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

| | |
|---|---|
| CHRISTIAN W. SANDVIG *et al.*,<br><br>Plaintiffs,<br><br>v.<br><br>WILLIAM P. BARR, in his official capacity as Attorney General of the United States,<br><br>Defendant. | Case No. 1:16-cv-1368 (JDB) |

**PLAINTIFFS' RESPONSE TO DEFENDANT'S STATEMENT OF MATERIAL FACTS NOT IN DISPUTE**

Plaintiffs Alan Mislove and Christopher "Christo" Wilson file this Response to Defendant's Statement of Material Facts Not in Dispute in Support of Cross-Motion for Summary Judgment, ECF Nos. 50-2 and 51-1, pursuant to Fed. R. Civ. P. 56(c) and Local Rule 7(h). Plaintiffs do not concede that any of Defendant's statements of fact are material to the legal questions now before the Court.

## I. Plaintiffs' Past Research

1. Both Plaintiff Mislove and Plaintiff Wilson were authors of a paper seeking to study potential racial and gender bias on two prominent online freelance marketplaces, TaskRabbit and Fiverr. *See Bias in Online Freelance Marketplaces: Evidence from TaskRabbit and Fiverr* (Feb. 2017) (PID0020-0036) (attached as Exh. 1) [hereafter "CSCW 2017 Paper"].

**PL. RESPONSE:** Undisputed.

2. Plaintiff Wilson was an author of a paper seeking to study gender-based inequalities in the context of resume search engines, and whether employment websites were using

inferred gender of candidates as explicit features in their ranking algorithms. See Investigating the Impact of Gender on Rank in Resume Search Engines (Apr. 2018) (PID0001-0019) (attached hereto as Exh. 2) [hereafter "CHI 2018 Paper"].

**PL. RESPONSE:** Undisputed.

3. Both of these studies were "algorithm audits" regarding potential discrimination on the particular platforms studied. *See* Mislove Depo. Tr. (attached hereto as Exh. 3) at 33–34; Wilson Depo. Tr. (attached hereto as Exh. 4) at 24–27; *see also* CSCW 2017 Paper (Exh. 1) at PID0022; CHI 2018 Paper (Exh. 2) at PID0003.

**PL. RESPONSE:** Undisputed to the extent that "part of the [CSCW 2017] paper is an algorithmic audit of TaskRabbit and Fiverr." Mislove Depo. at 34 (Def. Ex. 3, ECF No. 53-3). Plaintiff Mislove distinguishes between "looking at sort of feedback that various workers are getting on the platform" through reviews, which "is not an algorithm that we are auditing" and "look[ing] at the search algorithm" which is an algorithm audit. *See id*. at 33; *see also* Wilson Depo. at 27 (Def. Ex. 4, ECF No. 53-4) (describing an algorithmic audit as "some kind of black box algorithmic system as your subject" where the auditor "probe[s] its behavior").

4. To perform these two algorithm audits, the CSCW 2017 paper did not require creating any fictitious accounts or providing misleading information, and only one part of the CHI 2018 paper (the "direct discrimination" phase) required creating fictitious accounts or providing misleading information. *See* Mislove Depo. Tr. (Exh. 3) at 34; Wilson Depo. Tr. (Exh.at 37–39; see also CHI 2018 Paper (Exh. 2) at PID0001-0002 (distinguishing between "indirect discrimination" and "direct discrimination" phases of the study).

**PL. RESPONSE:** Undisputed.

## II. Facts Pertaining to Plaintiffs' Standing

5. Neither Plaintiff Wilson nor Plaintiff Mislove is currently undertaking academic research involving the creation of fictitious user accounts and/or providing false information in violation of website or platforms' Terms of Service (ToS). See Pls.' Resps. to Def.'s Requests for Admissions (RFAs) (attached hereto as Exh. 5), RFA No. 4.

**PL. RESPONSE:** Undisputed.

6. Plaintiff Wilson has "no concrete plans for research involving providing false information in violation of websites' terms of service" or for "research involving the creation of fictitious user accounts." Wilson Depo Tr. (Exh. 4) at 62–63; *see also id.* at 66.

**PL. RESPONSE:** Disputed as an incomplete statement of Plaintiff Wilson's deposition testimony to the extent this is a characterization of Plaintiff Wilson's intent to conduct the "research plan" as described in his Declaration in Support of Plaintiffs' Motion for Summary Judgment. *See* Wilson Dec., ECF No. 48-1, at ¶¶ 11–51 (describing methodology of intended research and receipt of funding from National Science Foundation for proposed research plan).

Plaintiff Wilson's use of the word "concrete" in connection with research refers in part to whether specific target platforms will definitely be tested. Prior to the cited deposition testimony on pages 62, 63, and 66, Plaintiff Wilson contextualizes his use of the word "concrete" with respect to research, by noting with respect to certain research that it is in "preliminary phases" and therefore the target platforms are not "concretely identified." Wilson Depo. at 61 (Def. Ex. 4, ECF No. 53-4). Plaintiff Wilson further testifies, with respect to certain research, that he can identify "[s]ome, but not all," of the target platforms, *id*. at 61, and that he would say that he "intend[s] to access them in the future for purposes of conducting academic research regarding

potential online discrimination," *id*. at 62, and describes this as a situation where there are "not concrete plans," *id*. He also testified, "When I said I don't have concrete plans, what I meant was we don't have software, we don't have a timeframe. There is no students assigned to it. . . . It is not happening now. But I do plan to conducting it in the future." Wilson Depo. at 215–16 (Pl. Ex. 19). When asked, "[A]s of today, have you taken any concrete steps to undertake that research?" Plaintiff Wilson testified that "the most concrete step is that I applied and received [] funding, applied and received IRB for those designs. I would say that is pretty concrete. . . . [B]ut am I implementing it right now, no." *Id*. at 217 (Pl. Ex. 19). When asked, "Do you have concrete plans to implement it?" Plaintiff Wilson testified, "Yes. I fully intend to do that research." *Id*.

Plaintiff Wilson's testimony that he has "no concrete plans" for research involving providing false information in violation of websites' terms of service or for research involving the creation of fictitious user accounts is consistent with his intent to conduct the research plan described in his Declaration. With respect to the research plan, Plaintiff Wilson testified that "the platforms and/or websites in the employment or hiring industry change rapidly and the practicability of auditing them may also vary" such that all such websites cannot now be identified. *See* Wilson Dec., ECF No. 48-1, at ¶ 43; *see also* Pls. Third Suppl. Resps. to Def. First Interrogatories at 3 (Def. Ex. 6, ECF No. 53-6) (objecting that "Plaintiffs cannot identify in advance all . . . websites that they may wish to test" but identifying the names of certain websites and/or platforms that Plaintiffs intend to access in the future and noting that the "list is not exhaustive" and that "[t]he platforms and/or websites in the employment or hiring industry change rapidly, and the practicability of auditing them may also vary, such that Plaintiffs cannot now identify all such platforms and/or websites that they will access in the future for purposes of conducting academic research regarding potential online discrimination").

7. Plaintiff Mislove has no concrete plans for any future research into potential discrimination by online hiring websites or platforms involving the provision of false information and/or creation of fictitious user accounts in violation of those websites' or platforms' ToS. Mislove Depo Tr. (Exh. 3) at 46–47; *see also id.* at 110–11 (making clear that the research project discussed on page 46 is not within the scope of this lawsuit).

**PL. RESPONSE:** Disputed to the extent this is a characterization of Plaintiff Mislove's intent to conduct the "research plan" as described in his Declaration in Support of Plaintiffs' Motion for Summary Judgment. *See* Mislove Dec., ECF No. 48-2, at ¶¶ 11–48 (describing methodology of intended research).

