

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

CHRISTIAN SANDVIG,
et al.,

Plaintiffs,

v.

WILLIAM P. BARR, in his official capacity
as Attorney General of the United States,

Defendant.

Case No. 1:16-cv-1368 (JDB)

**DEFENDANT'S MEMORANDUM IN SUPPORT OF CROSS-MOTION FOR
SUMMARY JUDGMENT, AND IN OPPOSITION TO PLAINTIFFS'
MOTION FOR SUMMARY JUDGMENT**

TABLE OF CONTENTS

INTRODUCTION1

BACKGROUND4

I. Legal Framework4

II. Factual and Procedural History.....6

STANDARD OF REVIEW8

ARGUMENT9

I. At Summary Judgment, Plaintiffs Have Not Carried Their Heightened Burden of Establishing Standing.....9

 A. Plaintiffs Lack Any Concrete Plans for Pursuing Their Research10

 B. Plaintiffs Cannot Demonstrate a Credible Threat of Prosecution.....12

 1. Plaintiffs Themselves Do Not Fear Prosecution Under the CFAA.....12

 2. The Government’s Past CFAA Prosecutions Do Not Create a Credible Threat as to Plaintiffs14

 3. The Government’s Charging Policies and Public Statements Further Confirm that Any Risk of Prosecution is Speculative16

 C. Plaintiffs’ Claims Are Not Sufficiently Ripe for Adjudication18

II. The First Amendment Does Not Extend to Enforcement of Private Parties’ Choices About Whom to Exclude20

 A. The Factual Record Here Confirms that, Under the Court’s Prior Framework, the Relevant Websites Are Not Public Forums.....21

 B. Private Websites Are Not “Public Forums” as a Matter of Law22

 1. The Supreme Court Has Held that Private Choices About Whom to Exclude are Not Subject to the First Amendment.....23

 2. The “Public Forum” Doctrine Is Limited to Government-Owned or Government-Controlled Property24

 3. The Supreme Court’s *Packingham* Decision Does Not Change the First Amendment Status of Private Websites27

 C. Plaintiffs’ Alternative Theory Focusing on State Action Likewise Does Not Allow First Amendment Scrutiny of Private Choices.....30

D. Applying the First Amendment to the Modern Internet Would Have Negative Consequences.....	34
III. At Most, the CFAA Would Be Subject to Intermediate Scrutiny	35
A. The Access Provision is Not a Content-Based Restriction	35
B. Plaintiffs’ Sole Remaining Claim Does Not Implicate Any Expressive Activity	37
C. At Most, Intermediate Scrutiny Would Apply	39
IV. The Access Provision Amply Satisfies Intermediate Scrutiny.....	40
A. Important Government Interests Are Furthered By the Access Provision.....	40
B. The Access Provision Directly Advances Important Government Interests, Including As Applied to Plaintiffs’ Conduct.....	42
1. Plaintiffs Misconceive the Appropriate Inquiry by Focusing Solely on Their Conduct.....	42
2. Applying the Access Provision to Plaintiffs’ Conduct Would, In Fact, Further Important Government Interests	45
3. Plaintiffs’ Conduct Goes Beyond <i>De Minimis</i> Harm.....	51
C. The Access Provision Leaves Open Ample Alternatives for Plaintiffs’ Conduct	53
CONCLUSION.....	55

TABLE OF AUTHORITES

Cases

281 Care Comm. v. Arneson,
766 F.3d 774 (8th Cir. 2014)..... 37

Am. Library Ass’n v. Barr,
956 F.2d 1178 (D.C. Cir. 1992)..... 19

Am. Library Ass’n v. Reno,
33 F.3d 78 (D.C. Cir. 1994) 40

Anderson v. Liberty Lobby, Inc.,
477 U.S. 242 (1986)..... 8

Animal Legal Def. Fund v. Wasden,
878 F.3d 1184 (9th Cir. 2018)..... 31

ANSWER Coal. v. Basham,
845 F.3d 1199 (D.C. Cir. 2017)..... 36, 40

ANSWER Coal v. Dist. of Colum.,
846 F.3d 391 (D.C. Cir. 2017) 46, 48, 54

Arcara v. Cloud Books, Inc.,
478 U.S. 697 (1986)..... 37, 38, 39

Arkansas Educ. Television Comm’n v. Forbes,
523 U.S. 666 (1998)..... 26

Ashcroft v. Free Speech Coalition,
535 U.S. 234 (2002)..... 35

Babbitt v. United Farm Workers Nat. Union,
442 U.S. 289 (1979)..... 17, 18, 19

Blumenthal v. Drudge,
992 F. Supp. 44 (D.D.C. 1998) 35

Brandenburg v. Ohio,
395 U.S. 444 (1969)..... 35

Cape Cod Nursing Home Council v. Rambling Rose Rest Home,
667 F.2d 238 (1st Cir. 1981) 33

Celotex Corp. v. Catrett,
477 U.S. 317 (1986)..... 21

Cent. Hardware Co. v. NLRB,
407 U.S. 539 (1972)..... 23

Christian Legal Soc’y v. Martinez,
561 U.S. 661 (2010)..... 25

City of Erie v. Pap’s A.M.,
529 U.S. 277 (2000)..... 35

City of Ladue v. Gilleo,
512 U.S. 43 (1994)..... 28

Clapper v. Amnesty Int’l USA,
568 U.S. 398 (2013)..... 18

Clark v. Cmty. For Creative Non-Violence,
468 U.S. 288 (1984)..... 43, 53

Clarke v. United States,
915 F.2d 699 (D.C. Cir. 1990) 17

Cohen v. Cowles Media Co.,
501 U.S. 663 (1991)..... 38, 53

Cornelius v. NAACP Legal Def. & Educ. Fund,
473 U.S. 788 (1985)..... 24

Cowan v. Prudential Ins. Co. of Am.,
141 F.3d 751 (7th Cir. 1998)..... 12

DaimlerChrysler Corp. v. Cuno,
547 U.S. 332 (2006)..... 14

Dep’t of Commerce v. U.S. House of Reps.,
525 U.S. 316 (1999)..... 10

Edwards v. Dist. of Colum.,
755 F.3d 996 (D.C. Cir. 2014) 41, 43

Freedom Watch, Inc. v. Google, Inc.,
--- F. Supp. 3d ---, 2019 WL 1201549, at (D.D.C. Mar. 14, 2019)..... 29

Galvin v. Eli Lilly & Co.,
488 F.3d 1026 (D.C. Cir. 2007) 12

Glass v. Lahood,
786 F. Supp. 2d 189 (D.D.C. 2011),
aff'd, No. 11-5144, 2011 WL 6759550 (D.C. Cir. Dec. 8, 2011) 12

Heffron v. Int'l Soc. for Krishna Consciousness, Inc.,
452 U.S. 640 (1981)..... 43, 44

Hudgens v. NLRB,
424 U.S. 507 (1976)..... 23, 30, 52

In re Navy Chaplaincy,
323 F. Supp. 3d 25 (D.D.C. 2018) 9

Int'l Soc'y for Krishna Consciousness, Inc. v. Lee,
505 U.S. 672 (1992)..... 25

Johnson v. Cache Cty. Sch. Dist.,
323 F. Supp. 3d 1301 (D. Utah 2018) 29

Kaiser Aetna v. United States,
444 U.S. 164 (1979)..... 41

Kalfus v. New York & Presbyterian Hosp.,
476 F. App'x 877 (2d Cir. 2012)..... 33

LaRouche v. Fowler,
152 F.3d 974 (D.C. Cir. 1998) 30

Lion Mfg. Corp. v. Kennedy,
330 F.2d 833 (D.C. Cir. 1964) 19

Lloyd Corp. v. Tanner,
407 U.S. 551 (1972)..... passim

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992)..... 1, 9, 10, 11

Mahoney v. Dist. of Colum.,
662 F. Supp. 2d 74 (D.D.C. 2009),
aff'd sub nom. Mahoney v. Doe, 642 F.3d 1112 (D.C. Cir. 2011) 43

Matal v. Tam,
137 S. Ct. 1744 (2017)..... 35

Matsushita Elec. Indus. Co. v. Zenith Radio Corp.,
475 U.S. 574 (1986)..... 8

McCullen v. Coakley,
573 U.S. 464 (2014)..... 37

McCutcheon v. FEC,
572 U.S. 185 (2014)..... 37

McNamara v. Miller,
269 F.2d 511 (D.C. Cir. 1959)..... 22

Members of City Council of City of Los Angeles v. Taxpayers for Vincent,
466 U.S. 789 (1984)..... 43, 44, 46, 49

Moore v. Carson,
322 F. Supp. 3d 163 (D.D.C. 2018) 8

Nat’l Org. for Women v. Operation Rescue,
37 F.3d 646 (D.C. Cir. 1994) 33, 41

Navegar, Inc. v. United States,
103 F.3d 994 (D.C. Cir. 1997) 12

New York Times Co. v. Sullivan,
376 U.S. 254 (1964)..... 31

Nyabwa v. FaceBook,
2018 WL 585467, at (S.D. Tex. Jan. 26, 2018)..... 29

O’Brien v. Brown,
409 U.S. 1 (1972)..... 30

Packingham v. North Carolina,
137 S. Ct. 1730 (2017)..... passim

Perry Educ. Ass’n v. Perry Local Educators’ Ass’n,
460 U.S. 37 (1983)..... 24, 25

Prager Univ. v. Google LLC,
2018 WL 1471939 (N.D. Cal. Mar. 26, 2018) 29

PruneYard Shopping Ctr. v. Robins,
447 U.S. 74 (1980)..... 30

Reed v. Town of Gilbert,
135 S. Ct. 2218 (2015)..... 36, 43

Reno v. ACLU,
521 U.S. 844 (1997)..... 34

Rosenberger v. Rector & Visitors of Univ. of Va.,
515 U.S. 819 (1995)..... 25

San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm.,
(USOC), 483 U.S. 522 (1987)..... 41, 48

Snyder v. Phelps,
562 U.S. 443 (2011)..... 35

Steffel v. Thompson,
415 U.S. 452 (1974)..... 13

Summers v. Earth Island Inst.,
555 U.S. 488 (2009)..... 10

Susan B. Anthony List v. Driehaus,
573 U.S. 149 (2014)..... 13, 14

Sw. Cmty. Res., Inc. v. Simon Prop. Grp., LP,
108 F. Supp. 2d 1239 (D.N.M. 2000) 33

Tele-Commc’ns of Key W., Inc. v. United States,
757 F.2d 1330 (D.C. Cir. 1985) 25

U.S. Telecom Ass’n v. FCC,
825 F.3d 674 (D.C. Cir. 2016) 39

United States v. Albertini,
472 U.S. 675 (1985)..... 43

United States v. Alvarez,
567 U.S. 709 (2012)..... 31, 41

United States v. Am. Library Ass’n, Inc.,
539 U.S. 194 (2003)..... 25

United States v. O’Brien,
391 U.S. 367 (1968)..... 39

<i>United States v. Stevens</i> , 559 U.S. 460 (2010).....	32, 34, 37, 43
<i>Utah Gospel Mission v. Salt Lake City Corp.</i> , 316 F. Supp. 2d 1201 (D. Utah 2004), <i>aff'd</i> , 425 F.3d 1249 (10th Cir. 2005)	33
<i>Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.</i> , 425 U.S. 748 (1976).....	34, 41
<i>Virginia v. Hicks</i> , 539 U.S. 113 (2003).....	38
<i>Walker v. Texas Div., Sons of Confederate Veterans, Inc.</i> , 135 S. Ct. 2239 (2015).....	25
<i>Ward v. Rock Against Racism</i> , 491 U.S. 781 (1989).....	40, 46
<i>Western Watersheds Project v. Michael</i> , 353 F. Supp. 3d 1176 (D. Wyo. 2018).....	33
<i>Williams v. Dodaro</i> , 576 F. Supp. 2d 72 (D.D.C. 2008)	52
<i>Worth v. Jackson</i> , 451 F.3d 854 (D.C. Cir. 2006)	11
<i>Younger v. Harris</i> , 401 U.S. 37 (1971).....	14
Statutes	
18 U.S.C. § 1030(a)(2)(C)	<i>passim</i>
18 U.S.C. § 1030(c)(2).....	5
18 U.S.C. § 1030(e)(2)(B)	5
18 U.S.C. § 1030(g).....	31
47 U.S.C. § 230(c)(2)(A)	35
Pub. L. No. 98-473, 98 Stat. 1837 (1984).....	4
Pub. L. No. 104-294, tit. II, § 201 (1996).....	5

Federal Rules

Fed. R. Civ. P. 36(b)..... 22

Fed. R. Civ. P. 54(b)..... 23

Fed. R. Civ. P. 56(a) 8

Fed. R. Civ. P. 56(c)(1) 8

Fed. R. Civ. P. 56(e) 52

Fed. R. Civ. P. 65(d)(1)(B)..... 19

Other Authorities

H.R. Rep. No. 98-894 (1984)..... 4

S. Rep. No. 104-357 (1996)..... 4

INTRODUCTION

Plaintiffs here are two academics challenging the constitutionality of a provision of the Computer Fraud and Abuse Act (CFAA)—specifically, the provision that makes it a crime for a person to “intentionally access[] a computer without authorization or exceed[] authorized access” and thereby obtain information from the computer. 18 U.S.C. § 1030(a)(2)(C) [hereafter the “Access Provision”]. Plaintiffs claim that the Access Provision unlawfully criminalizes their research efforts, which involve creating fictitious accounts and/or providing misleading information to online hiring websites, in violation of those websites’ Terms of Service (ToS). This Court previously dismissed all of Plaintiffs’ claims except an as-applied First Amendment claim. *See* Mot. to Dismiss Op. (ECF No. 24) at 33-44 [hereafter “MTD Op.”]. In that opinion, the Court also concluded that Plaintiffs had “plausibly pled standing at the motion to dismiss stage[.]” *Id.* at 24.

Following the Court’s motion-to-dismiss ruling, the parties engaged in discovery. As the factual record compiled during discovery now makes clear, Defendant is entitled to summary judgment on Plaintiffs’ sole remaining claim. That is so for three main reasons.

