the criminal penalties of the CFAA. In other words, Mislove and Wilson would violate the Access Provision "because of the [false] content of [their] particular message." Id. In these circumstances, the government must meet a "more demanding standard" than the O'Brien test. Id. (quoting Johnson, 491 U.S. at 403). Even if that test were applicable, however, "in the last analysis [it] is little, if any, different from the standard applied to time, place, or manner restrictions," Johnson, 491 U.S. at 407, and incorporates narrow tailoring requirements, see Edwards, 755 F.3d at 1002–03, so the analysis would not meaningfully change.

From the information available so far, significant interests appear to underlie the Access Provision. In addition to the legislative history regarding theft prevention, the government suggests that the Court analogize the CFAA to trespass law, arguing that Congress was also trying to prohibit the digital equivalent of trespassing. Def.'s Reply at 3–5. While plaintiffs dispute the trespass analogy, they recognize that the CFAA was passed to prevent computer theft and other cybercrime, and have not disputed that this is a significant interest. Pls.' Mem. at 31. The question is thus whether the statute fails narrow tailoring as applied to Mislove and Wilson's plan to "creat[e] profiles containing false information," Compl. ¶ 124, and "access[] websites using artificial tester profiles, in violation of [ToS] that prohibit providing false information," id. ¶ 154.

"To satisfy narrow tailoring, the [government] must prove the challenged regulations directly advance its asserted interests." Edwards, 755 F.3d at 1003. This means "the government must show '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. Coalition v. Basham, 845 F.3d 1199, 1213–14 (D.C. Cir. 2017) (citations omitted). At this early stage, the government has not put forward any evidence to show that prosecuting those who provide false information when creating accounts, without more, would advance its interest in preventing digital theft or trespass.

Indeed, presuming the allegations in the complaint to be true, it appears that the government's interest "is not implicated on these facts" at all. Johnson, 491 U.S. at 410. Plaintiffs allege that their conduct "will not cause material harm to the target websites' operations," and that "they have no intent to commit fraud or to access any data or information that is not made available to the public." Compl. ¶ 4. It is difficult to argue that trespass or theft concerns can justify

restricting—or even apply to—viewing information that a website makes available to anyone who chooses to create a username and password. Cf. Kerr, Cybercrime's Scope, supra, at 1646. And any inadvertent "fraud" plaintiffs may perpetrate against the target websites by creating fictitious accounts will be, plaintiffs allege, harmless. The CFAA already punishes harmful, intentional fraud in a separate section, see 18 U.S.C. § 1030(a)(4), providing additional evidence that the government can further its legitimate interests just as well without applying the Access Provision to plaintiffs' bare false statements. At this stage, "absent any evidence that the speech [would be] used to gain a material advantage," Alvarez, 567 U.S. at 723, plaintiffs' false speech on public websites retains First Amendment protection, see id. at 722, and rendering it criminal does not appear to advance the government's proffered interests. Hence, plaintiffs have plausibly alleged an as-applied First Amendment claim, and the motion to dismiss that claim will be denied.

E. RIGHT TO PETITION

In addition to their free speech and press claims, plaintiffs allege that the Access Provision violates their rights under the Petition Clause of the First Amendment. Compl. ¶ 193. That clause states: "Congress shall make no law . . . abridging . . . the right of the People . . . to petition the Government for a redress of grievances." U.S. Const. amend. I. Plaintiffs assert that the Access Provision, by criminalizing websites' prohibitions on critical speech or publishing, prevents people from using any information they might gain from plaintiffs' planned research to inform Congress or agencies about potential discrimination by those websites. Id. ¶¶ 162–67, 189. They also assert that, for the same reasons, the Access Provision prevents people from accessing the courts to enforce Title VII or the Fair Housing Act: nobody who had visited a website with a non-disparagement clause in its ToS could bring discrimination claims against that site in court without opening him- or herself up to a potential CFAA prosecution. Id. ¶¶ 168–69, 190.

These allegations are focused on ToS that restrict subsequent speech: disparagement, for instance, or use of the sites' information in court. However, such ToS constitute restrictions on the use of information, not on access to it. They therefore do not fall within the Access Provision's ambit, as properly interpreted. But even if one assumes that plaintiffs allege that access restrictions criminalized by the Access Provision violate the Petition Clause, see Compl. ¶ 162, plaintiffs' petition challenge is, at best, no stronger than their free speech challenge. Speech and petition rights are "generally subject to the same constitutional analysis," Wayte v. United States, 470 U.S. 598, 610 n.11 (1985), unless "the special concerns of the Petition Clause would provide a sound basis for a distinct analysis," Borough of Duryea v. Guarnieri, 564 U.S. 379, 389 (2011). Here, the rights appear to overlap: plaintiffs' Petition Clause claim focuses on speech restrictions that could then affect the petitioning process. Thus, plaintiffs "just as easily could have alleged"—and do, in fact, allege—a Speech Clause violation on the same set of facts. Id. at 387.