Plaintiff Mislove's testimony that he has no concrete plans for certain future research does not mean that he does not have specific plans or an intent to conduct such research. On the same pages of the deposition testimony cited by Defendant, Plaintiff Mislove contextualizes his understanding of the word "concrete" with respect to research, by stating, "I do have specific research plans or specific platforms that we are studying, yes, and . . . this is an area of my research that [I] intend to conduct work[] in." The question immediately following this testimony asks whether, setting aside a specified research project, Plaintiff Mislove "ha[s] concrete plans for any of that other future research," to which Plaintiff Mislove answers "no." *See* Mislove Depo. at 46–47 (Def. Ex. 3, ECF No. 53-3).

Plaintiff Mislove's deposition testimony is consistent with his intent to conduct the research plan described in his Declaration. With respect to the research plan, Plaintiff Mislove testified that "the platforms and/or websites in the employment or hiring industry change rapidly and the practicability of auditing them may also vary" such that all such websites cannot now be identified. *See* Mislove Dec., ECF No. 48-2, at ¶ 40; *see also* Pls. Third Suppl. Resps. to Def.

First Interrogatories at 3 (Def. Ex. 6, ECF No. 53-6) (objecting that "Plaintiffs cannot identify in advance all . . . websites that they may wish to test" but identifying the names of certain websites and/or platforms that Plaintiffs intend to access in the future and noting that the "list is not exhaustive" and that "the platforms and/or websites in the employment or hiring industry change rapidly, and the practicability of auditing them may also vary, such that Plaintiffs cannot now identify all such platforms and/or websites that they will access in the future for purposes of conducting academic research regarding potential online discrimination").

8. Plaintiffs have violated 18 U.S.C. § 1030(a)(2)(C) in the past. See Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 2; see also Pls.' Resps. to Def.'s First Interrogs. (attached hereto as Exh. 6), Interrog. Nos. 3, 5 (discussing past ToS violations).

**PL. RESPONSE:** Disputed. Any past violations of 18 U.S.C. § 1030(a)(2)(C) for visiting a website in a manner that violates its terms of service or terms of use (collectively, "ToS") by Plaintiffs are to the best of their knowledge and belief about the relevant ToS at the time they visited a website, and any such violations cannot constitutionally provide grounds for criminal liability. Pls. Resps. To Def. First RFAs at 2 (Def. Ex. 5, ECF No. 53-5) (Response to RFA No. 2).

9. Plaintiffs have never been prosecuted for any violations of 18 U.S.C. § 1030(a)(2)(C). *See* Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 3.

**PL. RESPONSE:** Undisputed.

10. Plaintiffs have received no communication from the federal government expressing any possibility of prosecution based on past ToS violations, including ToS violations concerning the creation of false accounts or providing false information. *See* Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 1.

**PL. RESPONSE:** Undisputed.

11. Plaintiff Mislove "think[s] it is unlikely that [he] would [be] prosecuted for the research described in the complaint." Mislove Depo Tr. (Exh. 3) at 146–47.

**PL. RESPONSE:** Disputed as an incomplete statement of Plaintiff Mislove's deposition testimony to the extent Plaintiff Mislove's statement about the likelihood of prosecution is intended to characterize his fear of prosecution for the research described in the Complaint. In the same response as that cited by Defendant, Plaintiff Mislove testified that "you are essentially relying on prosecutorial discretion about whether or not to bring charges" and "while I don't think it is likely, it is something I think about and it does affect my sort of thinking on a lot of this" and that "it really weights heavily on my mind . . . am I exposing my students to criminal—to potential criminal prosecution or the risk." Mislove Depo. at 146–47 (Def. Ex. 3, ECF No. 53-3); *see also* Mislove Dec., ECF No. 48-2, at ¶¶ 49, 51.

12. Plaintiff Wilson filed this lawsuit "to do good in the world" and because he believes that "the idea that a terms of service violation by itself [is] somehow a criminal or civil offense" is not "compatible with the modern world." Wilson Depo Tr. (Exh. 4) at 147, 142.

**PL. RESPONSE:** Disputed as an incomplete statement of Plaintiff Wilson's deposition testimony and to the extent this is intended as a complete statement of Plaintiff Wilson's reasons for filing this lawsuit. Shortly after the exchange cited by Defendant, Plaintiff Wilson explained that he is proud of being a plaintiff in this lawsuit because he believes that it is "very important" to "bring[] clari[t]y to the work so that we can conduct it." Wilson Depo. at 152 (Pl. Ex. 19). Plaintiff Wilson is "concerned that violating terms of service in the course of [his] research plan

will subject [him] to criminal prosecution under . . . 18 U.S.C. § 1030(a)(2)(C).” Wilson Dec., ECF No. 48-1, at ¶ 52.

13. Plaintiffs cannot recall any specific instances in which concerns about liability under the Access Provision prompted them to forego an algorithm audit into potential discrimination by an online hiring website. *See* Mislove Depo. Tr. (Exh. 3) at 60–62; Wilson Depo. Tr. (Exh. 4) at 71–72.

**PL. RESPONSE:** Disputed as an incomplete statement of Plaintiff Mislove’s deposition testimony regarding whether he has ever decided not to pursue research into potential online discrimination because of concerns about liability under the Access Provision. In response to two questions, Plaintiff Mislove testified that he “can’t recall specific instances of that. But, it is likely that that happened” and that he “can’t recall specific instances right now. But . . . it is very likely that there are instances that happened.” Mislove Depo. at 60–61 (Def. Ex. 3, ECF No. 53-3).

14. On September 11, 2014, the Attorney General issued a directive to subordinates within the Department of Justice (DOJ) entitled Intake and Charging Policy for Computer Crime Matters [hereafter “Charging Policy”]. *See* ECF No. 15-1; Lynch Affidavit (ECF No. 21-1) ¶ 4.

**PL. RESPONSE:** Undisputed.

15. The Attorney General’s Charging Policy remains in effect today. See Lynch Affidavit (ECF No. 21-1) ¶ 4; Def.’s Resps. to Pls.’ First Interrogs. (attached hereto as Exh. 7), Interrog. No. 2; Lynch Depo. Tr. (attached hereto as Exh. 8) at 113; *see also* P-SMF ¶ 17.

**PL. RESPONSE:** Undisputed.

16. The Charging Policy was intended to ensure that DOJ attorneys are applying the Computer Fraud and Abuse Act (CFAA) in a manner that is consistent and serves the Department's priorities. *See* Lynch Affidavit (ECF No. 21-1) ¶ 4.

**PL. RESPONSE:** Undisputed.

17. The Charging Policy requires (among other things) that any CFAA prosecution serve a substantial federal interest. *See* Lynch Affidavit (ECF No. 21-1) ¶ 5.

**PL. RESPONSE:** Undisputed.

18. The Justice Manual includes a list of factors that DOJ attorneys should consider in assessing whether a "substantial federal interest" exists, including the "nature and seriousness of the offense." Justice Manual § 9-27.230, *available at* https://www.justice.gov/jm/jm-9-27000-principles-federal-prosecution#9-27.230; *see also* Def.'s Resps. to Pls.' First Interrogs. (Exh. 7), Interrog. No. 1; Lynch Affidavit (ECF No. 21-1) ¶ 5.

**PL. RESPONSE:** Undisputed.

19. The Justice Manual states that "[i]t is important that limited federal resources not be wasted in prosecuting inconsequential cases or cases in which the violation is only technical." Justice Manual § 9-27.230, cmt. ¶ 2.

**PL. RESPONSE:** Undisputed.

20. In addition to the factors set forth in the Justice Manual, the Charging Policy directs that DOJ attorneys considering CFAA charges should also consider several other factors, including how much harm the activity caused within the relevant District or community. *See* Charging Policy (ECF No. 15-1) at 2, 5; Lynch Affidavit (ECF No. 21-1) ¶¶ 5, 8.