First, Plaintiffs have failed to carry their heightened burden at summary judgment to establish their standing. Although they allege a general intent to undertake research covered by their First Amendment claim—*i.e.*, involving fake and/or misleading accounts in violation of websites’ ToS—Plaintiffs admitted during their depositions that they have no concrete plans to undertake such research. This lack of concrete plans is fatal at the summary-judgment stage. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 564 (1992) (holding that “some day intentions . . . without any description of concrete plans” are inadequate to establish imminent injury-in-fact).

Moreover, Plaintiffs have not established a credible threat of prosecution for any such future research. Again, Plaintiffs admitted during their depositions that they do not actually fear

prosecution under the CFAA, and for good reason—Plaintiffs have never been threatened with any potential enforcement of the CFAA. Nor does the Government’s record of past enforcement of the CFAA create a credible threat, given that Plaintiffs, despite having the full tools of discovery available to them, have not identified a single past prosecution under the Access Provision involving conduct similar to theirs. Additionally, the Government’s public statements and actions regarding CFAA prosecutions make clear that any prosecution of Plaintiffs is wholly speculative.

Finally, even if Plaintiffs otherwise had standing for their claim, it is still too abstract to be capable of judicial resolution at this stage. Because Plaintiffs have not yet identified their target websites or their exact research methods, it is impossible for this Court to evaluate (or provide relief on) such abstract claims. Indeed, based on the limited record Plaintiffs have put forward, it is not even clear that injunctive relief is required for them to perform their research. Thus, even if Plaintiffs had standing, their claims are not yet ripe.

Second, even if Plaintiffs’ claims were justiciable, the claims still fail because the First Amendment does not extend to the Government’s enforcement of private parties’ decisions about whom to exclude from their private property. To be sure, the Court rejected this argument at the motion-to-dismiss stage, holding that private websites are “public forums” subject to First Amendment scrutiny, unless those websites “have taken real steps to limit who can access” them. MTD Op. at 9, 11. Even under this framework, however, the factual record now confirms that the relevant websites here *have* taken meaningful steps to limit access, particularly with respect to the creation of false or misleading accounts. Indeed, Plaintiffs admitted during discovery that none of the relevant websites here are “public forums,” which should itself be conclusive.

If the Court were to disagree with the above factual argument, then Defendant respectfully requests that the Court revisit its prior legal analysis regarding private websites being “public

forums.” The “public forum” doctrine is limited to government-owned or government-controlled property, and the Supreme Court’s decision in *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), does not change the analysis for websites. Plaintiffs do not contend otherwise, and instead offer an alternative argument for how their claims may proceed—one that likewise seeks to extend the entirety of the First Amendment to the Internet. But there is no support for such an approach, which would have negative consequences both in online and offline contexts. Thus, the First Amendment is simply not implicated by the Access Provision’s enforcement of private choices.

Third, even if Plaintiffs had standing and could bring a First Amendment claim against the Access Provision, the claim would fail on the merits. At most, the CFAA should be subject only to intermediate scrutiny. And under that standard, the Access Provision clearly serves important government interests. For example, enforcing private websites’ decisions about whom to exclude helps protect private property rights, prevent theft of information by digital means, limit economic harm, and ensure that websites can protect their data and integrity. Moreover, specifically in the context of fake and/or misleading accounts, enforcement of the Access Provision helps deter fraud and other related criminal conduct, protect third-party users of the websites, and protect the public and national interests from fake accounts seeking to promote misinformation.

Plaintiffs do not dispute the importance of these governmental interests, and instead contend that these interests are not furthered by application of the Access Provision *as to them specifically*. But the Supreme Court has made clear that, even in an as-applied challenge, the inquiry is not limited exclusively to the plaintiff’s own conduct. Plaintiffs here make no argument that the Access Provision should be invalidated if the Court considers the full set of interests furthered by the provision.

In any event, even if Plaintiffs were correct that the inquiry were limited solely to their

conduct, enforcement of the Access Provision as to their conduct would still further the governmental interests discussed above, as the discovery record makes clear. For example, because the Access Provision only restricts *unauthorized* access, then by definition enforcement against unauthorized fake accounts promotes private property rights. That is true even if the fake accounts were created for noble purposes, such as academic research (as Plaintiffs claim here). Moreover, the discovery record contains several declarations from third-party companies explaining the harms that fake accounts inflict on their businesses.

In sum, this Court should either dismiss Plaintiffs' remaining claim for lack of subject-matter jurisdiction or enter summary judgment for Defendant. Plaintiffs have not carried their heightened burden of demonstrating their standing; the First Amendment is not implicated by private parties' choices about whom to exclude from their websites; and even if the First Amendment were implicated, the Access Provision would survive intermediate scrutiny.

BACKGROUND

I. LEGAL FRAMEWORK

As discussed previously, *see* Gov't MTD Mem. (ECF No. 10-1) at 4-5, Congress enacted the Computer Fraud and Abuse Act ("CFAA") in 1984 in an attempt to address the emergence of computer crimes. *See* Pub. L. No. 98-473, 98 Stat. 1837 (1984); H.R. Rep. No. 98-894, at 6 (1984). In crafting the CFAA, Congress was responding to what it considered to be a "recent flurry of electronic trespassing incidents." H.R. Rep. No. 98-894, at 6, 9-10.

Originally, the CFAA's "unauthorized access" provision prohibited obtaining information only from computers belonging to financial institutions or consumer reporting agencies. In 1996, however, Congress noted that "increasingly computer systems provide the vital backbone to many other industries," and therefore expanded provisions were necessary beyond just financial institutions and consumer reporting agencies. S. Rep. No. 104-357, at 7 (1996).

Accordingly, Congress amended the statute and enacted subsection (a)(2)(C), which was “intended to protect against the interstate or foreign theft of information by computer,” and “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.” *Id.*; *see also* Pub. L. No. 104-294, tit. II, § 201 (1996). That subsection now makes it a crime for any person to “intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer[.]” 18 U.S.C. § 1030(a)(2)(C). The term “protected computer” is defined to include a computer “which is used in or affecting interstate or foreign commerce or communication[.]” *Id.* § 1030(e)(2)(B). A violation of § 1030(a)(2)(C) is generally punishable as a misdemeanor (absent certain aggravating factors). *See id.* § 1030(c)(2).

Importantly, because § 1030(a)(2)(C) prohibits “access[ing] a computer without authorization or exceed[ing] authorized access,” that provision does not itself prohibit any individuals from accessing any publicly available computers. Instead, the statute regulates access only when a private party—*i.e.*, the owner of a protected computer—has limited (or declined to authorize) access to a protected computer.

Criminal violations of the CFAA are prosecuted by the Department of Justice (DOJ). The CFAA may be enforced by the local United States Attorney’s Offices (USAOs), or by other criminal litigating components of DOJ located in Washington, D.C. *See* Pls.’ Stmt. of Material Facts (ECF No. 47-2) ¶¶ 7-8 [hereafter “P-SMF”]. Among the criminal litigating components in Washington, D.C., the office most likely to be involved in CFAA prosecutions is the Computer Crime and Intellectual Property Section (CCIPS), which is a section within DOJ’s Criminal Division. *See id.* ¶ 7; Affidavit of John T. Lynch, Jr. (ECF No. 21-1) ¶ 3.

On September 11, 2014, the Attorney General issued a directive to all USAOs, the Criminal

Division, and the National Security Division regarding CFAA prosecutions. *See* Def.’s Stmt. of Material Facts (filed herewith) ¶¶ 14-15 (citing *Intake and Charging Policy for Computer Crime Matters*, previously filed at ECF No. 15-1) [hereafter “D-SMF”]. That charging policy makes clear that CFAA charges should be brought only when “a substantial federal interest would be served by prosecution[.]” ECF No. 15-1 at 1. The policy requires DOJ attorneys to consider several factors when determining whether a CFAA prosecution should be pursued, such as “the likelihood and extent of harm associated with . . . unauthorized access to the computer system,” and “[t]he extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm or a threat to national security[.]” ECF No. 15-1 at 1, 2. The policy also requires attorneys to consider “[w]hether the criminal conduct is based upon exceeding authorized access consistent with the policy set forth . . . below,” and that policy in turn provides that, “if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution may not be warranted.” *Id.* at 2, 5. Finally, to promote consistency in charging decisions across the country, the policy requires consultation with CCIPS prior to any charging decisions, and “[t]he consultation should be substantive in nature.” *Id.* at 6. This policy directive from the Attorney General remains in effect today. *See* D-SMF ¶ 15.

II. FACTUAL AND PROCEDURAL HISTORY

The two remaining Plaintiffs in this case, Alan Mislove and Christopher Wilson, are both computer science professors at Northeastern University. This lawsuit seeks to challenge the constitutionality of the Access Provision, 18 U.S.C. § 1030(a)(2)(C).

As part of Plaintiffs’ research as computer science professors, they seek to “conduct online audit tests to determine whether hiring websites discriminate among users on the basis of characteristics, such as race or gender, that are protected by civil rights laws.” Pls.’ MSJ Br. (ECF

No. 48) at 1 [hereafter “Pls.’ Br.”]. Plaintiffs have previously published two papers involving such “online audits.” *See* D-SMF ¶¶ 1-3. One paper (for which both Plaintiffs were authors) studied whether two prominent online free-lance marketplaces—TaskRabbit and Fiverr—are impacted by racial and gender bias. *Id.* ¶ 1. Another paper (for which only Plaintiff Wilson was an author) investigated “gender-based inequalities in the context of resume search engines,” as well as whether websites use “inferred gender of candidates as explicit features in their ranking algorithms.” *Id.* ¶ 2. Between these two papers, only the second question of the second paper involved creating fictitious or misleading user accounts on the websites. *Id.* ¶ 4.

Plaintiffs filed this lawsuit in June 2016, alleging a variety of constitutional claims against the Access Provision. *See* Compl. (ECF No. 1). In particular, Plaintiffs alleged that they wish to “conduct research into algorithmic discrimination in the employment context,” *id.* ¶ 107, and some of that research will involve creating fictitious jobs and fictitious job-seekers, contrary to websites’ Terms of Service (ToS), *id.* ¶¶ 118-19, 124. Thus, Plaintiffs alleged that they “are concerned that violating terms of service in the course of this work will subject them to criminal prosecution under the [Access] Provision.” *Id.* ¶ 126.

The Government filed a motion to dismiss Plaintiffs’ claims, and the Court granted that motion as to all claims except one—*i.e.*, an as-applied First Amendment claim for Plaintiffs Mislove and Wilson. *See* MTD Op. at 35-38. Specifically, the Court concluded 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,” *id.* at 9; that the Access Provision should be evaluated pursuant to intermediate scrutiny, *id.* at 35-36; and that, at the motion-to-dismiss stage, Plaintiffs had stated a plausible as-applied First Amendment claim against the Access Provision, *id.* at 37-38. The Court also concluded that Plaintiffs Mislove and

Wilson had standing to pursue that claim based on their allegation of a credible fear of prosecution under the Access Provision. *See id.* at 20-23.

Following resolution of the Government’s motion to dismiss, the parties engaged in discovery regarding Plaintiffs’ remaining as-applied claim. The parties engaged in written discovery, and also conducted several depositions. Plaintiffs deposed John T. Lynch, Jr., who is the Chief of CCIPS. *See* Def.’s Exh. 8. Defendant deposed the two remaining Plaintiffs, *see* Def.’s Exhs. 3-4, and also obtained third-party discovery from several private companies—Monster.com, LinkedIn, Facebook, and Glassdoor.com. *See* Def.’s Exhs. 11-14. Based on the record compiled during discovery, Defendant hereby files this cross-motion for summary judgment.

STANDARD OF REVIEW

“The court shall grant summary judgment if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law.” Fed. R. Civ. P. 56(a). Summary judgment is therefore appropriate “[w]here the record taken as a whole could not lead a rational trier of fact to find for the non-moving party[.]” *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986). “To survive a motion for summary judgment, the nonmoving party ‘must do more than simply show that there is some metaphysical doubt as to the material facts.’ Rather, that party ‘must come forward with specific facts showing that there is a genuine issue for trial.’” *Moore v. Carson*, 322 F. Supp. 3d 163, 166-67 (D.D.C. 2018) (Bates, J.) (quoting *Matsushita*, 475 U.S. at 586, citations omitted); *see also* Fed. R. Civ. P. 56(c)(1).

“[T]he mere existence of *some* alleged factual dispute between the parties will not defeat an otherwise properly supported motion for summary judgment; the requirement is that there be no *genuine* issue of *material* fact.” *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 247-48 (1986). A fact is material if it would “affect the outcome of the suit under the governing law[.]” *Id.* at 248. Additionally, “[i]f the evidence is merely colorable, or is not significantly probative, summary

judgment may be granted.” *Id.* at 249-50 (citations omitted).

ARGUMENT

Based on the factual record compiled during discovery, this Court should grant summary judgment for Defendant for three reasons. *First*, although the Court held that Plaintiffs had sufficiently established standing at the motion-to-dismiss stage, Plaintiffs have not carried their heightened burden to establish their standing here at the summary-judgment stage. *Second*, the First Amendment does not extend to the Government’s actions in enforcing private parties’ choices about whom to exclude from their private property, which is all that the Access Provision does. Plaintiffs have not demonstrated that private employment websites are “public forums” as a factual matter, nor would such a conclusion be consistent with Supreme Court precedent. *Third* and finally, the Access Provision is subject at most to intermediate scrutiny, which it amply satisfies. Numerous important governmental interests are furthered by the Access Provision—such as protecting private property, preventing economic harm, and avoiding misinformation—and those interests are furthered even as applied to Plaintiffs’ conduct specifically. For each of these reasons, the Court should enter judgment for Defendant.

I. AT SUMMARY JUDGMENT, PLAINTIFFS HAVE NOT CARRIED THEIR HEIGHTENED BURDEN OF ESTABLISHING STANDING

Although this Court concluded that Plaintiffs had standing to raise their claims at the motion-to-dismiss stage, that conclusion is no longer binding at summary judgment. *See Defs. of Wildlife*, 504 U.S. at 561 (the elements of standing are “an indispensable part of the plaintiff’s case,” and therefore “each element must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation”); *see also In re Navy Chaplaincy*, 323 F. Supp. 3d 25, 39 (D.D.C. 2018) (“On summary judgment, the plaintiff must establish each of these elements [of

standing] with ‘specific facts’ set out by affidavit or other admissible evidence.”).