And it is on that free speech claim that plaintiffs' First Amendment case must rise or fall. The Speech and Press Clauses, rather than the Petition Clause, provide the more natural home for plaintiffs' concerns about the Access Provision. Plaintiffs assert that the CFAA "prevents them from engaging in" petitioning because some websites' ToS (and thus the Access Provision) "prohibit the speech necessary to engage in . . . petitioning." Pls.' Mem. at 43. The real concern, then, is the Access Provision's alleged restrictions on speech, which have ripple effects in a variety of contexts. The application of the Access Provision to the petitioning process constitutes one small subset of the speech and conduct the provision allegedly prohibits. Any effect the statute might have on plaintiffs' petition rights, then, is an extra step removed from the central speech harm, and is thus too attenuated to state a plausible claim for relief.

Ultimately, "the Petition Clause protects the right of individuals to appeal to courts and other forums established by the government for resolution of legal disputes," and "[i]nterpretation of the Petition Clause must be guided by the objectives and aspirations that underlie the right." Borough of Duryea, 564 U.S. at 387–88. As the government notes, the clause is not aimed at the right to gather facts, or to speak while doing so, as a preliminary step to help prepare that petition in a preferred way. See Def.'s Mem. at 28. That right is more naturally the province of the Speech and Press Clauses than of the Petition Clause. See Burt Neuborne, Madison's Music: On Reading the First Amendment 11–12, 89 (2015) (arguing that the First Amendment's protected rights form "a rigorous chronological narrative of free citizens governing themselves in an ideal democracy," and that the Petition Clause "concludes Madison's narrative, protecting [an] idea's introduction into the formal democratic process, forcing the legislature to place the issue on its agenda"). Hence, plaintiffs' Petition Clause claim will be dismissed.

F. VAGUENESS

Plaintiffs next allege that the Access Provision violates the Due Process Clause because it is unconstitutionally vague. A statute is void if it is "[1] so vague that it fails to give ordinary people fair notice of the conduct it punishes, or [2] so standardless that it invites arbitrary enforcement." Johnson v. United States, 135 S. Ct. 2551, 2556 (2015). Plaintiffs allege that the Access Provision meets both prongs of this test. Compl. ¶¶ 171–72. Because of potential chilling effects, "a more stringent vagueness test" applies when a law "interferes with the right of free speech." Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc., 455 U.S. 489, 499 (1982).

Properly interpreted, however, the Access Provision is not unconstitutionally vague. "A plaintiff whose speech is clearly proscribed cannot raise a successful vagueness claim" based on a lack of fair notice. Expressions Hair Design v. Schneiderman, 137 S. Ct. 1144, 1151–52 (2017)

(quoting Humanitarian Law Project, 561 U.S. at 20). Nor can that plaintiff bring a facial vagueness challenge "based on the speech of others." Humanitarian Law Project, 561 U.S. at 20. As we have already seen, the Access Provision plainly proscribes the creation of false accounts, but does not prohibit plaintiffs' other activities. Indeed, plaintiffs allege that they are aware that their proposed conduct would violate their target websites' ToS restrictions on creating false accounts. Compl. ¶ 124. As the Court has determined that the Access Provision applies to one of their activities but not to the others, and as plaintiffs admit that they have the requisite mens rea to commit the crime, no facial claim or as-applied notice claim can go forward.

Nor can plaintiffs plausibly allege that the Access Provision invites arbitrary enforcement. "[A] statute's vagueness is either susceptible to judicial construction or is void for vagueness based on the application of traditional rules for statutory interpretation." United States v. Bronstein, 849 F.3d 1101, 1106 (D.C. Cir. 2017). Thus, "before striking a federal statute as impermissibly vague," courts must "consider whether the prescription is amenable to a limiting construction." Welch v. United States, 136 S. Ct. 1257, 1268 (2016) (citation omitted). The Court has already determined that a more limited construction is not only possible, but is in fact more natural than the broad reading that raises vagueness concerns. Read to apply only to access, and not to use, restrictions, the Access Provision severely curtails both websites' ability to define the law and prosecutors' freedom arbitrarily to enforce it. Plaintiffs' Fifth Amendment vagueness claim will be dismissed.

G. NONDELEGATION DOCTRINE

Finally, plaintiffs allege that the Access Provision violates the Fifth Amendment because it delegates the content of criminal law to private parties. Compl. ¶¶ 173–77, 201. The primary case laying out the private nondelegation doctrine is Carter v. Carter Coal Co., 298 U.S. 238 (1936). The statute at issue in that case delegated to coal industry groups the power to create

binding codes for the regulation of coal miners' wages and hours. Id. at 310–11. The Court stated that this power "is legislative delegation in its most obnoxious form; for it is not even delegation to an official or an official body, presumptively disinterested, but to private persons whose interests may be and often are adverse to the interests of others in the same business." Id. at 311. Prior to Carter Coal, the Supreme Court also twice struck down ordinances that sanctioned a "standardless delegation of power to a limited group of property owners." City of Eastlake v. Forest City Enterprises, Inc., 426 U.S. 668, 678 (1976) (discussing Eubank v. Richmond, 226 U.S. 137 (1912), and Washington ex rel. Seattle Title Trust Co. v. Roberge, 278 U.S. 116 (1928)).