**PL. RESPONSE:** Undisputed.

21. The Charging Policy directs 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." Charging Policy (ECF No. 15-1) at 5; Lynch Affidavit (ECF No. 21-1) ¶ 6.

**PL. RESPONSE:** Undisputed.

22. The Charging Policy also states that "federal prosecution may not be warranted if the information obtained is otherwise publicly available or has little value." Charging Policy (ECF No. 15-1) at 3; Lynch Affidavit (ECF No. 21-1) ¶ 7.

**PL. RESPONSE:** Undisputed.

23. Plaintiffs understand the Charging Policy to "suggest that federal prosecution may not be warranted in instances where someone has only breached a website's terms of service," which Plaintiffs believe "sounds good." Mislove Depo Tr. (Exh. 3) at 157–58; Wilson Depo Tr. (Exh. 4) at 160–61.

**PL. RESPONSE:** Disputed as an incomplete statement of Plaintiff Mislove's deposition testimony regarding his opinion on the Department of Justice's ("DOJ") Charging Policy. On the same page as the deposition testimony cited by Defendant, Plaintiff Mislove testified that "the guidelines are guidelines," "[t]hey say things along the lines of prosecution may not be warranted, but they do not prohibit prosecution," "they are internal DOJ guidelines . . . [t]hey are not the law," "the guidelines could be changed at any time," and "the risk [of prosecution] comes not from the guidelines but the risk comes from the law." Mislove Depo. at 158 (Def. Ex. 3, ECF No. 53-3).

Disputed as an incomplete statement of Plaintiff Wilson's deposition testimony regarding his opinion on the DOJ Charging Policy. On the same page as the deposition testimony cited by

Defendant, Plaintiff Wilson testified that "the memorandum can be changed at any time" and that it is "better than nothing but it doesn't do anything." Wilson Depo. at 161 (Def. Ex. 4, ECF No. 53-4).

24. DOJ is unaware of any federal criminal prosecution under the CFAA of conduct resembling the conduct described in Plaintiffs' complaint that resulted in similarly *de minimis* harm. Lynch Affidavit (ECF No. 21-1) ¶ 9; Lynch Depo. Tr. (Exh. 8) at 147–49.

**PL. RESPONSE:** Undisputed.

25. DOJ does not expect to bring a CFAA prosecution based on the conduct described in Plaintiffs' complaint and *de minimis* harm. Lynch Affidavit (ECF No. 21-1) ¶ 9; Lynch Depo. Tr. (Exh. 8) at 147–49, 152.

**PL. RESPONSE:** Undisputed.

26. Plaintiffs are unaware of any federal government criminal prosecutions against researchers conducting an algorithm audit. *See* Wilson Depo. Tr. (Exh. 4) at 153; Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 15.

**PL. RESPONSE:** Undisputed.

27. Plaintiffs are unaware of any cases where a company has pursued a civil CFAA claim against researchers conducting an algorithm audit. *See* Wilson Depo. Tr. (Exh. 4) at 153; Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 15.

**PL. RESPONSE:** Undisputed, to the extent that "cases where a company has pursued a civil CFAA claim against researchers conducting an algorithm audit" is understood to mean the filing of a lawsuit.

28. Plaintiffs are unaware of any charges brought under 18 U.S.C. § 1030(a)(2)(C), since

June 29, 2015, in which the theory of "access[ing] a computer without authorization or exceed[ing] authorized access" was based, in whole or in part, on violation of a publicly available website or platform's Terms of Service. *See* Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 5.

**PL. RESPONSE:** Undisputed.

29. Aside from *United States v. Lowson*, No. 2:10-cr-114 (D.N.J.), and *United States v. Drew*, No. 08-cr-582 (C.D. Cal.), Plaintiffs are unaware of any charges brought under 18 U.S.C. § 1030(a)(2)(C) in which the theory of "access[ing] a computer without authorization or exceed[ing] authorized access" was based, in whole or in part, on violation of a publicly available website or platform's Terms of Service. *See* Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 6.

**PL. RESPONSE:** Undisputed.

30. The *Lowson* prosecution involved conduct that caused material harm, because the defendants deprived companies like Ticketmaster of their negotiated right to be the exclusive distributor of tickets for certain events and the right to define the terms of sale for those tickets, and also because the defendants caused third-party customers to pay higher prices for the tickets on the secondary market. *See United States v. Lowson*, 2:10-cr-114 (D.N.J.), Superseding Indictment (ECF No. 28) ¶¶ 2(a)-(e), 33 (Apr. 20, 2010).

**PL. RESPONSE:** Disputed to the extent it calls for a legal conclusion regarding whether the relevant conduct "caused material harm" and, to the extent it seeks to characterize the conduct and facts at issue in *United States v. Lowson*, the case speaks for itself. *See* Pls. Resps. To Def. First RFAs at 3 (Def. Ex. 5, ECF No. 53-5) (Response to RFA No. 9).

31. The *Lowson* prosecution involved "access[ing] a computer without authorization or

exceed[ing] authorized access" not only through violation of Terms of Service, but also through circumvention of code-based access restrictions. *See* MTD Op. at 21; *see also United States v. Lowson*, 2:10-cr-114 (D.N.J.), Superseding Indictment (ECF No. 28) ¶¶ 2(l)–(q), (s) (Apr. 20, 2010).

**PL. RESPONSE:** Undisputed.

32. The *Drew* prosecution involved conduct that caused material harm, because the defendant harassed a 13-year-old girl who ultimately killed herself as a result of the harassment. *See United States v. Drew*, No. 08-cr-582 (C.D. Cal.), Indictment (ECF No. 1) ¶¶ 2, 15(a)–(d) (May 15, 2008).

**PL. RESPONSE:** Disputed to the extent it calls for a legal conclusion about whether the relevant conduct "caused material harm" and, to the extent it seeks to characterize the conduct and facts at issue in *United States v. Drew*, the case speaks for itself. *See* Pls. Resps. To Def. First RFAs at 3–4 (Def. Ex. 5, ECF No. 53-5) (Response to RFA No.10).

33. After implementation of the Attorney General's Charging Policy in 2014, the Computer Crime and Intellectual Property Section (CCIPS) of DOJ's Criminal Division has a reasonably comprehensive record of past CFAA prosecutions, including prosecutions that resulted in plea agreements. *See* Lynch Depo Tr. (Exh. 8) at 132–34; Suppl. Lynch Decl. (attached hereto as Exh. 9) ¶¶ 5–6.

**PL. RESPONSE:** Disputed to the extent that "reasonably comprehensive" is a self-serving statement of opinion by Defendant's representative regarding the completeness of DOJ's Criminal Division's records of past CFAA prosecutions since June 29, 2015, including prosecutions that resulted in plea agreements. John T. Lynch, Jr., the Chief of the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division, admits that

"reasonably comprehensive" does not mean "fully comprehensive" records of past CFAA prosecutions because there are "situations where consultations [with CCIPS] did not occur prior to charges being filed" and "there may be other situations [he is] not yet aware of." Suppl. Lynch Dec. at ¶¶ 5–6 (Def. Ex. 9, ECF No. 53-9).

34. Independent of CCIPS, the Executive Office of United States Attorneys (EOUSA) also maintains data regarding past CFAA prosecutions, including prosecutions that resulted in plea agreements. *See* Def.'s Resps. to Pls.' First Interrogs. (Exh. 7), Interrog. No. 4; Suppl. Lynch Decl. (Exh. 9) ¶¶ 7–9.