Here, the factual record confirms that Plaintiffs lack standing for three reasons: Plaintiffs lack any concrete plans for conducting future research covered by their as-applied claim, *i.e.*, involving fake or misleading accounts; Plaintiffs have not demonstrated a credible threat of prosecution for any such research; and their claims are too abstract to be evaluated and therefore are not ripe. Accordingly, summary judgment for Defendant is warranted. At a minimum, Plaintiffs cannot obtain summary judgment because there are genuine disputes of material facts as to their standing. *See Dep’t of Commerce v. U.S. House of Reps.*, 525 U.S. 316, 329 (1999).

A. Plaintiffs Lack Any Concrete Plans for Pursuing Their Research

Plaintiffs’ sole remaining claim is about future research involving the creation of fake accounts and/or provision of misleading information. Plaintiffs lack standing, however, because they do not have any concrete plans to pursue such research. *See Defs. of Wildlife*, 504 U.S. at 564 (“Such ‘some day’ intentions—without any description of concrete plans, or indeed even any specification of *when* the some day will be—do not support a finding of the actual or imminent injury that our cases require.”); *see also Summers v. Earth Island Inst.*, 555 U.S. 488, 496 (2009) (an affidavit that “does not assert . . . any firm intention” but only a “vague desire” is “insufficient to satisfy the requirement of imminent injury”).

The most salient testimony comes from Plaintiffs’ depositions, during which they admitted that they lack concrete plans for research covered by their as-applied claim, *i.e.*, involving the creation of fake or misleading accounts. Plaintiff Wilson testified as follows:

Q: So just to summarize, there are no concrete plans for research involving providing false information in violation of websites’ terms of service?

A: Correct.

Q: And would it be the same answer for research involving the creation of fictitious user accounts?

A: Correct.

Q: Going beyond the projects that we have been discussing right now, are there concrete plans for any other type of research to test online discrimination where the research would involve creating fake user accounts?

A: No.

Q: And what about where the research would involve providing false information?

A: No.

Wilson Depo. Tr. at 62-63. Similarly, Plaintiff Mislove testified that “I am not currently undertaking research that currently involves creation of fictitious user accounts and providing false information.” Mislove Depo. Tr. at 45. And when asked about future research, he responded:

Q: Setting aside [a research project not at issue in this lawsuit], do you have concrete plans for any of that other future research?

A: No.

Id. at 47. Plaintiffs’ own deposition testimony thus confirms that they lack standing.

To be sure, Plaintiffs attempt now to resurrect their standing by filing two declarations—virtually identical—asserting that they “intend” to conduct research involving creating fake accounts and/or providing misleading information in violation of websites’ ToS. *See, e.g.*, Wilson Decl. (ECF No. 48-1) ¶ 10; Mislove Decl. (ECF No. 48-2) ¶ 10. At most, however, Plaintiffs’ declarations discuss only how they “intend” to undertake certain research, but they never discuss *when* that will actually be. Accordingly, the declarations still reflect nothing more than the “some day intentions” that are insufficient to establish standing. *See Worth v. Jackson*, 451 F.3d 854, 858 (D.C. Cir. 2006) (“Worth’s assertion that he ‘intends to apply for new positions and promotions at HUD on a regular basis in the future’ is just the kind of speculative intention normally insufficient for standing purposes.”); *see also Defs. of Wildlife*, 504 U.S. at 564 n.2.

Moreover, to the extent that Plaintiffs intend to rely on these declarations to suggest that

they *do* have concrete plans for their research, these declarations must be disregarded as an improper attempt to walk back their deposition testimony. “Virtually every circuit has adopted a form of the so-called ‘sham affidavit rule,’ which precludes a party from creating an issue of material fact by contradicting prior sworn testimony unless the shifting party can offer persuasive reasons for believing the supposed correction is more accurate than the prior testimony.” *Galvin v. Eli Lilly & Co.*, 488 F.3d 1026, 1030 (D.C. Cir. 2007); *see also Cowan v. Prudential Ins. Co. of Am.*, 141 F.3d 751, 756 (7th Cir. 1998) (“[A] deposition is the time for the plaintiff to make a record capable of surviving summary judgment—not a later filed affidavit.” (cited approvingly in *Galvin*, 488 F.3d at 1030)); *Glass v. Lahood*, 786 F. Supp. 2d 189, 216 (D.D.C. 2011), *aff’d*, No. 11-5144, 2011 WL 6759550 (D.C. Cir. Dec. 8, 2011). Plaintiffs’ declarations, therefore, cannot overcome their clear deposition testimony regarding their lack of concrete plans.

B. Plaintiffs Cannot Demonstrate a Credible Threat of Prosecution

Even if Plaintiffs had concrete plans to engage in future research involving the creation of fake accounts and/or the provision of misleading information in violation of websites’ ToS, Plaintiffs would still lack standing because they cannot “show that there is a credible threat of prosecution for th[eir] conduct under the statute.” MTD Op. at 19. “The question of whether a threat of prosecution adequate to satisfy the requirements of justiciability is present in any particular preenforcement challenge is a factual and case-specific one.” *Navegar, Inc. v. United States*, 103 F.3d 994, 999 (D.C. Cir. 1997). Here, the record confirms that Plaintiffs do not have a credible fear of prosecution: their own testimony acknowledges that they do not fear prosecution; the Government’s record of past CFAA prosecutions underscores that no prosecution is likely; and the Government’s public statements further confirm the speculative nature of any prosecution.

1. Plaintiffs Themselves Do Not Fear Prosecution Under the CFAA

The record compiled during discovery demonstrates that Plaintiffs themselves do not

actually fear prosecution under the CFAA. This fact alone should defeat Plaintiffs' standing.

Again, the most salient testimony comes from Plaintiffs' own depositions, during which they did not express any fear of prosecution under the Access Provision. Indeed, Plaintiff Mislove expressly acknowledged his lack of fear: "I think it is unlikely that I would [be] prosecuted for the research described in the complaint." Mislove Depo. Tr. at 146. And Plaintiff Wilson, when testifying about the reasons he brought this lawsuit, did not mention any concern about prosecution; he instead testified that the intent in filing the lawsuit "is to do good in the world." Wilson Depo. Tr. at 147; *see also id.* at 142 ("[T]he idea that a terms of service violation by itself it somehow a criminal or civil offense, I don't think that is compatible with the modern world."). Thus, Plaintiffs' own testimony highlights that this lawsuit is motivated by Plaintiffs' policy disagreements with the CFAA—not by any fear of prosecution under the CFAA.

Further confirming Plaintiffs' lack of fear of prosecution is the fact that Plaintiffs have *already engaged in* the very conduct that they claim to be prohibited by the CFAA. *See* D-SMF ¶ 8. Thus, Plaintiffs cannot contend that the threat of prosecution has "chilled" them from engaging in their desired conduct. *Cf. Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158-61 (2014). Indeed, neither Plaintiff could recall a single circumstance in which concerns about liability under the Access Provision prompted them to forego an algorithm audit into potential discrimination by an online website. *See* D-SMF ¶ 13. And notably, despite having already engaged in conduct allegedly prohibited by the CFAA, Plaintiffs concede that they have never once been threatened with arrest or prosecution based on such conduct. *See* D-SMF ¶¶ 9-10. Thus, there is no record of threatened enforcement against Plaintiffs that could support a credible fear of prosecution. *See, e.g., Steffel v. Thompson*, 415 U.S. 452, 459 (1974).

The closest Plaintiffs come to expressing a fear of prosecution is when, in their virtually

identical declarations appended to their motion for summary judgment, Plaintiffs each state: “I am concerned that violating terms of service in the course of the research plan will subject me to criminal prosecution[.]” Wilson Decl. (ECF No. 48-1) ¶ 52; Mislove Decl. (ECF No. 48-2) ¶ 49. But again, these self-serving affidavits cannot overcome their prior deposition testimony. *See* Part I.A, *supra*. More fundamentally, these statements represent nothing more than subjective “concerns” which are legally insufficient to establish Plaintiffs’ standing. *See Younger v. Harris*, 401 U.S. 37, 41-42 (1971) (holding that a bare assertion of “feel[ing] inhibited” is insufficient for pre-enforcement standing). Because any asserted fear of prosecution is therefore “imaginary or speculative,” *id.* at 42, Plaintiffs lack standing.

2. The Government’s Past CFAA Prosecutions Do Not Create a Credible Threat as to Plaintiffs

Plaintiffs’ motion does not contend, and cannot contend, that DOJ has previously enforced the Access Provision against conduct similar to Plaintiffs’ research. Instead, Plaintiffs rely on the fact that “the government has enforced the Access Provision in the past[.]” Pls.’ Br. at 8. But past prosecutions generally are not enough to establish Plaintiffs’ standing here.

As the Supreme Court recently stated, unless a plaintiff has been threatened with prosecution, the plaintiff must “allege[] an intent to engage in *the same speech* that was the subject of a prior enforcement proceeding.” *Susan B. Anthony List*, 573 U.S. at 166 (emphasis added); *see also id.* at 164 (“We have observed that past enforcement *against the same conduct* is good evidence that the threat of enforcement is not ‘chimerical.’” (emphasis added)). That logic should apply with particular force here, given that Plaintiffs’ only remaining claim is an as-applied one. Allowing Plaintiffs to rely on *other* prosecutions under the Access Provision—*i.e.*, prosecutions that do not implicate the same conduct as Plaintiffs’ as-applied claim—would not ensure a live case-or-controversy for Plaintiffs’ as-applied claim here. *Cf. DaimlerChrysler Corp. v. Cuno*, 547

U.S. 332, 352 (2006) (“[A] plaintiff must demonstrate standing for each claim he seeks to press.”).

Despite having the full tools of civil discovery available to them, Plaintiffs here have not identified a *single prosecution* under the Access Provision based on factual conduct similar to their research. Plaintiffs have conceded that they are unaware of *any* charges brought under the Access Provision since June 29, 2015, where the theory of “unauthorized access” was based, in whole or in part, on violation of a website’s ToS. *See* D-SMF ¶ 28.¹ Moreover, even without any time limitation, Plaintiffs have conceded that the *only* prosecutions they are aware of under the Access Provision involving ToS violations, in whole or in part, are the *Lowson* and *Drew* prosecutions. *See* Pls.’ Resp. to RFA No. 6 (Exh. 5); *see also* D-SMF ¶¶ 26, 29. But those prosecutions were initiated approximately nine or more years ago. *See* D-SMF ¶¶ 30-32. And as the Court previously noted, both of those cases “did, in fact, involve harmful conduct.” MTD Op. at 19; *see also* D-SMF ¶¶ 30-32. Thus, those two prosecutions provide a thin reed on which to conclude that Plaintiffs here face a credible threat of prosecution for their conduct.

Plaintiffs attempt to distract from their lack of evidence by accusing the Government of “not know[ing] whether prosecutors may have employed the Access Provision to obtain plea agreements in which defendants admitted to harmless ToS violations.” Pls.’ Br. at 9 (quoting MTD Op. at 21). At this stage, however, it is not the Government’s burden to prove a negative; Plaintiffs have the burden of demonstrating a “genuine issue” regarding their standing, and Plaintiffs cannot duck that burden after being given an opportunity to pursue the issue through discovery.

In any event, the record here disproves Plaintiffs’ assertion. Plaintiffs rely on the lack of comprehensive records within CCIPS regarding past CFAA prosecutions, *see* P-SMF ¶¶ 12-16,

¹ The June 29, 2015 date is important because that is the date that Plaintiffs themselves identified during discovery as the appropriate cut-off date for relevant information.

but Plaintiffs ignore that Defendant’s discovery responses were based not only on the internal records of CCIPS but also tracking data maintained by EOUSA. *See* D-SMF ¶¶ 33-39. After reviewing *both* sources of data, DOJ determined that no charges have been filed since June 29, 2015, under the Access Provision—whether by indictment, information, or complaint—in which the element of the element of “access[ing] a computer without authorization or exceed[ing] authorized access” was satisfied, in whole or in part, based on violation of a website’s or platform’s ToS. *See* D-SMF ¶¶ 36-38. Thus, DOJ has in fact determined that, since at least June 29, 2015, the Access Provision has not been used to obtain plea agreements based on website or platform ToS violations (harmless or otherwise). *See id.* ¶ 39. Even after a full opportunity to conduct discovery, then, Plaintiffs have failed to identify any past prosecutions (including those resolved by plea agreements) involving conduct similar to theirs.²

3. The Government’s Charging Policies and Public Statements Further Confirm that Any Risk of Prosecution is Speculative

Finally, if there were any remaining doubt, the Government’s public statements and actions underscore that any risk of prosecution for Plaintiffs’ purported conduct is speculative.

First, the Attorney General’s *Intake and Charging Policy for Computer Crime Matters* remains in effect, *see* D-SMF ¶ 15, and expressly cautions against prosecutions based on ToS violations. *See* ECF No. 15-1 at 2, 5; D-SMF ¶¶ 18-19, 21-23. Moreover, prosecution is especially unlikely under the policy if the conduct is genuinely harmless. *See* D-SMF ¶¶ 18-20, 40.

Second, DOJ officials have stated to Congress multiple times, across Administrations, that DOJ does not intend to prosecute harmless violations of contractual restrictions. *See* D-SMF ¶ 41.

² In its motion-to-dismiss opinion, the Court also noted the possibility of civil actions by private parties under the CFAA. *See* MTD Op. at 22 n.7. But Plaintiffs here do not rely on the prospect of such civil suits for purposes of their standing. *See, e.g.,* Pls.’ Resp. to Interrog. No. 15 (Def.’s Exh. 6); *see also* Pls.’ Br. at 8-9. And in any event, the record is similarly clear that Plaintiffs are unaware of any such civil suits being filed in the past. *See* D-SMF ¶ 27.

Although many of these statements were made in the context of proposing legislative changes to Congress, *cf.* MTD Op. at 22-23 n.8, the statements about a lack of intent to prosecute were not contingent on Congress adopting any such legislative proposals.

Third, with respect to the particular Plaintiffs and the conduct at issue in this case, the head of CCIPS—John T. Lynch, Jr.—has filed a sworn affidavit stating that “I am unaware of any federal criminal prosecution under the CFAA of conduct resembling the conduct described in the complaint” and “I do not expect that the Department would bring a CFAA prosecution based on such facts[.]” Affidavit of John T. Lynch, Jr. (ECF No. 21-1) ¶ 9. Mr. Lynch also reiterated this testimony during his deposition on behalf of DOJ as a whole. *See* D-SMF ¶¶ 24-25.