The D.C. Circuit has gleaned two rules from these cases. First, "[f]ederal lawmakers cannot delegate regulatory authority to a private entity." Ass'n of Am. R.Rs. v. U.S. Dep't of Transp. (Ass'n of Am. R.Rs. I), 721 F.3d 666, 670 (D.C. Cir. 2013), vacated and remanded on other grounds, 135 S. Ct. 1225 (2015). Unlike with delegations to agencies, "[e]ven an intelligible principle cannot rescue a statute empowering private parties to wield regulatory authority." Id. at 671. And second, "the due process of law is violated when a self-interested entity is 'intrusted with the power to regulate the business . . . of a competitor.'" Ass'n of Am. R.Rs. II, 821 F.3d at 31 (quoting Carter Coal, 298 U.S. at 311). Plaintiffs claim that the Access Provision violates the first of these principles. They allege that the law allows website owners to define the content of a crime—thus sweeping beyond other statutes that merely enforce private contractual agreements—and that the statute relinquishes any government control over the lawmaking process. Compl. ¶¶ 174–76. They also assert that the Access Provision provides no standards to guide what website owners may effectively criminalize. See Pls.' Mem. at 40.

Plaintiffs raise an intriguing argument, but it is ultimately an unsuccessful one. As with First Amendment overbreadth and vagueness, the courts can avoid nondelegation concerns by

"giving narrow constructions to statutory delegations that might otherwise be thought to be unconstitutional." Mistretta v. United States, 488 U.S. 361, 373 n.7 (1989). Plaintiffs assert that the Access Provision provides a limitless, standardless delegation of power to individual websites to define crimes. But that assertion is based on a reading of the provision that sweeps in use, purpose, or manner restrictions on obtaining or altering information. Properly read as applying only to access restrictions, websites can write whatever ToS they please, but a congressionally-imposed standard limits which ToS can lead to liability or prosecution. Nor do websites have the power to impose formal rules on an industry or otherwise exercise regulatory authority in the manner that courts have found constitutionally impermissible. See, e.g., Yakus v. United States, 321 U.S. 414, 424 (1944); Carter Coal, 298 U.S. at 310–11; Ass'n of Am. R.Rs. I, 721 F.3d at 670–72. Plaintiffs have cited no case—nor has the Court found one—in which a court struck down on private nondelegation grounds a statute that incorporated private parties' chosen restrictions, which are only binding on those who interact with those parties' individual businesses. It is thus difficult to argue that the Access Provision improperly delegates legislative or regulatory authority.

Indeed, when read narrowly, the Access Provision looks similar to many criminal laws that are rendered operative by a private party's decision whether to authorize certain conduct. Examples cited in the government's brief, see Def.'s Mem. at 32–33, include criminal trespass laws, see D.C. Code § 22–3302; 25 C.F.R. § 11.411, and laws against misappropriation of trade secrets, see 18 U.S.C. § 1831, copyrights, see 17 U.S.C. §§ 106, 506, individuals' identities, see 18 U.S.C. § 1029, and money (e.g., embezzlement). In none of these instances does a private party's control over the law's operation render it a nondelegation problem. Rather, "a legislative delegation to private citizens" is constitutional so long as "[1] the underlying exercise of authority [is] a reasonable regulation within the power of the government . . . . and [2] the legislature's

restriction [is] in the form of a general prohibition, and the delegation [is] in the form of permitting private citizens to waive the protection of that prohibition." Silverman v. Barry, 845 F.2d 1072, 1086 (D.C. Cir. 1988). A different rule would make it so that "[a]lmost any system of private or quasi-private law could be subject to the" nondelegation doctrine. New Motor Vehicle Bd. of Cal. v. Orrin W. Fox Co., 439 U.S. 96, 109 (1978). Since the Access Provision creates a blanket prohibition on accessing information in protected computers, which owners of those computers can waive through permission, plaintiffs do not plausibly allege that the provision unconstitutionally delegates legislative power. Hence, the nondelegation claim will be dismissed.

CONCLUSION

This case raises important questions about the government's ability to criminalize vast swaths of everyday activity on the Internet. However, the Court need not answer all of them today, because it concludes that the CFAA prohibits far less than the parties claim (or fear) it does. For the reasons explained above, plaintiffs have plausibly alleged that they have standing to sue, and that the Access Provision violates the Free Speech and Free Press Clauses of the First Amendment as applied to them. The government's motion to dismiss for lack of standing and on this single as-applied claim will therefore be denied. But the Access Provision, as the Court reads it, does not sweep widely enough to render plausible plaintiffs' First Amendment overbreadth and petition claims, or their Fifth Amendment vagueness and nondelegation claims. The government's motion to dismiss those claims, therefore, will be granted. A separate order will issue on this date.

/s/
JOHN D. BATES
United States District Judge

Dated: March 30, 2018