**PL. RESPONSE:** Undisputed.

35. EOUSA takes steps to ensure that its data is accurate and reliable, including requiring all USAO districts to prepare semi-annual certifications indicating that the information contained in the local databases has been reviewed and accurately reflects the status of pending matters, cases and appeals. *See* Suppl. Lynch Decl. (Exh. 9) ¶ 7.

**PL. RESPONSE:** Disputed as being a self-serving statement of opinion by Defendant's representative to the extent it asserts the truth of whether the Executive Office of United States' Attorneys' ("EOUSA") data regarding past CFAA prosecutions is in fact "accurate and reliable." Disputed as not being based on personal knowledge of the declarant, who testified that "[a]fter discussion with representatives of EOUSA, my understanding is that an important role of EOUSA is to maintain a centralized computer database" and whose testimony regarding the accuracy and reliability of the EOUSA database is based on such "discussion" and "understanding." *See* Suppl. Lynch Dec. at ¶¶ 7–9 (Def. Ex. 9, ECF No. 53-9).

36. In preparing DOJ's response to Plaintiffs' Interrogatory No. 4, DOJ reviewed not only CCIPS' information regarding past CFAA prosecutions, but also EOUSA's data

regarding past CFAA prosecutions. *See* Def.'s Resps. to Pls.' First Interrogs. (Exh. 7), Interrog. No. 4; Suppl. Lynch Decl. (Exh. 9) ¶ 8.

**PL. RESPONSE:** Undisputed.

37. In preparing DOJ's response to Plaintiffs' Interrogatory No. 4, although the Interrogatory was limited to prosecutions initiated by indictment, DOJ's review encompassed all CFAA prosecutions regardless of the type of charging instrument—and thus included CFAA prosecutions that resulted in plea agreements. *See* Lynch Depo. Tr. (Exh. 8) at 137–40; Suppl. Lynch Decl. (Exh. 9) ¶ 9.

**PL. RESPONSE:** Undisputed to the extent that "DOJ's review encompassed all CFAA prosecutions regardless of the type of charging instrument" is understood to mean all CFAA prosecutions of which DOJ (CCIPS and EOUSA) has a record.

38. Based on DOJ's review of CCIPS' records as well as EOUSA's data, DOJ has determined that no charges have been filed since June 29, 2015, under 18 U.S.C. § 1030(a)(2)(C)—whether by indictment, information, or complaint—in which 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* Def.'s Resps. to Pls.' First Interrogs. (Exh. 7), Interrog. No. 4; Lynch Depo. Tr. (Exh. 8) at 137–40; Suppl. Lynch Decl. (Exh. 9) ¶ 10.

**PL. RESPONSE:** Undisputed to the extent that, regarding relevant CFAA prosecutions, "DOJ has determined that no charges have been filed since June 29, 2015." Disputed regarding the truth of whether no such charges have been filed, in light of undisputed evidence that CCIPS' records might not be "fully comprehensive" and that "DOJ believes that it has reviewed the most

comprehensive records with respect to past charges" in coming to its determination regarding past charges. *See* Suppl. Lynch Dec. at ¶¶ 6, 8, 10 (Def. Ex. 9, ECF No. 53-9).

39. Based on that same review, DOJ has determined that, since at least June 29, 2015, 18 U.S.C. § 1030(a)(2)(C) has not been used to obtain plea agreements based on website or platform ToS violations (harmless or otherwise). Def.'s Resps. to Pls.' First Interrogs. (Exh. 7), Interrog. No. 4; Lynch Depo. Tr. (Exh. 8) at 137–40; Suppl. Lynch Decl. (Exh. 9) ¶ 10.

**PL. RESPONSE:** Undisputed to the extent that, regarding relevant CFAA plea agreements, "DOJ has determined that" no such plea agreements have been obtained since June 29, 2015. Disputed regarding the truth of whether no such plea agreements have been obtained, in light of undisputed evidence that CCIPS' records might not be "fully comprehensive" and that "DOJ believes that it has reviewed the most comprehensive records with respect to past charges" in coming to its determination regarding past plea agreements. *See* Suppl. Lynch Dec. at ¶¶ 6, 8, 10 (Def. Ex. 9, ECF No. 53-9).

40. DOJ has limited resources and therefore does not prioritize enforcement of the CFAA against conduct that does not cause significant harm. Lynch Depo. Tr. (Exh. 8) at 42–43; Justice Manual § 9-27.230; Charging Policy (ECF No. 15-1) at 5.

**PL. RESPONSE:** Undisputed.

41. DOJ has stated to Congress multiple times, across Administrations, that DOJ does not intend to use the CFAA to prosecute harmless violations of contractual restrictions. *See* Stmt. of Sujit Raman, Assoc. Deputy Att'y Gen., Before the Subcmte. On Crime & Terrorism, Sen. Judic. Cmte. (Aug. 21, 2018) (attached hereto as Exh. 10) at DOJ-00019 ("I would like to reiterate that the Department of Justice has no interest in

prosecuting harmless violations of use restrictions like these."); Stmt. of David Bitkower, Deputy Asst. Att'y Gen., Criminal Div., Before the Subcmte. On Crime & Terrorism, Sen. Judic. Cmte. (July 8, 2015) (ECF No. 10-3) at 6 ("The Department of Justice has no interest in prosecuting harmless violations of use restrictions like these.").

**PL. RESPONSE:** Undisputed to the extent that the evidence cited by Defendant reflects the following: DOJ has stated to Congress multiple times, across administrations, that DOJ "has no interest" in using the CFAA to prosecute harmless violations of contractual restrictions, as opposed to "DOJ does not intend" to so use the CFAA.

42. Plaintiffs cannot identify in advance all such websites that they may wish to test, nor what their terms of service may be on any future date. *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 2.

**PL. RESPONSE:** Undisputed.

43. Determining whether a particular ToS provision is a genuine access restriction depends on the type of website and the ToS of that particular website. *See* Lynch Depo. Tr. (Exh. 8) at 45–46.

**PL. RESPONSE:** Disputed because this is a legal conclusion regarding which terms of service violations constitute violations of 18 U.S.C. § 1030(a)(2)(C) (the "Access Provision").

44. Different websites have different tolerances for false information. *See* Lynch Depo. Tr. (Exh. 8) at 47–49.

**PL. RESPONSE:** Undisputed to the extent websites' differing "tolerance" for false information is understood in context to mean that some false information that is provided to such websites is considered "harmless" and "acceptable false information." *See* Lynch Depo. at 47–49 (Def. Ex.

8, ECF No. 53-8) (same pages of deposition testimony cited by Defendant for the fact that "[d]ifferent web sites have different tolerances . . . for false information").

45. Plaintiffs have not yet determined the number of fictitious accounts or postings that will be necessary or how long each account or posting will exist. *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 8.

**PL. RESPONSE:** Undisputed.

46. "[E]very algorithm audit is bespoke, and every platform is different." Wilson Depo. Tr. (Exh. 4) at 107.

**PL. RESPONSE:** Undisputed.

47. Evaluating the ethics and potential harm of a particular study requires a fact- specific, case-by-case analysis regarding the details of the study and the platforms being studied. *See* Mislove Depo. Tr. (Exh. 3) at 101–04, 106–07, 110; Wilson Depo. Tr. (Exh. 4) at 106–07, 156.

**PL. RESPONSE:** Undisputed.

48. Even when Plaintiffs intend to undertake research on a particular topic, frequently the research may change direction and ultimately investigate something different and/or using different methods. *See* Mislove Depo. Tr. (Exh. 3) at 52–55; Wilson Depo. Tr. (Exh. 4) at 54.

**PL. RESPONSE:** Disputed to the extent that intended research by Plaintiffs may "frequently" change direction. Plaintiff Mislove testified as follows:

Q: Could your research plan change depending on information you learn as you do experiments?