Plaintiffs make little effort to explain how, in light of the above policies and statements, they face anything more than an “imaginary or wholly speculative” chance of prosecution. *Babbitt v. United Farm Workers Nat. Union*, 442 U.S. 289, 302 (1979). Plaintiffs’ only response is to say that these statements do not “expressly disavow” any intent to prosecute them, and do not make it “impossible” for DOJ to bring a prosecution against them. Pls.’ Br. at 8, 9. Plaintiffs cite no authority, however, establishing that a plaintiff’s burden to demonstrate standing is satisfied where the Government has not come forward with proof of a non-existent threat of prosecution. Indeed, even in the mootness context—when the burdens are flipped, and the substantive standard is much higher—the D.C. Circuit has not required proof that a prosecution would be impossible. *See Clarke v. United States*, 915 F.2d 699, 702 (D.C. Cir. 1990) (en banc) (“Of course we cannot say that the risk of an attempted prosecution is zero. . . . But zero risk is not the test.”).

In short, even if Plaintiffs had standing at the motion-to-dismiss stage, the record compiled in discovery now warrants a different conclusion. Plaintiffs themselves do not fear prosecution; Plaintiffs have not uncovered even a single CFAA prosecution brought against similar facts using

a similar legal theory; and DOJ itself has implemented a charging policy, and publicly stated pursuant to that charging policy, that DOJ does not expect to initiate a CFAA prosecution based on Plaintiffs' conduct. Based on this record, Plaintiffs have established at most only a speculative risk of prosecution. *Cf. Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 420 (2013) (no standing where plaintiffs "present no concrete evidence to substantiate their fears, but instead rest on mere conjecture about possible governmental actions").

C. Plaintiffs' Claims Are Not Sufficiently Ripe for Adjudication

Finally, even if Plaintiffs' intent to conduct their research at some point in the future were sufficient to establish injury-in-fact, this Court should still decline to resolve Plaintiffs' claims given the abstract factual context in which those claims arise. *See, e.g., Babbitt*, 442 U.S. at 300 ("Even though a challenged statute is sure to work the injury alleged, however, adjudication might be postponed until a better factual record might be available.").

Here, even if Plaintiffs' general intent to conduct research were enough to establish standing, their claims are still too abstract for this Court to evaluate (or provide relief on). For example, Plaintiffs have not yet identified the specific websites that they intend to access for their research. *See* D-SMF ¶ 42. It is therefore impossible to know what those websites' ToS will be at the time of Plaintiffs' research, including whether the websites' ToS will even prohibit the creation of fictitious user accounts and/or provision of misleading information. *Id.* ¶¶ 42, 44. Similarly, even assuming the websites' ToS prohibit such actions, it is impossible to know whether those ToS will *condition access* on compliance sufficient to implicate the Access Provision.³ Thus, it is

³ As the Court recognized in its motion-to-dismiss opinion, not all ToS constitute genuine "access restrictions" sufficient to invoke the CFAA. *See* MTD Op. at 34 ("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."); *see also* D-SMF ¶¶ 43-44. Thus, some ToS may simply provide notice that providing false information

wholly speculative whether injunctive relief is even necessary—because if the websites’ ToS do *not* condition access in such a manner, then Plaintiffs are free to pursue their research without regard to the Access Provision. In such circumstances, courts have declined to hear pre-enforcement claims. *See, e.g., Babbitt*, 442 U.S. at 304; *Lion Mfg. Corp. v. Kennedy*, 330 F.2d 833, 839-41 (D.C. Cir. 1964).

Additionally, Plaintiffs also do not know the exact steps they will need to perform in order to conduct their research—including “the number of fictitious accounts or postings that will be necessary or how long each account or posting will exist.” Pls.’ Resp. to Def.’s Interrog. No. 8 (Def.’s Exh. 6); *see also* D-SMF ¶¶ 45-46, 48. The lack of concrete plans in this regard prevents the Court (and Defendant) from evaluating the potential harms caused by Plaintiffs’ studies. As Plaintiffs themselves testified during their depositions, evaluating the ethics of a potential study, and the potential harms caused by any study, requires an individualized, fact-specific, case-by-case analysis. *See* D-SMF ¶ 47. Were the Court to enter an injunction, therefore, the Court would effectively be providing judicial relief for as-yet-undefined conduct.

Granting judicial license for indeterminate conduct is not only contrary to principles of ripeness, *see, e.g., Am. Library Ass’n v. Barr*, 956 F.2d 1178, 1194 (D.C. Cir. 1992), but also Rule 65 itself. *See* Fed. R. Civ. P. 65(d)(1)(B), (C) (requiring that every injunction must “state its terms specifically” and “describe in reasonable detail—and not by referring to the complaint or other document—the act or acts restrained or required”). Plaintiffs’ proposed order here plainly contravenes these requirements. *See* ECF No. 47-1 ¶¶ 1, 2 (seeking relief authorizing them to conduct the research “described in Plaintiffs’ Complaint and Plaintiffs’ Declarations”). Plaintiffs’

may result in future revocation of access, but may not actually condition access upfront on the user’s provision of truthful information.

inability to request more specific relief underscores that the dispute, at present, is still too abstract to be ripe for adjudication.

II. THE FIRST AMENDMENT DOES NOT EXTEND TO ENFORCEMENT OF PRIVATE PARTIES' CHOICES ABOUT WHOM TO EXCLUDE

Even if this Court concludes it has jurisdiction over Plaintiffs' claim, Defendant is also entitled to summary judgment on the merits of the claim. Most fundamentally, the First Amendment does not extend to the Government's enforcement of private parties' decisions about how to restrict access to their websites. Admittedly, the Court concluded otherwise in its motion-to-dismiss opinion, holding that, unless a website has "taken real steps to limit who can access it," then even "privately-owned sites . . . are part of a public forum, government regulation of which is subject to heightened First Amendment scrutiny." MTD Op. at 9-11. Notwithstanding this prior conclusion, at this stage in the litigation, summary judgment is warranted in Defendant's favor.

First, as a factual matter, the record here confirms that many websites *have* taken meaningful steps to limit access to them—thereby bringing the websites outside the "public forum" concept under the Court's prior framework. Indeed, the parties have now stipulated that the websites here are not "public forums" for First Amendment purposes.

Second, if the Court is not persuaded by the factual argument, Defendant respectfully requests that the Court reconsider its prior legal analysis regarding private websites constituting public forums. The "public forum" doctrine applies only to government-owned or government-controlled property, and the Supreme Court's recent decision in *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), does not change that analysis.

Finally, Plaintiffs' alternative theory of First Amendment scrutiny—that the CFAA constitutes "state action" sufficient to allow this Court to review private parties' decisions about whom to exclude—conflates the concept of "state action" with the scope of the First Amendment

itself. The Supreme Court has made clear that, even when there is state action, the First Amendment still does not extend to enforcement of private parties' choices regarding their private property. Indeed, adopting either Plaintiffs' theory or the "public forum" theory—thereby rendering much of the Internet subject to the First Amendment—would have negative consequences for the Internet as a whole.

A. The Factual Record Here Confirms that, Under the Court's Prior Framework, the Relevant Websites Are Not Public Forums

The Court's motion-to-dismiss opinion held that, although private websites are generally part of a public forum, "it would be ill-advised to equate the *entirety* of the Internet with public streets and parks." MTD Op. at 10 (modifications omitted). Specifically, "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." *Id.* at 11 (modifications omitted). Here, the factual record confirms that the relevant websites are *not* public forums even under the Court's framework.

In particular, Plaintiffs admitted that, for the websites and/or platforms that they previously accessed for research, as well as those that they may access in the future, "none of the websites or platforms identified by Plaintiffs . . . constitutes a 'public forum' for First Amendment purposes." Pls.' Resp. to RFA No. 11 (Def.'s Exh. 5); *see also* D-SMF ¶ 49. Nor did Plaintiffs identify any facts supporting a conclusion that any of those websites constitutes a "public forum" for First Amendment purposes. *See* D-SMF ¶ 50.

Collectively, this discovery confirms that summary judgment to Defendant is required. *Cf. Celotex Corp. v. Catrett*, 477 U.S. 317, 325 (1986) (summary judgment is appropriate if "there is an absence of evidence to support the nonmoving party's case"). Indeed, Plaintiffs' response to the request for admission is binding on the Court and should itself be the end of the analysis. *See*

Fed. R. Civ. P. 36(b) (“A matter admitted under this rule is conclusively established unless the court, on motion, permits the admission to be withdrawn or amended.”); *cf. McNamara v. Miller*, 269 F.2d 511, 515 (D.C. Cir. 1959).

Other evidence in the record likewise confirms that social media and online employment websites are not public forums. As the declarations from third-party companies highlight, those companies have indeed “taken real steps to limit who can access” their websites, MTD Op. at 11, particularly with respect to preventing the creation of fictitious and/or misleading accounts. *See* D-SMF ¶¶ 51-60. For example, LinkedIn “employs a range of technological measures and investigative tools to block, detect, and restrict fake accounts.” Rockwell Decl. (Exh. 11) ¶ 19. Other companies similarly rely on technological or automated processes to detect and prevent fictitious accounts. *See* D-SMF ¶¶ 52-54. Additionally, one of the companies Plaintiffs previously studied imposes a meaningful barrier to access by requiring that a valid business license be provided before access to the site is granted. *See* D-SMF ¶ 58. Plaintiffs obtained access to the site only after providing business license information from a company with which Plaintiffs are not actually affiliated. *See* D-SMF ¶¶ 59-60.

Even if it appears to a real user that a website allows anyone to freely create an account, therefore, the website may still have erected meaningful technological obstacles in an effort “to limit who can access” the website. MTD Op. at 11. Thus, the record here—particularly Plaintiffs’ binding response to Defendant’s request for admission—establishes that the relevant websites are not “public forums” even under the framework previously articulated by the Court.

B. Private Websites Are Not “Public Forums” as a Matter of Law

To the extent the Court concludes as a factual matter that the relevant websites here may still qualify as public forums, Defendant respectfully requests the Court revisit its prior legal conclusion that “public forum” analysis is appropriate for privately owned websites. There is no

impediment to the Court revisiting the issue at this stage, *cf.* Fed. R. Civ. P. 54(b), particularly given that the issue was not fully briefed at the motion-to-dismiss stage and Plaintiffs themselves are not urging this Court to base its summary-judgment ruling on “public forum” analysis. *See* Pls.’ Br. at 10. In light of the more fulsome briefing below, the Government respectfully submits that there are strong reasons to revisit the prior analysis.

1. The Supreme Court Has Held that Private Choices About Whom to Exclude are Not Subject to the First Amendment

As the Government argued (and the Court recognized) at the motion-to-dismiss stage, the Supreme Court has held that private actors may, without running afoul of the First Amendment, limit the speech that occurs on their private property. *See* MTD Op. at 7-8.

The Supreme Court first held as much in *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972), which addressed whether a shopping mall could prohibit individuals from distributing handbills in opposition to the Vietnam War within the mall. The Supreme Court rejected the individuals’ First Amendment claim, holding that private property does not “lose its private character merely because the public is generally invited to use it for designated purposes.” *Id.* at 569.

Several years later, the Supreme Court re-affirmed *Lloyd Corp.*, and again held that a shopping mall could lawfully exclude employees of a store from picketing within the mall. *See Hudgens v. NLRB*, 424 U.S. 507, 520-21 (1976) (holding that because “the respondents in the *Lloyd* case did not have a First Amendment right to enter that shopping center to distribute handbills concerning Vietnam, then the pickets in the present case did not have a First Amendment right to enter this shopping center for the purpose of advertising their strike against the Butler Shoe Co.”); *see also Cent. Hardware Co. v. NLRB*, 407 U.S. 539, 547 (1972) (holding that private property “open to the public” does not become subject to the First Amendment, because that would “constitute an unwarranted infringement of long-settled rights of private property protected by the

Fifth and Fourteenth Amendments”). Consistent with these cases, the First Amendment does not prohibit private actors—such as private website owners—from excluding individuals from their private property even when those individuals seek to engage in speech.

At the motion-to-dismiss stage, the Court rejected the applicability of these cases, reasoning that “quite simply, the Internet is different.” MTD Op. at 8. In particular, the Court concluded that “the public Internet is too heavily suffused with First Amendment activity . . . to sustain a direct parallel to the physical world.” *Id.* at 10. Therefore, even “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.” *Id.* at 9.

Respectfully, however the “public forum” doctrine should not be extended to a new arena of privately owned websites, and the *Packingham* decision does not support such an extension. In particular, the application of *Packingham* here overlooks two important distinctions: first, *Packingham* did not involve “public forum” analysis because that doctrine is limited to government-owned or government-controlled property; and second, *Packingham* involved a *state* prohibition on individuals accessing social media websites, not enforcement of *private parties’* choices about whom to exclude (as in *Lloyd Corp.* and *Hudgens*).

2. The “Public Forum” Doctrine Is Limited to Government-Owned or Government-Controlled Property

Under the First Amendment, a “public forum” consists of either “public property which the state has opened for use by the public as a place for expressive activity” or “places which by long tradition . . . have been devoted to assembly and debate[.]” *Perry Educ. Ass’n v. Perry Local Educators’ Ass’n*, 460 U.S. 37, 45 (1983). Quintessential examples of public forums include “[p]ublic streets and parks[.]” *Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 802 (1985). Public forums may also exist “more in a metaphysical than in a spatial or geographic

sense,” such as a state university’s student activities fund. *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 830 (1995).

In all such “public forum” cases, however, the critical feature is that the forum constitutes government-owned or government-controlled property. *See, e.g., Walker v. Texas Div., Sons of Confederate Veterans, Inc.*, 135 S. Ct. 2239, 2250 (2015) (“We have previously used what we have called ‘forum analysis’ to evaluate government restrictions on purely private speech *that occurs on government property.*” (emphasis added)); *Christian Legal Soc’y v. Martinez*, 561 U.S. 661, 679 (2010) (“[I]n a progression of cases, this Court has employed forum analysis to determine when a governmental entity, in *regulating property in its charge*, may place limitations on speech.” (emphasis added)); *Int’l Soc’y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 678 (1992) (“These cases reflect . . . a ‘forum based’ approach for assessing restrictions that the government seeks to place on the use *of its property.*” (emphasis added)); *Perry Educ. Ass’n*, 460 U.S. at 44 (discussing forum analysis in the context of “[t]he existence of a right of access to *public property*” (emphasis added)); *Tele-Comm’ns of Key W., Inc. v. United States*, 757 F.2d 1330, 1337 (D.C. Cir. 1985) (“The public forum doctrine . . . defines situations in which the government cannot close *government-owned property* to parties who desire to use that property as a forum for exercising their First Amendment rights.” (emphasis added)); *cf.* Pls.’ Br. at 10 (acknowledging that “forum analysis is appropriate in the context of *government-owned property*”).

Here, of course, private websites are not government-owned or government-controlled property, and therefore cannot be considered public forums. The Supreme Court, moreover, has made clear that “public forum” analysis should not be extended into new and developing arenas. *See, e.g., United States v. Am. Library Ass’n, Inc.*, 539 U.S. 194, 205-06 (2003) (holding that “Internet access in public libraries” is not a public forum and noting that “[w]e have rejected the

view that traditional public forum status extends beyond its historic confines”); *Arkansas Educ. Television Comm’n v. Forbes*, 523 U.S. 666, 672-73 (1998).

In its motion-to-dismiss opinion, the Court offered a hypothetical to support its “public forum” analysis. The Court discussed the situation of food trucks, which “are privately owned businesses” that “lin[e] the streets.” MTD Op. at 9. The Court hypothesized:

[I]f 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.

Id. In the Court’s view, it “makes good sense to treat the Internet” in the same manner. *Id.*

Respectfully, this hypothetical does not accurately capture the legal question presented here. Specifically, in the hypothetical the customer is standing on the sidewalk when making her comments, and there is no dispute that a public sidewalk constitutes a public forum. The very question to be decided here, however, is whether a public forum exists or not—*i.e.*, whether an individual creating an account on a private website is in a public forum (entitled to First Amendment protection) or instead on private property (with no First Amendment protection).

In the Government’s view, the appropriate analogy would be if the customer were to stand on the *roof* of the food truck and criticize her purchase. Even if the food truck would otherwise exist in a public forum (*i.e.*, the side of a public street), and even if the food truck were willing to permit *favorable* reviews to be shouted from its rooftop, the food truck would not violate the First Amendment by excluding the negative customer from its rooftop (and/or in requesting the Government’s assistance in excluding the patron from the rooftop). *Cf. Lloyd Corp.*, 407 U.S. at 569 (“Nor does property lose its private character merely because the public is generally invited to use it for designated purposes.”). The same is true of the private websites here; even though they generally invite the public to use the websites, that does not transform them into a “public

forum” for First Amendment purposes.

To be sure, the Internet is different from a food truck rooftop because the Internet is “a primary location for First Amendment activity[.]” MTD Op. at 8 (citing *Packingham*, 137 S. Ct. at 1735). The amount of First Amendment activity occurring in a private location, however, is not a basis for subjecting that property to the First Amendment’s requirements. Prior to the Internet’s existence, there was surely a significant amount of First Amendment-protected activity occurring in shopping malls throughout the country. *Cf. Lloyd Corp.*, 407 U.S. at 553-55 (discussing the various activities that were allowed to occur throughout the shopping mall’s facilities). And even today, significant First Amendment-protected activity occurs in privately owned restaurants and other commercial establishments. Even so, there is no First Amendment violation when one of those privately owned establishments instructs a patron to leave—even if the reasons for instructing the patron to leave would constitute a First Amendment violation if relied upon by a municipal official to remove the patron from a public sidewalk.⁴

Notwithstanding the amount of First Amendment activity occurring on websites, therefore, they remain private property that is not subject to “public forum” analysis. Instead, the private websites are more analogous to the private shopping centers at issue in *Hudgens* and *Lloyd Corp.*

3. The Supreme Court’s *Packingham* Decision Does Not Change the First Amendment Status of Private Websites

In its motion-to-dismiss opinion, the Court rejected the applicability of *Hudgens* and *Lloyd Corp.*, relying heavily on the *Packingham* decision. Respectfully, however, there is a key distinction between *Packingham* and the First Amendment issues implicated here—namely,

⁴ For example, a bar owner can direct a patron espousing unpopular political views to leave his bar, even though a police officer plainly cannot do so if the patron is on a public sidewalk. *Cf. MTD Op.* at 9 (“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.”).

Packingham involved a *state* prohibition on conduct, not merely enforcement of *private parties'* choices. Because state prohibitions are clearly subject to First Amendment scrutiny, the Court in *Packingham* had no occasion to address “public forum” doctrine, or a statute like the CFAA that merely enforces private parties’ choices.

In *Packingham*, the law at issue “ma[de] it a felony for a registered sex offender ‘to access a commercial social networking Web site where the sex offender knows that the site permits minor children to become members or to create or maintain personal Web pages.’” *Packingham*, 137 S. Ct. at 1733 (quoting N.C. Gen. Stat. Ann. § 14–202.5(a), (e) (2015)). Thus, there was no dispute that *the state itself* had enacted a criminal prohibition on a sex offender accessing websites. *Cf. Packingham*, 137 S. Ct. at 1737 (noting that the North Carolina statute had the effect of “foreclos[ing] access to social media altogether” and thereby “prevent[ing] the user from engaging in the legitimate exercise of First Amendment rights”).

State prohibitions on expressive activity are clearly subject to First Amendment scrutiny without regard to “public forum” analysis. For example, if a state were to enact a ban on yard signs, there is no question that the ban would be subject to First Amendment scrutiny—even though each individual person’s yard is not a “public forum” under the First Amendment. *See, e.g., City of Ladue v. Gilleo*, 512 U.S. 43 (1994) (invalidating an ordinance restricting the display of residential yard signs). That type of *state* prohibition on expressive activity is distinct from the CFAA, however, which merely prohibits “access[ing] a computer without authorization or exceed[ing] authorized access[.]” 18 U.S.C. § 1030(a)(2)(C). Under the CFAA, it is the *private website* that decides whether someone is permitted to access the website; the Government itself has not forbidden any access.

To use an analogy to illustrate the distinction, if the Government passed a law making it a

criminal offense to distribute political handbills in private shopping centers, there is no dispute that such a law would be subject to First Amendment scrutiny (and would almost certainly be struck down). The situation is altogether different, however, if the *owner of the shopping center* is the one who has decided to prohibit such political handbilling and the Government is merely enforcing that private owner's choice. The former situation is equivalent to what the Court confronted in *Packingham*, whereas the latter situation is what arises under the CFAA—and is what the Supreme Court upheld in *Hudgens* and *Lloyd Corp.* The two situations—a governmental prohibition, versus government enforcement of a private party's prohibition—are fundamentally different, and warrant different treatment under the First Amendment.

Recognizing this key distinction, several courts have held even after *Packingham* that private websites themselves remain outside the First Amendment. *See, e.g., Freedom Watch, Inc. v. Google, Inc.*, --- F. Supp. 3d ----, 2019 WL 1201549, at *7 (D.D.C. Mar. 14, 2019) (“True, in *Packingham*, the Supreme Court recognized that Facebook and Twitter are among the ‘most important places (in a spatial sense) for the exchange of views’ in society today. But the case involved a challenge to a state law that limited the speech rights of certain criminals on these platforms. It did not create a new cause of action against a private entity for an alleged First Amendment violation.”); *Prager Univ. v. Google LLC*, 2018 WL 1471939, at *8 (N.D. Cal. Mar. 26, 2018) (“*Packingham* did not, and had no occasion to, address whether private social media corporations like YouTube are state actors that must regulate the content of their websites according to the strictures of the First Amendment.”); *Nyabwa v. FaceBook*, 2018 WL 585467, at *1 (S.D. Tex. Jan. 26, 2018); *Johnson v. Cache Cty. Sch. Dist.*, 323 F. Supp. 3d 1301, 1314 (D. Utah 2018). Consistent with these decisions and “public forum” doctrine generally, this Court should decline to hold that private websites are “public forums” subject to the First Amendment.

C. Plaintiffs' Alternative Theory Focusing on State Action Likewise Does Not Allow First Amendment Scrutiny of Private Choices

Plaintiffs do not argue that private websites are “public forums,” and instead offer an alternative theory for how the First Amendment extends to their claims—*i.e.*, because “[t]he government action that is being challenged is the criminalization of [Plaintiffs’] false statements[.]” Pls.’ Br. at 9. But Plaintiffs’ argument improperly conflates the concept of state action with the scope of the First Amendment itself. Moreover, Plaintiffs’ argument sweeps too broadly: it would apply the First Amendment not only to private websites but also to other statutes in which the Government enforces private parties’ choices, *e.g.*, trespass, copyright, etc.

The Government does not dispute that initiation of a criminal prosecution under the CFAA would constitute state action. *Cf.* MTD Op. at 16-17. Even when state action exists, however, the scope of the underlying First Amendment rights presents a separate question. *See LaRouche v. Fowler*, 152 F.3d 974, 993 (D.C. Cir. 1998) (“[E]ven if party delegate-selection rules are state action, we still must consider ‘the reach of the Due Process Clause in this unique context.’” (quoting *O’Brien v. Brown*, 409 U.S. 1, 4 (1972))).

Here, the problem with Plaintiffs’ claim is not a lack of state action; rather, the problem is that the First Amendment’s protections do not extend to private parties’ choices about whom to exclude from private property. *See* Part II.B.1, *supra*; *Hudgens*, 424 U.S. at 520-21 (“[T]he pickets in the present case *did not have a First Amendment right* to enter this shopping center for the purpose of advertising their strike against the Butler Shoe Co.” (emphasis added)); *see also PruneYard Shopping Ctr. v. Robins*, 447 U.S. 74, 81 (1980). Because there is no First Amendment right of access to private property over the property owner’s objections, there is *a fortiori* no First Amendment violation when the Government enforces the private property owner’s decision.

With respect to the Access Provision, Plaintiffs seek to gloss over the role of private

property owners. *See* Pls.’ Br. at 10 (“The government does not, and cannot, dispute that as applied to Plaintiffs, the Access Provision operates as a ban on false speech.”). But that assertion is flatly incorrect: the Access Provision does not “ban” any speech at all; it simply allows *private parties* to choose under what conditions people are authorized to access their platforms, and then the Access Provision provides an enforcement mechanism for those private choices. Indeed, this Court essentially recognized as much at the motion-to-dismiss stage, noting that “the Access Provision looks similar to many criminal laws that are rendered operative *by a private party’s decision* whether to authorize certain conduct.” MTD Op. at 43 (emphasis added).⁵

If Plaintiffs’ argument were correct—that the existence of the CFAA is “state action” sufficient to subject private parties’ access choices to First Amendment scrutiny—then private websites would be required to comply with the First Amendment *in toto*. As this Court has acknowledged, “state action” can exist simply through judicial action, even in a dispute between private parties. *See* MTD Op. at 16 (citing *New York Times Co. v. Sullivan*, 376 U.S. 254, 265 (1964)). Even apart from the prospect of CFAA criminal enforcement, therefore, a *civil* lawsuit arising under the CFAA would also involve “state action” sufficient to bring the First Amendment into play. *See* 18 U.S.C. § 1030(g) (authorizing private civil actions for damages and injunctive relief). Under Plaintiffs’ approach, then, the “state action” of a civil CFAA suit would expose the private website’s full range of decisions to First Amendment scrutiny.

⁵ The fact that the CFAA only enforces private parties’ choices is also what distinguishes the Access Provision from cases like *United States v. Alvarez*, 567 U.S. 709 (2012), and the cases addressing so-called “ag-gag” laws. In those cases, the criminal statutes directly prohibit false speech by itself. *See, e.g., Alvarez*, 567 U.S. at 722-23 (“The Act by its plain terms applies to a false statement made at any time, in any place, to any person.”); *Animal Legal Def. Fund v. Wasden*, 878 F.3d 1184, 1196 (9th Cir. 2018) (“[T]he misrepresentation provision . . . regulates protected speech while targeting falsity and nothing more.” (modifications omitted)). Here, however, the Access Provision does not directly prohibit any speech (false or otherwise); rather, it prohibits only unauthorized access, and it allows private website owners to define what access is authorized.

To illustrate the problems with such an approach, imagine an online forum devoted to hosting cute pictures of animals. To fulfill its purpose, the forum has made clear that it will revoke access for anyone posting pictures of animals being harmed. A particularly obnoxious user repeatedly posts videos of animal cruelty, however, and continues to create new accounts for that purpose while the forum does its best to disable each new account. When the forum (frustrated with needing to constantly disable the user's accounts) finally sues to obtain an injunction prohibiting the user from creating new accounts and posting such content, under Plaintiffs' approach, the First Amendment would *prohibit* a court from ruling in favor of the forum—because state action exists in the form of the civil suit, and the user's videos of animal cruelty constitute speech protected by the First Amendment. *See generally United States v. Stevens*, 559 U.S. 460 (2010). In essence, then, Plaintiffs' approach would require private websites to comply in full with the strictures of the First Amendment.⁶

Furthermore, the impact of Plaintiffs' approach would not be limited to the online arena. Again, the example of trespass is instructive. Imagine a scenario where a host invites several neighbors over to the host's home for dinner, but one of the neighbors then begins talking politics over the host's objection. The host directs the neighbor to leave, and ultimately the host calls the police for assistance in removing the neighbor. Under Plaintiffs' approach, police enforcement of trespass law would constitute state action, and it would therefore violate the First Amendment for the police to remove the neighbor based on the neighbor's political speech.

⁶ In a footnote, Plaintiffs insist that they are “not challeng[ing] the ability of online websites to remove false posts or fictitious accounts[.]” Pls.' Br. at 10 n.1. But the logic of their argument would prohibit online websites from enlisting any Government machinery (such as police or the courts) in their efforts to prevent such conduct. Moreover, a user could sue a website prospectively—seeking a judicial declaration that the user is entitled to access the website, *cf. Lloyd Corp.*, 407 U.S. at 556—and Plaintiffs' logic would compel courts to grant that relief.