A: That it feasibly could change.

Q: Does that happen frequently with research?

A: Um, I don't know if I would say "frequently." What I have found is when you start investigating online services, oftentimes you start with one idea, you start investigating and you find some other thing that is also interesting and so then you investigate that as well.

Mislove Depo. at 54 (Def. Ex. 3, ECF No. 53-3).

**III. Facts Pertaining to Private Websites' Status as "Public Forums"**

49. None of the websites or platforms that Plaintiffs previously accessed for their research regarding potential online discrimination, or that Plaintiffs may access in the future for such research, constitutes a "public forum" for First Amendment purposes. *See* Pls.' Resps. to Def.'s RFAs (Exh. 5), RFA No. 11.

**PL. RESPONSE:** Undisputed.

50. For each website or platform that Plaintiffs previously accessed for their research regarding potential online discrimination, or that Plaintiffs may access in the future for such research, Plaintiffs are unaware of any facts supporting the contention that those websites or platforms are "public forums" for First Amendment purposes. *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 7.

**PL. RESPONSE:** Undisputed.

51. LinkedIn "employs a range of technological measures and investigative tools to block, detect, and restrict fake accounts." Rockwell Decl. (attached hereto as Exh. 11) ¶ 19 [hereafter "LinkedIn Decl."]; *see also id.* ¶¶ 20–31.

**PL. RESPONSE:** Undisputed.

52. Facebook "undertakes substantial efforts to identify and remove fake accounts," including through technological means. Gleicher Decl. (attached hereto as Exh. 12) ¶ 12 [hereafter "Facebook Decl."]; *see also id.* ¶¶ 14–17.

**PL. RESPONSE:** Undisputed.

53. Glassdoor employs various "methods and strategies . . . to combat fake accounts," including employing "certain technology filters and algorithms that scan its website for suspicious user activity[.]" O'Brien Decl. (attached hereto as Exh. 13) ¶ 18 [hereafter "Glassdoor Decl."].

**PL. RESPONSE:** Undisputed.

54. Monster.com "uses an automated process" to remove fictitious accounts. Kardon Aff. (attached hereto as Exh. 14) ¶ 4 [hereafter "Monster.com Aff."].

**PL. RESPONSE:** Undisputed.

55. Monster.com requires credit card information before someone can create a recruiter account. *See* Wilson Depo. Tr. (Exh. 4) at 171; PID2185-2188 (attached hereto as Exh. 15); Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 5.

**PL. RESPONSE:** Undisputed to the extent that Monster required credit card information at the time Plaintiff Wilson created an account for his research. *See* Wilson Depo. at 171 (Def. Ex. 4, ECF No. 53-4); Pls. Third Suppl. Resps. to Def. First Interrogatories at 5 (Def. Ex. 6, ECF No. 53-6).

56. Plaintiff Wilson created the Monster.com recruiter account using his credit card information and a fake company name. *See* Wilson Depo. Tr. (Exh. 4) at 171–72; PID2185-2188 (Exh. 15); Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 5.

**PL. RESPONSE:** Undisputed.

57. CareerBuilder requires credit card information before someone can create a recruiter account. *See* Wilson Depo. Tr. (Exh. 4) at 174; Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 5.

**PL. RESPONSE:** Undisputed to the extent that CareerBuilder required credit card information at the time Plaintiff Wilson attempted to create an account for his research. *See* Wilson Depo. at 174–75 (Def. Ex. 4, ECF No. 53-4); Pls. Third Suppl. Resps. to Def. First Interrogatories at 5 (Def. Ex. 6, ECF No. 53-6).

58. Before enabling a recruiter account, CareerBuilder also requires verification that the accountholder is associated with a business by requiring certain business information—i.e., company name, company website, state of incorporation, and federal tax ID. *See* Wilson Depo. Tr. (Exh. 4) at 174–75, 180–81; PID7243-46 (attached hereto as Exh. 16); Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 5.

**PL. RESPONSE:** Undisputed to the extent that CareerBuilder required certain business information at the time Plaintiff Wilson attempted to create an account for his research. *See* Wilson Depo. at 174–75, 178–79 (Def. Ex. 4, ECF No. 53-4); Pls. Third Suppl. Resps. to Def. First Interrogatories at 5 (Def. Ex. 6, ECF No. 53-6).

59. Plaintiff Wilson attempted to create a recruiter account on CareerBuilder but was unable to do so because he lacked the requisite business information. *See* Wilson Depo. Tr. (Exh. 4) at 174–81; PID7237-38 (attached hereto as Exh. 17).

**PL. RESPONSE:** Undisputed.

60. One of Plaintiff Wilson's co-authors on the paper successfully created a recruiter account on CareerBuilder by pretending to be an employee of a real company and providing that company's business information to CareerBuilder for verification purposes. *See* Wilson Depo. Tr. (Exh. 4) at 177–81; PID7243-46 (Exh. 16); PID7237-38 (Exh. 17); Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 5.

**PL. RESPONSE:** Disputed to the extent that Defendant's characterization of Plaintiff Wilson's co-author "pretending to be an employee of a real company" suggests the co-author did not use her real name, did not have the company's consent, or was required to be an employee of the company. Plaintiff Wilson's co-author "created an account using her real name and credit card information but supplied the business license information of a third-party company, after informing the company of the purposes for which the business license information was needed and receiving the company's consent." Pls. Third Suppl. Resps. to Def. First Interrogatories at 5 (Def. Ex. 6, ECF No. 53-6).

## IV. Facts Pertaining to Plaintiffs' Lack of Expressive Activity

61. Plaintiffs seek to ensure that "false accounts or false postings do not attract attention from other users or lead other users to take action in response to those postings." Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 6.

**PL. RESPONSE:** Undisputed.

62. In any future research, Plaintiffs intend to "mak[e] sure that real job seekers are unlikely to find, and discouraged from applying to, the fictitious jobs" that Plaintiffs create, and "will take similar steps with their fictitious job seeker accounts to ensure they are unlikely to appear in search results for real recruiters' reasonable search queries." Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 6.

**PL. RESPONSE:** Undisputed.

63. In general, when Plaintiffs create a fake account for research purposes, their aim is to have no interactions at all with any real-world individuals. Wilson Depo. Tr. (Exh. 4) at 92; *see also id.* at 165.

**PL. RESPONSE:** Undisputed.

64. When Plaintiffs create fake accounts for research purposes, their goal is to have the fake accounts be the proverbial "tree [that] falls in the woods and no one is around." Wilson Depo. Tr. (Exh. 4) at 92–93.

**PL. RESPONSE:** Undisputed.

**V. Facts Pertaining to Application of Intermediate Scrutiny**

65. The CFAA was enacted to "prevent the digital equivalent of theft" and "prohibit the digital equivalent of trespassing." MTD Op. (ECF No. 24) at 36–37.

**PL. RESPONSE:** Undisputed to the extent that "the legislative history indicates that Congress was interested in passing the Access Provision to prevent the digital equivalent of theft." MTD Op., ECF No. 24, at 36. Disputed to the extent that Defendant's characterization of the Court's opinion on Defendant's motion to dismiss suggests the Court concluded that the CFAA was enacted to "prohibit the digital equivalent of trespassing," when in fact the Court simply acknowledged that the government had made that argument. *See id.* at 37.

66. 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.' Interrogs. Nos. 6, 7 (attached hereto as Exh. 18) at 3.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

67. The Government's enforcement of the Access Provision promotes private property rights. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

68. The Government's enforcement of the Access Provision helps prevent economic harm. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

69. The Government's enforcement of the Access Provision helps deter fraud and other related criminal conduct. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3–4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

70. The Government's enforcement of the Access Provision protects third-party users. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

71. The Government's enforcement of the Access Provision protects the integrity of data, websites, and platforms. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

72. The Government's enforcement of the Access Provision protects the public and national interests, particularly with respect to efforts to promote misinformation. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3–4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding what the Government's enforcement of the Access Provision accomplishes.