There is simply no support for the unstated premise of Plaintiffs' argument—*i.e.*, that when the Government enforces private parties' choices about whom to exclude, the Government may lawfully do so only if the private parties' choice itself complies with the First Amendment. To the contrary, numerous courts—including the D.C. Circuit—have held that the First Amendment is not violated when the Government enforces trespass law on private property. *See Nat'l Org. for Women v. Operation Rescue*, 37 F.3d 646, 655 (D.C. Cir. 1994) (“Appellants have no general First Amendment right to trespass on private property or to physically block access to private property as a means of protest[.]” (citations omitted)); *Cape Cod Nursing Home Council v. Rambling Rose Rest Home*, 667 F.2d 238, 243 (1st Cir. 1981) (rejecting a “bootstrap argument” in which “Plaintiffs are attempting to create a first amendment right of access simply from the police involvement in arresting them”); *see also, e.g., Kalfus v. New York & Presbyterian Hosp.*, 476 F. App'x 877, 879-80 (2d Cir. 2012); *Utah Gospel Mission v. Salt Lake City Corp.*, 316 F. Supp. 2d 1201, 1225 n.24 (D. Utah 2004), *aff'd*, 425 F.3d 1249 (10th Cir. 2005); *Sw. Cmty. Res., Inc. v. Simon Prop. Grp., LP*, 108 F. Supp. 2d 1239, 1250 (D.N.M. 2000). Again, the Access Provision is analogous to physical trespass law—both involve private parties determining who is authorized to access private property, and then the Government merely upholding property owners' rights to make those private choices about their property.

Finally, for the same reason, Plaintiffs get no benefit from their straw-man hypothetical: “If a person's First Amendment rights were extinguished the moment she stepped foot on private property, the State could, for example, criminalize any criticism of the Governor, or any discussion about the opposition party, or any talk of politics whatsoever, if done on private property.” Pls.' Br. at 10 (quoting *Western Watersheds Project v. Michael*, 353 F. Supp. 3d 1176, 1189 n.7 (D. Wyo. 2018)). As discussed above, a government statute criminalizing political discussion (whether on

private or public property) would clearly violate the First Amendment. But here, the Access Provision only enforces *private parties'* choices about what to allow, and whom to exclude, on their private property. As such, the First Amendment is not implicated, consistent with the Supreme Court's decisions in *Hudgens* and *Lloyd Corp.*

D. Applying the First Amendment to the Modern Internet Would Have Negative Consequences

Accepting either of the legal theories above—that private websites are “public forums,” or are subject to First Amendment scrutiny based on the existence of state action—would effectively be a declaration that much of the modern Internet is subject to the First Amendment's requirements. That far-reaching holding would have serious detrimental consequences.

First, to the extent the Court's First Amendment analysis turns on whether websites “have taken real steps to limit who can access” their information, MTD Op. at 11, that would only encourage websites to limit access further, and to place more of their information behind secure barriers. Such a result would be contrary to First Amendment values, which tend to promote the free flow of information. *Cf. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc.*, 425 U.S. 748, 765 (1976). Encouraging websites to erect additional barriers would also threaten to transform the very nature of the Internet—away from hosting “vast democratic fora,” *Reno v. ACLU*, 521 U.S. 844, 868 (1997), and allowing individuals to “explor[e] the vast realms of human thought and knowledge,” *Packingham*, 137 S. Ct. at 1737—even though those are the very First Amendment values that seemed to motivate the *Packingham* decision itself.

Second, even apart from websites' accessibility, applying the First Amendment to websites would also fundamentally transform their content. If the First Amendment indeed applies to private websites, those websites can no longer prohibit users from posting numerous types of objectionable content: videos depicting animal cruelty, *see Stevens*, 559 U.S. at 472; patently

offensive speech, *see Snyder v. Phelps*, 562 U.S. 443 (2011); videos of nude dancing, *see City of Erie v. Pap's A.M.*, 529 U.S. 277 (2000); virtual or simulated child pornography, *see Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002); messages that advocate violence in a non-imminent way, *see Brandenburg v. Ohio*, 395 U.S. 444 (1969) (per curiam); as well as “[s]peech that demeans on the basis of race, ethnicity, gender, religion, age, disability, or any other similar ground [that] is hateful,” *Matal v. Tam*, 137 S. Ct. 1744, 1764 (2017) (opinion of Alito, J.).

Indeed, Congress through the Communications Decency Act has seen fit to grant websites express approval to remove objectionable content from their websites. *See* 47 U.S.C. § 230(c)(2)(A) (“No provider or user of an interactive computer service shall be held liable on account of . . . any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected[.]”). Requiring private websites to comply with the First Amendment would call into question the constitutionality of this statute, which would likewise have significant consequences for the modern Internet. *Cf. Blumenthal v. Drudge*, 992 F. Supp. 44, 49 (D.D.C. 1998) (explaining the uniqueness of this statute for the Internet, compared to other publishing mediums).

III. AT MOST, THE CFAA WOULD BE SUBJECT TO INTERMEDIATE SCRUTINY

Even assuming that the First Amendment extends to the type of conduct covered by the Access Provision, the next step would be to define the appropriate standard of review. Contrary to Plaintiffs’ argument, the Access Provision is not a content-based restriction. Indeed, Plaintiffs’ claim does not implicate any expressive conduct at all. At most, the Access Provision would be subject to intermediate scrutiny, as the Court held in its motion-to-dismiss opinion.

A. The Access Provision is Not a Content-Based Restriction

Plaintiffs briefly assert that the Access Provision should be subject to strict scrutiny because

it is a content-based regulation of their speech. *See* Pls.’ Br. at 12-13. A statute can be content-based if it “on its face draws distinctions based on the message a speaker conveys,” if it “cannot be justified without reference to the content of the regulated speech,” or if it was “adopted by the government because of disagreement with the message the speech conveys.” *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). Here, the Court has already correctly concluded that the Access Provision “itself does not target speech, or impose content-based regulations, on its face,” nor was “the government’s purpose . . . to restrict speech based on its content or viewpoint.” MTD Op. at 36. Thus, the Access Provision is not subject to strict scrutiny. *Id.*

Plaintiffs do not dispute the Court’s prior conclusion, and instead argue that even if the Access Provision is facially neutral, “the Access Provision’s application to Plaintiffs specifically is content based, because it would apply to Plaintiffs only when the message they convey to a website is false, instead of true.” Pls.’ Br. at 12. Plaintiffs cite no authority, however, establishing that the content-based analysis is different for as-applied claims—*i.e.*, that an otherwise content-neutral statute can become content-based according to its “application to Plaintiffs specifically[.]” *Id.*; *cf. ANSWER Coal. v. Basham*, 845 F.3d 1199, 1210 (D.C. Cir. 2017) (“ANSWER’s admittedly viewpoint-based reason for seeking access to the Plaza does not, however, make any rule that stands in its way content based.”). Indeed, Plaintiffs’ approach would threaten to transform *all* as-applied claims into challenging content-based restrictions, because the very nature of such claims is to focus on the “application to Plaintiffs specifically.”

In any event, even when examining Plaintiffs’ particular conduct, the Access Provision still is not content-based. The applicability of the Access Provision does not turn on whether Plaintiffs’ speech is true or false; instead it depends on whether Plaintiffs’ access to the platform is authorized or not. Thus, Plaintiffs violate the statute not based on *what* they say, but based on their presence

on a private platform without authorization. *See McCullen v. Coakley*, 573 U.S. 464, 479-80 (2014) (holding that a statute is not content-based because “[w]hether petitioners violate the Act depends not on what they say, but simply on where they say it” (citations omitted)).

Plaintiffs also suggest that, following the Supreme Court’s decision in *Alvarez*, some courts “have focused on the value of the expression at issue and the likelihood that the targeted expression will result in significant harm in determining what level of scrutiny to apply.” Pls.’ Br. at 13. Only one of Plaintiffs’ cited cases meaningfully engaged on the appropriate level of scrutiny, however, and that case involved a content-based restriction on false political speech. *See 281 Care Comm. v. Arneson*, 766 F.3d 774, 784 (8th Cir. 2014). Thus, it says little about the appropriate level of scrutiny for the content-neutral Access Provision here. And more generally, Plaintiffs’ request for an *ad hoc* balancing of the value of their speech would run *counter* to First Amendment values, which typically discourage such value judgments. *See Stevens*, 559 U.S. at 470 (“The First Amendment’s guarantee of free speech does not extend only to categories of speech that survive an *ad hoc* balancing of relative social costs and benefits.”); *see also McCutcheon v. FEC*, 572 U.S. 185, 206 (2014) (plurality op.). Thus, Plaintiffs’ cited cases likewise do not provide a reason to apply strict scrutiny to the Access Provision.

B. Plaintiffs’ Sole Remaining Claim Does Not Implicate Any Expressive Activity

In its motion-to-dismiss opinion, the Court concluded that intermediate scrutiny should apply to the Access Provision. *See* MTD Op. at 36 n.14. But even if the Court concludes that the websites here are public forums, before applying intermediate scrutiny the Court must also conclude that Plaintiffs’ proposed conduct constitutes expressive activity. *See Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 707 (1986) (holding that intermediate scrutiny “has no relevance to a statute directed at imposing sanctions on nonexpressive activity”). Here, Plaintiffs’ conduct is not expressive in any way, as confirmed by the discovery record.

First, because the Access Provision prohibits unauthorized access to computers, it is legally irrelevant whether Plaintiffs' intent to access the websites is for speech or other expressive purposes. As the Supreme Court has explained, even when a person intends to engage in speech, regulating unauthorized access to property does not implicate expressive activity:

Even assuming the streets of Whitcomb Court are a public forum, the notice-barment rule subjects to arrest those who reenter after trespassing and after being warned not to return—regardless of whether, upon their return, they seek to engage in speech. Neither the basis for the barment sanction (the prior trespass) nor its purpose (preventing future trespasses) has anything to do with the First Amendment. Punishing its violation by a person who wishes to engage in free speech no more implicates the First Amendment than would the punishment of a person who has (pursuant to lawful regulation) been banned from a public park after vandalizing it, and who ignores the ban in order to take part in a political demonstration. Here, as there, it is Hicks' nonexpressive conduct—his entry in violation of the notice-barment rule—not his speech, for which he is punished as a trespasser.

Virginia v. Hicks, 539 U.S. 113, 123 (2003).

Indeed, were it otherwise, *every* governmental action with a potential downstream effect on First Amendment activity would become subject to challenge—*e.g.*, an author who is prohibited from breaking into a printing press for purposes of publishing his book, or a reporter who is prohibited from breaking into private places for purposes of news-gathering. The Supreme Court, however, has rejected such claims. *See Cohen v. Cowles Media Co.*, 501 U.S. 663, 669 (1991) (“The press may not with impunity break and enter an office or dwelling to gather news.”); *Arcara*, 478 U.S. at 706 (noting that “every civil and criminal remedy imposes some conceivable burden on First Amendment protected activities,” but “no one would suggest that such liability gives rise to a valid First Amendment claim”). Consistent with these decisions, Plaintiffs' desire to access websites for which they lack authorization is not expressive activity.

Second, the factual record compiled during discovery likewise confirms that Plaintiffs' conduct is not expressive activity protected by the First Amendment. Plaintiffs' purported

speech—creating fake and/or misleading accounts—is specifically intended *not* to have any expressive or communicative content. As Plaintiffs acknowledge, they take efforts to *prevent* their fake accounts from being observed by others. *See* D-SMF ¶¶ 61-64. Indeed, as Plaintiff Wilson testified, the goal in creating the fake accounts is to have them be the proverbial “tree [that] falls in the woods and no one is around.” Wilson Depo. Tr. at 92-93.

Given that Plaintiffs affirmatively desire *not* to have their fake accounts viewed by others, Plaintiffs are not engaging in speech or other expressive activity. *See U.S. Telecom Ass’n v. FCC*, 825 F.3d 674, 741 (D.C. Cir. 2016) (“The Supreme Court has explained that the First Amendment comes ‘into play’ only where particular conduct possesses sufficient communicative elements, that is, when an intent to convey a particularized message is present, and in the surrounding circumstances the likelihood is great that the message would be understood by those who viewed it.” (modifications and citations omitted)). Thus, no First Amendment scrutiny is warranted because the “activity carried on in this case manifests absolutely no element of protected expression.” *Arcara*, 478 U.S. at 705.

C. At Most, Intermediate Scrutiny Would Apply

If the Court rejects the above argument, the appropriate result would be to analyze the Access Provision under intermediate scrutiny. The Government believes that, at most, the Access Provision regulates conduct with only “incidental limitations on First Amendment freedoms,” *United States v. O’Brien*, 391 U.S. 367, 376 (1968), and therefore the four-factor *O’Brien* test would be the correct standard. As the Court recognized in its motion-to-dismiss opinion, however, there is “little, if any, differen[ce]” between the *O’Brien* standard and the standard applied to time, place, or manner restrictions. MTD Op. at 36 n.14. Accordingly, the precise form of intermediate scrutiny is not critical. The important point is that, to the extent this Court applies any First Amendment scrutiny to the Access Provision, at most it should apply intermediate scrutiny.

IV. THE ACCESS PROVISION AMPLY SATISFIES INTERMEDIATE SCRUTINY

“In order to survive intermediate scrutiny, a law must be narrowly tailored to serve a significant governmental interest. In other words, the law must not burden substantially more speech than is necessary to further the government’s legitimate interests.” *Packingham*, 137 S. Ct. at 1736 (citation omitted). Importantly, however, “[t]he narrow tailoring requirement is not a ‘least intrusive’ or ‘least restrictive’ means test.” *ANSWER Coal.*, 845 F.3d at 1215. “Rather, the requirement of narrow tailoring is satisfied so long as the regulation promotes a substantial government interest that would be achieved less effectively absent the regulation.” *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989) (modifications omitted); *see also Am. Library Ass’n v. Reno*, 33 F.3d 78, 88 (D.C. Cir. 1994).

Here, the Access Provision amply satisfies intermediate scrutiny, including with respect to Plaintiffs’ purported conduct. First, the Access Provision seeks to further numerous important government interests. Second, enforcement of the Access Provision directly furthers those interests, including when enforced against Plaintiffs’ particular conduct. Third, the Access Provision leaves open ample alternative modes of communication. Thus, it satisfies narrow tailoring, and there is no basis for invalidating the provision under intermediate scrutiny.

A. Important Government Interests Are Furthered By the Access Provision

As the Court acknowledged previously, the CFAA’s legislative history establishes several important government interests furthered by the statute. *See* MTD Op. at 36-37 (the CFAA was enacted to “prevent the digital equivalent of theft” and “prohibit the digital equivalent of trespassing”); Pls.’ Br. at 16. The factual record compiled in discovery elaborates on those interests further, and reveals several additional government interests implicated by the Access Provision.

In general, the Government’s enforcement of the Access Provision “protects the freedom of private parties to decide how to design their platforms, to exclude unauthorized users from their

systems, and to prohibit the creation of fake accounts on their network.” Def.’s Suppl. Resps. to Pls.’ Interrog. Nos. 6, 7 (Def.’s Exh. 18) at 3. In the specific context here—enforcing the Access Provision when private websites or platforms have chosen to impose access restrictions on fake or misleading accounts—enforcement of the Access Provision supports several important governmental interests: (1) promoting private property rights; (2) preventing economic harm; (3) deterring fraud and other related criminal conduct; (4) protecting third-party users; (5) protecting the integrity of data, websites, and platforms; and (6) protecting the public and national interests, particularly based on misinformation. These governmental interests are explained at length in Defendant’s discovery responses. *Id.* at 3-4; *see also* D-SMF ¶¶ 65-72.

This Court has previously determined that such interests are “significant.” MTD Op. at 37. Other courts have likewise held as much. *See, e.g., Kaiser Aetna v. United States*, 444 U.S. 164, 179-80 (1979) (holding that “the right to exclude” is “universally held to be a fundamental element of the property right”); *Nat’l Org. for Women*, 37 F.3d at 655 (holding that “protecting . . . property rights” is “a significant governmental interest”); *Edwards v. Dist. of Colum.*, 755 F.3d 996, 1002 (D.C. Cir. 2014) (“Undoubtedly, promoting a major industry that contributes to the economic vitality of the District is a substantial government interest.”); *San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm. (USOC)*, 483 U.S. 522, 537 (1987) (Congress could legitimately give the USOC exclusive use of the word Olympic “to ensure that the USOC receives the benefit of its own efforts so that the USOC will have an incentive to continue to produce a quality product”); *Virginia State Bd. of Pharmacy*, 425 U.S. at 771-72 (the First Amendment does not prohibit states from protecting individuals from fraud); *Alvarez*, 567 U.S. at 734-36 (Breyer, J., concurring in judgment) (states may legitimately outlaw false statements that cause harm).

Indeed, Plaintiffs do not dispute the importance of these Government interests generally,

see Pls.’ Br. at 16, and have affirmatively conceded the importance of some. *See, e.g.*, Wilson Depo. Tr. at 69-70 (agreeing that political misinformation is harmful); D-SMF ¶¶ 91, 97, 100, 103-06. Accordingly, there is no dispute that the Access Provision, at least as a general matter, furthers significant Government interests.

B. The Access Provision Directly Advances Important Government Interests, Including As Applied to Plaintiffs’ Conduct

Rather than dispute the importance of the Government’s interests, Plaintiffs instead assert that “the government cannot demonstrate that its enumerated interests are substantial with respect to *specifically preventing* false speech in the course of civil rights testing and research.” Pls.’ Br. at 16. For several reasons, however, Plaintiffs’ argument is meritless. First, even in an as-applied challenge, the First Amendment analysis is not limited solely to Plaintiffs’ conduct. The Access Provision is properly justified with respect to the full range of governmental interests. Second, even when examining Plaintiffs’ particular conduct, enforcing the Access Provision does, in fact, further the important governmental interests discussed above. Third, the premise of Plaintiffs’ argument—that their conduct would cause only *de minimis* harm—is incorrect, and therefore Plaintiffs’ claim is unsupported even under their own First Amendment analysis.

1. Plaintiffs Misconceive the Appropriate Inquiry by Focusing Solely on Their Conduct

Plaintiffs contend that even if the Access Provision generally advances legitimate government interests, those interests would not be furthered if the Access Provision were applied to their civil rights-related false speech. *See* Pls.’ Br. at 16-19. Even if that were true, however, the argument is flawed both legally and factually. As a legal matter, the correct inquiry is broader than just Plaintiffs’ particular conduct. And factually, Plaintiffs’ argument is unworkable because it is not possible to identify *ex ante* which fake accounts are being used for academic research-related purposes and which are being used for more harmful purposes.

First, as a legal matter, even in an as-applied challenge a neutral regulation is not invalid “merely because a party contends that allowing an exception in the particular case will not threaten important government interests.” *United States v. Albertini*, 472 U.S. 675, 688 (1985). Instead, such regulations “must be evaluated in terms of their general effect.” *Id.* at 689; *see also Clark v. Cmty. For Creative Non-Violence*, 468 U.S. 288, 296-97 (1984) (“[I]t is evident from our cases that the validity of this regulation need not be judged solely by reference to the demonstration at hand.”); *Members of City Council of City of Los Angeles v. Taxpayers for Vincent*, 466 U.S. 789, 815-16 (1984); *Heffron v. Int’l Soc. for Krishna Consciousness, Inc.*, 452 U.S. 640, 652 (1981); *Mahoney v. Dist. of Colum.*, 662 F. Supp. 2d 74, 91 (D.D.C. 2009), *aff’d sub nom. Mahoney v. Doe*, 642 F.3d 1112 (D.C. Cir. 2011); *cf. Edwards*, 755 F.3d at 1001 (noting that “[t]he substantive rule of law is the same for both” facial and as-applied challenges, and the difference simply “goes to the breadth of the remedy employed by the Court”).

Indeed, the analysis must proceed in a general manner because otherwise the Court would itself be engaging in content-based (and potentially viewpoint-based) discrimination, contrary to First Amendment values. For example, granting an exception to Plaintiffs allowing them to create fake accounts for purposes of their civil rights research, but *denying* an exception to someone seeking to create a fake account for purposes of political speech, would undoubtedly be content-based discrimination. Under Plaintiffs’ approach, then, essentially every as-applied claim would require the regulation to satisfy strict scrutiny. *See Reed*, 135 S. Ct. at 2226-27 (content-based restrictions are subject to strict scrutiny).

Moreover, courts would have to engage in exactly the type of “ad hoc balancing of relative social costs and benefits” that the Supreme Court has rejected. *Stevens*, 559 U.S. at 470. For that reason alone, the Supreme Court has made clear that as-applied claims should be evaluated

according to the full range of conduct that a judicially crafted exception would allow. *See, e.g., Heffron*, 452 U.S. at 653-54 (holding that a regulation survives intermediate scrutiny notwithstanding that granting an exception to one religious group would have only an “incidental effect,” because if the challenged restriction were invalid as to that group, “it is no more valid with respect to the other social, political, or charitable organizations that” seek to engage in the same conduct); *Taxpayers for Vincent*, 466 U.S. at 816 (“To create an exception for appellees’ political speech and not these other types of speech might create a risk of engaging in constitutionally forbidden content discrimination.”).

Here, then, Plaintiffs’ claim cannot proceed solely with respect to their false speech. Granting an exception to that speech would likely require granting exceptions to numerous other types of speech—*e.g.*, fake accounts engaging in political speech, fake accounts seeking to promote particular products, fake accounts used to develop relationships with others under false pretenses, fake accounts that distort real users’ experiences on a platform, etc. All of these interests are properly considered in an as-applied challenge, therefore, and Plaintiffs do not argue that the Access Provision fails intermediate scrutiny based on this full range of interests.

Second, even if Plaintiffs were correct about the law, their approach would still be factually unworkable. Specifically, Plaintiffs’ theory would require that, before the Government or a private platform takes action against a fake account, the Government and/or platform would need to know whether the fake account was being used for socially beneficial purposes (like civil rights-related research) or for harmful purposes, because otherwise the Government or platform would risk violating the user’s First Amendment rights if the account were a socially beneficial one. But Plaintiffs adduced absolutely no evidence that either the Government or private platforms are capable of making such distinctions, and in fact the record here indicates the opposite, particularly

given the volume of fake accounts that private websites already face. *See* D-SMF ¶¶ 73-80. Accordingly, even if it were legally appropriate to narrow the inquiry here only to Plaintiffs' conduct, as a *factual* matter such an approach would be inappropriate; the Access Provision does not fail narrow tailoring if it is factually impossible to apply it in a narrower way.

2. Applying the Access Provision to Plaintiffs' Conduct Would, In Fact, Further Important Government Interests

Even limiting the inquiry solely to Plaintiffs' conduct, application of the Access Provision still furthers the significant governmental interests discussed above. Plaintiffs' argument to the contrary is based on a distortion of the record compiled in discovery, particularly about the meaning of various DOJ statements. Indeed, the record makes clear that all of the Government's interests are implicated, either directly or indirectly, by Plaintiffs' conduct.

a. The Record Confirms that All of the Government's Interests are Implicated by Plaintiffs' Conduct

Plaintiffs assert that “[t]he government admits that its interests in the Access Provision are not implicated by every violation of a website term of service prohibiting providing false information, because some such ToS violations would be trivial.” Pls.' Br. at 17 (citing P-SMF ¶ 24). That is incorrect. During discovery, the Government specifically explained that all of the Government's interests are furthered by application of the Access Provision to Plaintiffs' conduct: “All of the above interests are implicated by Defendant's ability to enforce the CFAA with respect to violations of ToS prohibiting the creation of false accounts, including when those false accounts are created as part of academic research intended to test for potential discrimination by a website or platform.” Def.'s Suppl. Resp. to Interrogs. Nos. 6, 7 (Def.'s Exh. 18) at 5; *see also* D-SMF ¶¶ 82-86. Thus, Plaintiffs can hardly claim that DOJ has admitted that its interests are *not*

implicated by Plaintiffs' conduct.⁷

Indeed, the applicability of several governmental interests to Plaintiffs' conduct is "self-evident." *ANSWER Coal. v. Dist. of Colum.*, 846 F.3d 391, 408 (D.C. Cir. 2017). For example, the protection of private property: because the Access Provision is limited only to persons who "intentionally accesses a computer without authorization or exceeds authorized access," 18 U.S.C. § 1030(a)(2)(C), then by definition such persons have transgressed the website owner's right to exclude them. *See also* D-SMF ¶¶ 87-88. And because the Access Provision necessarily applies only when private property rights have been transgressed, it is narrowly tailored to that purpose. *Cf. Taxpayers for Vincent*, 466 U.S. at 810 (because "the substantive evil—visual blight—is not merely a possible by-product of the activity, but is created by the medium of expression itself," then "application of the ordinance in this case responds precisely to the substantive problem which legitimately concerns the City" and "curtails no more speech than is necessary to accomplish its purpose").

Similarly, the purposes of preventing economic harm, protecting third-party users, and preserving the integrity of websites would clearly "be achieved less effectively absent the [Access Provision]," *Ward*, 491 U.S. at 799, even if the fake or misleading accounts are created for research-related purposes. In his deposition, Plaintiff Mislove agreed that the presence of fake users and fake job postings "would have a potential negative impact on the employment platform."

⁷ The only citation offered by Plaintiffs for this assertion is pages 45-46 of the Lynch deposition transcript. *See* P-SMF ¶ 24. But that testimony was discussing how some violations of websites' ToS are "trivial" in the sense that the ToS are not even genuine access restrictions sufficient to invoke the CFAA. *See* note 3, *supra*; *see also* Lynch Depo. Tr. at 45-46 (explaining that "[r]elatively trivial violations might include nonaccess restrictions" and "the question specifically with regard to false information is going to depend on the . . . terms of use of a particular Web site"). Thus, it does not "admit" that some applications of the Access Provision do not further the Government's interests.

Mislove Depo. Tr. at 108. And the record submitted by third-party companies confirms as much. For example, if Plaintiffs had a First Amendment right to create fake accounts on Monster.com, that would affect Monster.com's ability to charge its paying customers for each account view, and the presence of fake accounts would affect Monster.com's reputation:

Monster cannot knowingly permit users to create fictitious or false accounts and then turn around and charge employers for viewing such fictitious or false resumes. In addition, employers would be frustrated and increasingly dissatisfied with Monster if they spend time reviewing resumes and attempting to contact potential job candidates only to find out they were fictitious or false.

Kardon Affirmation (Def.'s Exh. 14) ¶ 2; *see also* Rockwell Decl. (Def.'s Exh. 11) at ¶ 8 (“Fake profiles are the root and starting point for many types of abuse on LinkedIn. They harm LinkedIn’s business, brand, customers, and members.”); Gleicher Decl. (Def.'s Exh. 12) at ¶ 10 (“[W]e have observed that the presence of fake accounts can create a feeling of unease and wariness when using Facebook and also lead to annoying spam-like or misleading content, unwanted friend requests, and unwanted messages.”); D-SMF ¶¶ 88-91.

The example of Glassdoor.com is particularly striking because, in order for a user to access content on that website beyond a trial period, Glassdoor requires the user to “submit[] a company review or take[] other action beneficial to Glassdoor[.]” O’Brien Decl. (Def.'s Exh. 13) ¶ 8. This policy “has been a central component of Glassdoor’s strategy to strengthening and maintaining the continued vitality of glassdoor.com.” *Id.* ¶ 9. If Plaintiffs had a First Amendment right to create fake accounts and provide false information, however, that would necessarily undermine the Glassdoor platform by introducing incorrect data and/or reviews—thereby also harming real users who rely on Glassdoor for accurate information, as well as the companies that have been reviewed dishonestly. *See id.* ¶ 16 (“Fake accounts, or creating accounts under false or fraudulent pretenses, impact the authenticity of glassdoor.com because they can skew certain statistics and metrics, such as average salary calculations, and may contribute fake content such as untrustworthy reviews

about employers that might mislead Glassdoor users.”). Plaintiffs’ claimed First Amendment right, therefore, would effectively preclude Glassdoor from operating an accurate, trustworthy platform as currently designed. *See id.* at ¶ 21; *see also* D-SMF ¶¶ 92-95.

Notably, the above harms will occur to private companies regardless of the purpose for which the fake accounts are created, *i.e.*, regardless of whether they are created for academic research or any other purpose. *See* D-SMF ¶¶ 88-98. Moreover, although significant evidence of these harms is present here, *see id.*, no evidence is required for the obvious proposition that private companies’ brands may be harmed if they cannot prevent the proliferation of fake users and postings. *See ANSWER Coal.*, 846 F.3d at 408 (evidentiary proof not required if justification “is utterly plausible and not novel”); *cf. San Francisco Arts & Athletics, Inc.*, 483 U.S. at 539 (upholding prohibition on unauthorized use of the word “Olympic” because Congress could reasonably “determine that unauthorized uses, even if not confusing, nevertheless may harm the USOC by lessening the distinctiveness and thus the commercial value” of the word).