73. "On average, LinkedIn blocks millions of attempts to create fake accounts and shuts down hundreds of thousands of fake accounts each quarter." LinkedIn Decl. (Exh. 11) ¶ 7.

**PL. RESPONSE:** Undisputed.

74. Between January and September 2018, Facebook "disabled approximately 2.1 billion fake accounts." Facebook Decl. (Exh. 12) ¶ 16.

**PL. RESPONSE:** Undisputed.

75. From January 2018 through December 3, 2018, Monster.com suspended over 170,000 fraudulent accounts of supposed job seekers in the EU and North America. *See* Monster.com Aff. (Exh. 14) ¶ 4.

**PL. RESPONSE:** Undisputed.

76. "Given the volume of fake accounts, there is no way for Monster.com to distinguish between fake accounts that might be created by researchers and those created for fraudulent or other activities." Monster.com Aff. (Exh. 14) ¶ 4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding whether there is literally "no way" for Monster to determine whether a fake account is being used by researchers.

77. "It is difficult, and often impossible, to determine immediately whether a fake account is created with a socially beneficial or malicious intent. When an account is created, LinkedIn cannot discern whether a fake account will be used either immediately or at some future date for any . . . abuses or as part of academic or journalistic research." LinkedIn Decl. (Exh. 11)

**PL. RESPONSE:** Undisputed.

78. Absent compliance with safeguards that Facebook has created, "Facebook will have difficulty determining (among other things) whether a researcher seeking data is a legitimate researcher or a bad actor, what data they intend to access, and how they plan to secure and use the data." Facebook Decl. (Exh. 12) ¶ 19.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement by a third party that only "compliance with safeguards that Facebook has created" would eliminate any "difficulty determining . . . whether a researcher . . . is a legitimate researcher or a bad actor . . . ." Disputed as inconsistent with other testimony by the same party, which demonstrates that Facebook is able to identify bad actors using false accounts. Elsewhere in the Facebook declaration cited by Defendant is testimony regarding "efforts" made by Facebook that have "enabled [it] to identify and take action against a number of bad actors who have engaged in improper and abusive conduct in the United States and elsewhere around the world using fake accounts," citing the examples of 82 pages, groups, and accounts that originated in Iran, and 559 pages and 251 account that "consistently broke [] rules against spam and coordinated behavior." Facebook Dec. at ¶ 17 (Def. Ex. 12, ECF No. 53-12). Facebook also identifies specific harmful conduct that bad actors use fake accounts to engage in: "tricking people into sharing private information and images; grooming and exploiting minors; harassing and intimidating domestic abuse survivors, human rights activists, and other targeted communities; and bullying, extorting, and other abusive behavior. Bad actors also use fake accounts to manipulate and corrupt public debate, including by creating networks of accounts to mislead others about who they represent or what message they intend to deliver." *Id.* at ¶ 11.

79. When a fake account is created, private websites are unable to determine whether the fake account will be used for socially beneficial purposes (such as academic research) or

for more harmful purposes. *See* ¶¶ 76–78, supra; *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 2–3.

**PL. RESPONSE:** Disputed to the extent it relies on the disputed statements in paragraphs 76–78 by third-party companies. Disputed to the extent that stating that private websites are "unable" to determine whether the fake account will be used for socially beneficial purposes is a self-serving statement by Defendant that is not competent proof.

80. When Plaintiffs perform audits of websites for potential discrimination, Plaintiffs intend for their research activity to remain unknown to the website. *See* Wilson Depo. Tr. (Exh. 4) at 99 ("We want to stay under the service's radar to the greatest extent possible."); *see also* Mislove Decl. (ECF No. 48-2) ¶¶ 36–38; Wilson Decl. (ECF No. 48-1) ¶¶ 36–38; Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 4; Pls.' Resps. to Def.'s Second Interrogs. (attached hereto as Exh. 19), Interrog. No. 18.

**PL. RESPONSE:** Undisputed to the extent Plaintiffs intend for their research activity to remain unknown to the website for the duration of the research activity. Plaintiffs typically inform websites or platforms of their research findings prior to publication, *see* Mislove Depo. at 62–63 (Def. Ex. 3, ECF No. 53-3), and when they publish a paper naming the websites they studied, that information becomes public and known to the website, *see* Wilson Depo. at 72–73 (Def. Ex. 4, ECF No. 53-4).

81. People who have been prosecuted under the CFAA have previously tried to claim that they were engaging in "security research." *See* Lynch Depo. Tr. (Exh. 8) at 74–77.

**PL. RESPONSE:** Disputed, as incomplete and misleading with respect to the testimony cited, to the extent Defendant suggests that past CFAA prosecutions have only involved those who "tried to claim that they were engaging in 'security research.'" Mr. Lynch, in his individual capacity,

testified that "some people who have at least called themselves security researchers" have been prosecuted under the CFAA, Lynch Depo. at 76 (Def. Ex. 8, ECF No. 53-8), and also that he has "read about cases where security researchers have either been prosecuted or have expressed concern about prosecution." *Id*. at 77.

82. "All of the [Government's] 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. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 5; *see also* Lynch Depo. Tr. (Exh. 8) at 90.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

83. "[W]hen a fake account is created in violation of a website's ToS, regardless of whether the fake account is well-intentioned or not—i.e., regardless of whether it is being used for academic research regarding potential discrimination or some other purpose—the fake account still undermines private parties' property rights, and can still create economic harms, negatively affect third-party users, and undermine the integrity of a website or platform." Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 5.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

84. "[B]y preserving Defendant's ability to enforce the CFAA in all circumstances covered by the CFAA's terms, that indirectly re-enforces all of the [governmental] interests encompassed by the CFAA." Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 5; *see also* Lynch Depo. Tr. (Exh. 8) at 90.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

85. "If the First Amendment were construed to prohibit Defendant from enforcing the CFAA against academic researchers who violate websites' ToS restricting the creation of fake accounts . . . that could threaten Defendant's ability to enforce the CFAA against other individuals not performing academic research but nonetheless engaging in conduct (allegedly) protected by the First Amendment—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." Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 5–6.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

86. If the First Amendment were construed to prohibit Defendant from enforcing the CFAA against academic researchers who violate websites' ToS restricting the creation of fake accounts, "[s]uch a construction could also decrease the CFAA's deterrent value with respect to individuals who might create fake accounts in violation of websites' ToS for more directly harmful purposes." Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 6.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

87. By definition, every time someone intentionally accesses a computer without authorization or exceeds authorization, that person has transgressed the computer owner's

right to exclude that person. *See* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3, 6.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding the Government's interests, which is additionally a legal conclusion.

88. The mere presence of fake accounts harms private platforms, regardless of the purpose for which the fake account was created or any subsequent actions taken by the fake accountholder. *See* LinkedIn Decl. (Exh. 11) ¶¶ 8–10, 13; Glassdoor Decl. (Exh. 13) ¶¶ 16, 20–21; Facebook Decl. (Exh. 12) ¶¶ 6, 10; Monster Aff. (Exh. 14) ¶ 2.

**PL. RESPONSE:** Disputed. To the extent the statement can be attributed to the cited testimony of third parties LinkedIn, Glassdoor, Facebook, and Monster, it is a self-serving and conclusory statement by third parties that the "mere presence of fake accounts harms" them, "regardless of the purpose for which the fake account was created or any subsequent actions taken by the fake accountholder," that is not competent proof of actual harm. *See* LinkedIn Dec. at ¶ 13 (Def. Ex. 11, ECF No. 53-11) (making conclusory statement that the "mere presence of fake accounts pollutes LinkedIn's platforms and causes harms"). It is also not competent proof as to all "private platforms" beyond the four third-party platforms listed. Disputed also to the extent that "harm" is a legal conclusion or legal determination at issue in this case.

Additionally, the cited paragraphs of the Facebook declaration do not support the categorical statement that the "mere presence of fake accounts" causes harm to Facebook regardless of purpose or subsequent actions taken. *See* Facebook Dec. at ¶¶ 6, 10 (Def. Ex. 12, ECF No. 53-12) (describing Facebook's Community Standards, and noting that "the presence of fake accounts *can* create a feeling of unease and wariness when using Facebook" and "*can* also

feed into *potential* concerns about unwanted contact, safety, and privacy when using Facebook") (emphases added).

The cited paragraphs of the Glassdoor declaration do not support the categorical statement that the "mere presence of fake accounts" causes harm to Glassdoor regardless of purpose or subsequent actions taken. *See* Glassdoor Dec. at ¶¶ 16, 20–21 (Def. Ex. 13, ECF No. 53-13) (noting fake accounts "impact the authenticity" of the website because they "*can* skew certain statistics and metrics . . . and *may* contribute fake content . . . *that might* mislead Glassdoor users," that "[f]ake accounts could *theoretically affect* Glassdoor's services in a number of ways," and additionally discussing "false, manufactured or artificially inflated *reviews*" of employers that, if not monitored, could "*theoretically*" lead to fewer Glassdoor users) (emphases added).

The cited paragraph of the Monster affirmation does not support the categorical statement that the "mere presence of fake accounts" causes harm to Monster regardless of purpose or subsequent actions taken. *See* Monster Aff. at ¶ 2 (Def. Ex. 14, ECF No. 53-14) (discussing the harms to Monster specifically from Monster's own business model because when users "create fictitious or false accounts," Monster "*then turn[s] around*" and charges employers for viewing fictitious or false resumes that were, presumably, uploaded by users after the fact of creating fictitious accounts) (emphasis added).

89. Recognizing a First Amendment right to create false or misleading accounts—even ones to be used for research purposes—would threaten online hiring websites' ability to earn money through paid services. *See* Monster Aff. (Exh. 14) ¶ 2; LinkedIn Decl. (Exh. 11) ¶ 10; Glassdoor Decl. (Exh. 13) ¶¶ 20–21.

**PL. RESPONSE:** Disputed. To the extent the statement can be attributed to the cited testimony of third parties LinkedIn, Glassdoor, Facebook, and Monster, it is a self-serving and conclusory statement regarding third parties' ability to earn money in the future.

90. The presence of fake accounts on private websites—even for purposes of research—harms the websites' reputation, brand, and authenticity. *See* LinkedIn Decl. (Exh. 11) ¶¶ 4–5, 8–10; Facebook Decl. (Exh. 12) ¶¶ 6, 10; Glassdoor Decl. (Exh. 13) ¶¶ 15–16, 21; Monster Aff. (Exh. 14) ¶ 2; *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3–5.

**PL. RESPONSE:** Disputed. To the extent the statement can be attributed to the cited testimony of third parties LinkedIn, Glassdoor, Facebook, and Monster, it is a self-serving and conclusory statement regarding harm to third parties' reputation, brand, and authenticity. Disputed also to the extent that "harm" is a legal conclusion or legal determination at issue in this case.

91. Plaintiff Mislove believes that if a platform is known to have many fake resumes, "that could impact the site or platform." Mislove. Depo. Tr. (Exh. 3) at 109–110.

**PL. RESPONSE:** Undisputed.

92. Because Glassdoor requires users to submit user-generated content (such as a company review) in order to maintain access to Glassdoor's information, the creation of a fake account—even for purposes of academic research—would introduce unreliable information onto the platform, thereby harming the authenticity and integrity of Glassdoor. Glassdoor Decl. (Exh. 13) ¶¶ 8, 16, 20–21.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement by Glassdoor regarding the harm to the "authenticity and integrity" of Glassdoor's interests. Disputed also to the extent that "harm" is a legal conclusion or legal determination at issue in this case.

93. Glassdoor has taken many steps to encourage subscribers to submit authentic information, including going to court when necessary to protect its subscribers' anonymity. *See* Glassdoor Decl. (Exh. 13) ¶¶ 11–14.

**PL. RESPONSE:** Undisputed.

94. Glassdoor believes that its "give to get" policy—of requiring users to contribute content or other information about their current or former employer in order to maintain access to certain content on the website—has multiple benefits and "has been a central component of Glassdoor's strategy to strengthening and maintaining the continued vitality of glassdoor.com." Glassdoor Decl. (Exh. 13) ¶ 9; *see also id*. ¶¶ 8, 10.

**PL. RESPONSE:** Undisputed to the extent the statement is a reflection of Glassdoor's belief.

95. The presence of unreliable information on Glassdoor harms third-party users who rely on the information made available on Glassdoor for their own employment decisions. *See* Glassdoor Decl. (Exh. 13) ¶¶ 3, 16–18, 20–21.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement about harm to third-party users. Disputed also to the extent that "harm" is a legal conclusion or legal determination at issue in this case.

96. The presence of fake accounts on hiring websites, regardless of the fake accounts' purpose, threatens to harm third-party users by making it harder for real users to find other authentic accounts on the platform, by potentially displacing real users in employers' search queries, and by potentially causing real users to waste their time applying for fictitious jobs. *See* LinkedIn Decl. (Exh. 11) ¶ 9; Glassdoor Decl. (Exh. 13) ¶ 20; *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 4–6.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement about "threaten[ed]" harms to third-party users and "potential" displacement or "potential" waste of time. Disputed also to the extent that "harm" is a legal conclusion or legal determination at issue in this case.

97. Plaintiff Mislove believes that if a website or platform has fake accounts and those fake accounts are posting fake jobs or applying to jobs fictitiously, "that would have a potential negative impact on the employment platform." Mislove Depo. Tr. (Exh. 3) at 108.

**PL. RESPONSE:** Undisputed, to the extent Plaintiff Mislove was testifying in the context of a question about whether the mere existence of fake accounts on a website would have a negative impact on a platform's reputation. Plaintiff Mislove testified that it would require more than simply the existence of fake accounts, and that if a website is "known to not only have fake accounts but the accounts" are used "for things like posting fake jobs or applying to fake jobs—or applying to jobs fictitiously . . . that would have a potential negative impact on the employment platform." Mislove Depo. at 108 (Def. Ex. 3, ECF No. 53-3). Plaintiff Mislove further testified that "if you have a handful of fake resumes . . . that is a de minimus harm to the site" "[b]ut if it rises to the level where . . . the site has a reputation for having fake accounts or fake resumes—excuse me, just fake resumes, that is the point at which I would say the harm changes." *Id*. at 109.

98. The presence of fake accounts on websites, regardless of the fake accounts' purpose, undermines the integrity of the websites and their data. *See* LinkedIn Decl. (Exh. 11) ¶ 11; Glassdoor Decl. (Exh. 13) ¶¶ 16, 20; Wilson Depo. Tr. (Exh. 4) at 97–98; *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 4–6.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement by third parties regarding whether fake accounts undermine their integrity and their data. Disputed also to the extent that harm is a legal conclusion or legal determination at issue in this case.

The testimony of Plaintiff Wilson cited by Defendant does not support the categorical statement regarding the "presence of fake accounts on websites" writ large. Plaintiff Wilson testified that "[i]f the number of fake [accounts] you made was a significant number relative to the totality of the population" on a "smaller company [that] is presumably in their growth phase" then the "harms are difficult to conceptualize but *perhaps* . . . it could be misleading" to the company's engineers. *See* Wilson Depo. at 98 (Def. Ex. 4, ECF No. 53-4) (emphasis added).