Finally, enforcement of the Access Provision against Plaintiffs’ conduct also furthers several other government interests, at least indirectly. If academic researchers were granted an exception to prosecution, it would become harder for the Government to enforce the Access Provision against people who engage in harmful conduct but call themselves “researchers,” as well as against non-researchers who are (allegedly) engaging in similar First Amendment activity—*e.g.*, “an individual who creates fake accounts for the purpose of manipulating trends on websites in order to promote a particular viewpoint or product over different ones; or an individual creating fake accounts as part of the initial steps of a scheme to defraud, or a plan to recruit children for harmful purposes.” D-SMF ¶ 85; *see also id.* ¶¶ 81-84. Indeed, absent a clear definition of “research,” such an exception could threaten to swallow the rule, thereby undermining all of the

Government’s interests. *Cf. Taxpayers for Vincent*, 466 U.S. at 816 (“[T]he volume of permissible postings under such a mandated exemption might so limit the ordinance’s effect as to defeat its aim of combating visual blight.”).

These harms concerning fake accounts are far from hypothetical. Online companies are routinely required to disable fictitious accounts, including fictitious accounts used by bad actors as a means for engaging in directly harmful conduct—such as fraud, harassment, recruitment of children for harmful purposes, phishing, astroturfing (masking the true sponsor of a message), and spreading or promoting misinformation (including on matters of national interest). *See* D-SMF ¶¶ 99; *see also, e.g.,* Rockwell Decl. (Exh. 11) ¶ 7 (“Like other social media websites, LinkedIn is the target of bad actors who constantly try to create fake accounts. Indeed, on average, LinkedIn blocks millions of attempts to create fake accounts and shuts down hundreds of thousands of fake accounts each quarter.”); *id.* ¶ 12 (discussing how “[f]ake profiles are often the starting point for other types of abuse on LinkedIn”); Gleicher Decl. (Exh. 12) ¶¶ 16-18 (Facebook “take[s] action against millions of attempts to create fake accounts every day,” including against “bad actors who have engaged in improper and abusive conduct in the United States and elsewhere around the world using fake accounts”). In fact, Plaintiffs themselves have previously studied the types of abusive conduct that fake accounts can perpetrate. *See* D-SMF ¶¶ 103-06. And Plaintiffs do not dispute that removing fake accounts helps prevent these harms from occurring, and that the Government has a legitimate interest in removing fake accounts before these schemes come to fruition or a person is actually defrauded. *See id.* ¶¶ 101-02.

In short, the factual record here establishes numerous governmental interests promoted by the Access Provision’s enforcement, including as applied to Plaintiffs’ conduct.

b. Plaintiffs Mischaracterize the Meaning of Past DOJ Statements

Plaintiffs’ motion does not engage with any of the Government interests established in the

discovery record; instead, Plaintiffs rely on past DOJ statements such as legislative testimony. *See* Pls.’ Br. at 16-18. As an initial matter, it is not clear that past Executive Branch statements are even capable of narrowing the full range of governmental interests underlying a validly enacted statute. In any event, DOJ’s statements here do not undermine the Access Provision’s interests.

First, Plaintiffs point to statements about DOJ having “no interest in prosecuting harmless terms of service violations under the Access Provision.” Pls.’ Br. at 17. Those statements, however, are about DOJ’s *prosecutorial* decisions—not about the interests underlying the *statute*. DOJ choosing to prioritize its limited resources, *see* Lynch Depo Tr. at 43, does not establish that no valid government interests exist in the conduct remaining illegal—otherwise every exercise of prosecutorial discretion would be conceding an as-applied First Amendment claim for that conduct. Just as criminal prosecutions for trespass do not result literally every time someone commits a physical trespass, the same is true under the Access Provision. But a lack of intent to prosecute certain cases does not create a constitutional right to engage in that conduct.

Second, Plaintiffs rely on past DOJ legislative proposals that would narrow liability under the Access Provision. *See* Pls.’ Br. at 18-19. But Plaintiffs ignore the context for those proposals—they were part of a compromise package proposed by DOJ, whereby the Access Provision would be broadened in one respect (expressly allowing the prosecution of insiders) while narrowing it in another respect (requiring the information obtained to be valued at more than \$5,000). *See* D-SMF ¶ 108. As Mr. Lynch explained, those two amendments “should not be looked at as individuated” because “the Department has not proposed one without the other.” Lynch Depo Tr. at 57-58.

Thus, DOJ’s legislative proposals do not reflect that the Government has no interest in prohibiting Plaintiffs’ conduct under the Access Provision as currently drafted. Instead, the discovery record confirms that the Government has substantial interests in enforcing the Access

Provision, including as to Plaintiffs' conduct.

3. Plaintiffs' Conduct Goes Beyond *De Minimis* Harm

Finally, all of Plaintiffs' First Amendment analysis proceeds from the assumption that their speech "will cause no harm or, at most, *de minimis* harm to a target website's operations." Pls.' Br. at 1. But that premise is wrong. Thus, their claim is not supported even by their own analysis.

As an initial matter, Plaintiffs fail to address a key issue—what exactly they believe constitutes *de minimis* harm. Plaintiffs' depositions, however, revealed that their definition of *de minimis* harm is actually quite broad. See D-SMF ¶¶ 109-11. For example, when discussing the conduct at issue in the *Lowson* prosecution, both Plaintiff Wilson and Plaintiff Mislove rejected the idea that Ticketmaster suffered more than *de minimis* harm in those circumstances—even though individuals circumvented Ticketmaster's code-based restrictions in order to purchase more tickets than they otherwise would have been permitted, in contravention of Ticketmaster's negotiated right to be the exclusive distributor of tickets for those events. See D-SMF ¶¶ 109; see also *id.* ¶ 110 (Plaintiff Wilson believes that displacing users in search results is not "a substantive harm"); *id.* ¶ 111 (Plaintiff Mislove believes that some cyber attacks where a person "creates many fake accounts with the intention of obtaining more privileges than they would otherwise get" may pose only *de minimis* harm). Even if Plaintiffs' research poses only *de minimis* harms in their view, therefore, that does not mean their research would objectively cause only *de minimis* harm.

Moreover, Plaintiffs are not properly situated to evaluate whether their conduct is harmful or not. Although Plaintiffs are computer science professionals who understand the technical side of their research design, they have no basis for determining whether their research is harmful to the companies themselves (outside of certain technical concepts like burden on the companies' servers, storage space, etc.). See D-SMF ¶¶ 112-15. For example, Plaintiffs have no business experience with employment platforms and no basis for determining how or whether their conduct

might harm those businesses' profitability and other internal operations. *See id.* ¶¶ 112-15. Accordingly, Plaintiffs' predictions about a lack of harm to third-party users and companies are inadmissible for lack of foundation, and thus should not be considered even at the summary-judgment stage. *See* Fed. R. Civ. P. 56(e); *Williams v. Dodaro*, 576 F. Supp. 2d 72, 78 n.2 (D.D.C. 2008) (Bates, J.) (disregarding affidavit for failure to comply with Rule 56(e)).

In any event, for the reasons explained above, Plaintiffs' conduct goes beyond mere *de minimis* harm. Among other things, Plaintiffs' research transgresses the private websites' property rights, negatively affects real users of the websites, and undermines the private websites' integrity and potential profitability by diluting them with fake accounts. *See* D-SMF ¶¶ 65-72. A more specific analysis is not possible given that Plaintiffs have not yet finalized any intended research plans. *See* Parts I.B-C, *supra*. For present purposes, however, it suffices to note that, at a minimum, Plaintiffs' research will result in at least these material harms. Nor are these harms speculative, as confirmed by the third-party companies themselves. *See* D-SMF ¶¶ 82-102.

Finally, Plaintiffs try to minimize the harms caused by their conduct by analogizing their research to offline "testing" used to uncover discrimination. *See* Pls.' Br. at 20-21. In those situations, however, there is no generally applicable law that prohibits the activity. Here, there is such a law—*i.e.*, prohibiting unauthorized access to websites and platforms. Whatever the correct policy judgment about whether online "testing" of websites should be permissible, that judgment is for Congress to make. And the fact that "testing" activities are permitted in some circumstances does not create a First Amendment right to engage in such activities in different circumstances, in contravention of a generally applicable prohibition. *See Hudgens*, 424 U.S. at 513 ("[W]hile statutory or common law may in some situations extend protection or provide redress against a private corporation or person who seeks to abridge the free expression of others, no such protection

or redress is provided by the Constitution itself.”); *see also Cohen*, 501 U.S. at 669 (“[G]enerally applicable laws do not offend the First Amendment simply because their enforcement against the press has incidental effects on its ability to gather and report the news.”).

In short, Plaintiffs’ conduct goes beyond *de minimis* harms, and therefore is not supported even by their own legal analysis. Additionally, such harms confirm that the Access Provision is narrowly tailored to advancing important governmental interests, even when applied to Plaintiffs’ conduct. *Cf. Clark*, 468 U.S. at 297 (“[I]f the parks would be more exposed to harm without the sleeping prohibition than with it, the ban is safe from invalidation under the First Amendment[.]”).

C. The Access Provision Leaves Open Ample Alternatives for Plaintiffs’ Conduct

Finally, the Access Provision is lawful because it preserves ample alternative methods for Plaintiffs to pursue their research. *See Lloyd Corp.*, 407 U.S. at 567 (“It would be an unwarranted infringement of property rights to require them to yield to the exercise of First Amendment rights under circumstances where adequate alternative avenues of communication exist.”). Indeed, Plaintiffs’ motion fails to present any meaningful argument on this issue. *See* Pls.’ Br. at 15-22. The record here confirms that adequate alternatives exist for at least four reasons.

First, performing the type of “algorithm audits” that Plaintiffs undertake does not necessarily require creating fake or misleading accounts. Plaintiffs have performed algorithm audits in the past, and only one part of one paper actually involved the creation of fictitious accounts. *See* D-SMF ¶¶ 3-4, 116. Thus, Plaintiffs remain free to pursue research into online discrimination that does not require the creation of fake or misleading accounts.

Second, Plaintiffs are free to pursue algorithm audits, even those requiring fake or misleading accounts, on any website that does not condition access on the provision of truthful information. *See* D-SMF ¶ 117. Plaintiffs rely on the fact that three employment websites have ToS “prohibiting creating accounts using false information and/or providing false or misleading

information[.]” P-SMF ¶ 3. But that does not establish that those ToS are genuine access restrictions, *see* note 3, *supra*, nor does it establish that *all* employment websites have such access restrictions. Thus, the Access Provision would not prohibit Plaintiffs from performing algorithm audits on websites lacking such access restrictions.

Third, even with respect to algorithm audits requiring the creation of user accounts, nothing prevents Plaintiffs from relying on *real* individuals with the necessary characteristics to perform such an audit. *See* D-SMF ¶¶ 118. In this respect, Plaintiffs’ analogy to in-person housing testing is instructive, as such testing may involve real-world individuals with approximately the same characteristics except for the protected class being “tested.” *See* P-SMF ¶ 28. If the use of real-world individuals is adequate for some in-person housing testing, Plaintiffs have not demonstrated why it is inadequate for purposes of their activities. *See* D-SMF ¶¶ 118-22.⁸

Fourth and finally, even if Plaintiffs genuinely needed to use fictitious user accounts and the relevant websites had genuine access restrictions on such accounts, Plaintiffs could still ask the websites for consent to perform their audit. Although Plaintiffs contend that seeking advance permission “would affect the scientific validity of such research,” P-SMF ¶ 88, their depositions revealed that there are at least some circumstances in which requesting advance permission would not necessarily affect the validity. *See* D-SMF ¶¶ 125-26. Indeed, requesting advance permission would not necessarily provide any greater “notice” to the websites of Plaintiffs’ intent to audit beyond what Plaintiffs have already said publicly. *See id.* ¶¶ 127-32. Moreover, Plaintiffs conceded that it would be “pure speculation” on their part as to whether companies would refuse

⁸ Using fictitious accounts may make conducting such an algorithm audit easier than going out and finding real individuals with the necessary characteristics. However, even if Plaintiffs’ preferred conduct has “admitted advantages,” that does not mean that the alternative methods are inadequate. *ANSWER Coal.*, 846 F.3d at 409.

to permit such audits, *see id.* ¶ 134, and the record here reflects that at least some companies would be willing to consider such a request. *See id.* ¶ 135. Thus, there are ample alternative methods available for Plaintiffs to perform their potential research—thereby further confirming that the Access Provision is narrowly tailored even as to Plaintiffs’ contemplated conduct.

* * * *

In sum, even if this Court concludes that the Access Provision is subject to First Amendment scrutiny, the statute easily survives intermediate scrutiny. Plaintiffs do not seriously dispute that significant governmental interests are furthered by enforcement of the Access Provision generally. And even if the First Amendment analysis were limited solely to Plaintiffs’ conduct, enforcement of the Access Provision would still serve important governmental interests—*e.g.*, the protection of private property, preventing economic harm, and protecting third-party users of websites. Indeed, because Plaintiffs’ conduct directly implicates those interests, their conduct goes beyond mere *de minimis* harm. Moreover, the Access Provision still preserves ample alternative methods for Plaintiffs to pursue their research.

Accordingly, even assuming that Plaintiffs have standing to challenge the Access Provision, and even assuming that the Access Provision is subject to First Amendment scrutiny, Defendant is still entitled to summary judgment because the Access Provision is narrowly tailored and survives intermediate scrutiny.

CONCLUSION

For the foregoing reasons, the Court should dismiss Plaintiffs’ remaining claim for lack of subject-matter jurisdiction, or in the alternative enter summary judgment for Defendant.

Dated: April 15, 2019

Respectfully submitted,

JOSEPH H. HUNT
Assistant Attorney General

JOHN R. TYLER
Assistant Branch Director

/s/ Daniel Schwei
DANIEL SCHWEI (N.Y. Bar)
Senior Trial Counsel
United States Department of Justice
Civil Division, Federal Programs Branch
1100 L Street NW, Room 12024
Washington, DC 20530
Tel.: (202) 305-8693
Fax: (202) 616-8460
E-mail: daniel.s.schwei@usdoj.gov

Mailing Address:
Post Office Box 883
Washington, D.C. 20044

Courier Address:
1100 L Street NW, Room 12024
Washington, D.C. 20005

Counsel for Defendants