99. Fake accounts on private platforms are routinely used to perpetrate various types of harmful acts—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* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3–4; LinkedIn Decl. (Exh. 11) ¶ 12(a)–(e); Facebook Decl. (Exh. 12) ¶¶ 11, 17–18; Monster Aff. (Exh. 14) ¶ 3.

**PL. RESPONSE:** Disputed to the extent that the behaviors described are categorized as "routine" uses of fake accounts, which is not supported by the cited declarations of third-party companies. To the extent the behaviors are described by "routine" by Defendant in its Interrogatory response, such a statement is self-serving and not competent proof for the proposition asserted.

100. Misinformation, including political mis-information by state and non-state actors, causes significant harms. *See* Wilson Depo. Tr. (Exh. 4) at 68–70; LinkedIn Decl. (Exh. 11) ¶ 12(e); Facebook Decl. (Exh. 12) ¶¶ 17–18; Def.'s Suppl. Resps. to Pls.' Interrogs.

Nos. 6, 7 (Exh. 18) at 4; *see also Report of the Attorney General's Cyber Digital Task Force* (July 2, 2018) (attached hereto as Exh. 20) at DOJ-00334 ("Using false U.S. personas, adversaries could covertly create and operate social media pages and other forums designed to attract U.S. audiences and spread disinformation or divisive messages.") [hereafter "*Cyber Digital Task Force Report*"].

**PL. RESPONSE:** Disputed to the extent that the characterization of the harms from misinformation as "significant" is a legal conclusion. Plaintiff Wilson's deposition testimony cited by Defendant does not use the phrase "significant harms." *See* Wilson Depo. at 68–70 (Def. Ex. 4, ECF No. 53-4).

101. Removing fake accounts helps prevent the perpetration of these various harmful acts because "bad actors rarely engage in bad acts openly." LinkedIn Decl. (Exh. 11) ¶ 12; *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 3 (noting that fake accounts are often used "in an attempt to frustrate law enforcement"); *Cyber Digital Task Force Report* (Exh. 20) at DOJ-00341 (noting that "the success of a foreign influence campaign via the Internet and social media depends heavily on the adversary's ability to obscure the true motivation and origin of its activities—something the Internet can facilitate").

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement by Defendant about whether removing *all* fake accounts "helps prevent the perpetration of these various harmful acts," *see supra*. Disputed also to the extent that harm is a legal conclusion or legal determination at issue in this case.

102. The Government has an interest in "removing fake accounts before these schemes come to fruition or a person is actually defrauded." Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 4.

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding Defendant's interests, which is additionally a legal conclusion.

103. In a past research paper, Plaintiff Wilson acknowledged that "[f]ake identities and Sybil accounts are pervasive in today's online communities"; that "[t]hey are responsible for a growing number of threats, including fake product reviews, malware and spam on social networks, and astroturf political campaigns"; and that "[u]nfortunately, studies show that existing tools such as CAPTCHAs and graph-based Sybil detectors have not proven to be effective defenses." *You Are How You Click: Clickstream Analysis for Sybil Detection,* 22nd USENIX Security Symposium (Aug. 2013) (attached hereto as Exh. 21) at 241 ("Abstract"); *see also* Wilson Depo. Tr. (Exh. 4) at 206–07.

**PL. RESPONSE:** Undisputed.

104. In a past research paper, Plaintiff Wilson acknowledged that "[o]nline social networks (OSNs) are popular collaboration and communication tools for millions of Internet users;" that "[u]nfortunately, recent evidence shows that these trusted communities can become effective mechanisms for spreading malware and phishing attacks"; and that "[u]sing compromised or fake accounts, attackers can turn the trusted OSN environment against its users by masquerading spam messages as communications from friends and family members." *Detecting and Characterizing Social Spam Campaigns*, IMC 2010 (Nov. 2010) (attached hereto as Exh. 22) at 1 ("Introduction"); *see also* Wilson Depo. Tr. (Exh. 4) at 208–09.

**PL. RESPONSE:** Undisputed.

105. In a past research paper, Plaintiff Mislove acknowledged that "[u]sers increasingly rely on crowdsourced information, such as reviews on Yelp and Amazon, and liked posts and ads on Facebook"; that "[t]his has led to a market for black-hat promotion techniques via fake (e.g., Sybil) and compromised accounts"; and that "[c]ustomers of these black-market services seek to influence the otherwise 'organic' user interactions on the service." *Towards Detecting Anomalous User Behavior in Online Social Networks*, 23rd USENIX Security Symposium (Aug. 2014) (attached hereto as Exh. 23) at 223 ("Abstract," "Introduction"); *see also* Mislove Depo. Tr. (Exh. 3) at 179–80.

**PL. RESPONSE:** Undisputed.

106. In a past research paper, Plaintiff Mislove acknowledged that "[m]ultiple identity, or Sybil, attacks pose a fundamental problem in web-based and distributed systems"; that in such an attack "a malicious user creates multiple (Sybil) identities and takes advantage of the combined privileges associated with these identities to attack the system"; that on auction sites these attacks allow "a fraudulent user [to] continue to use the system by creating a new user account whenever her existing accounts have acquired a bad reputation"; and that on social networking sites "an attacker can create multiple identities to cast bogus votes and manipulate content popularity." *Exploring the Design Space of Social Network-Based Sybil Defenses*, IEEE (2012) (attached hereto as Exh. 24) at 1 ("Introduction"); *see also* Mislove Depo. Tr. (Exh. 3) at 182–83.

**PL. RESPONSE:** Undisputed.

107. DOJ's past statements to Congress about having "no interest in prosecuting harmless violations of use restrictions" reflect DOJ's lack of intent to prosecute such conduct, not a statement about the governmental interests underlying the statute. *See* Lynch Depo. Tr. (Exh. 8) at 36–38 ("It is not a statement relating to the scope of the crime. It is a statement regarding our interests in prosecution of those – of certain sorts of Computer Fraud and Abuse Act violations."); *see also* Def.'s Suppl. Resps. to Pls.' Interrogs. Nos. 6, 7 (Exh. 18) at 5–6 (confirming that governmental interests are implicated by Plaintiffs' conduct).

**PL. RESPONSE:** Disputed as a self-serving and conclusory statement regarding Defendant's interests, which is additionally a legal conclusion. The DOJ's past statements to Congress speak for themselves.

108. DOJ's past legislative proposals to Congress were part of a compromise package, 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 or meet another predicate). *See* Stmt. of Sujit Raman (Exh. 10) at DOJ-00019; Stmt. of David Bitkower (ECF No. 10-3) at 6–7; Lynch Depo. Tr. at 55–58.

**PL. RESPONSE:** Undisputed.

109. Plaintiffs believe that Ticketmaster would suffer only de minimis harm if an individual circumvented Ticketmaster's code-based access 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* Mislove Depo. Tr. (Exh. 3) at 150–53; Wilson Depo. Tr. (Exh. 4) at 154–56.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinion expressed by Plaintiff Wilson regarding whether the described harm suffered by Ticketmaster is de minimus. Plaintiff Wilson testified that to determine harm "you have to get into the nuance of the situation. Am I doing this because I have eight family members? I don't see that as harm. We are all buying tickets to go to the show." Wilson Depo. at 156 (Def. Ex. 4, ECF No. 53-4). He also testified that "[i]f this is done at larger scale for personal profit, then yes, I would view that as harm." *Id*. at 155.

Disputed as an incomplete and misleading statement of the opinion expressed by Plaintiff Mislove regarding whether the described harm suffered by Ticketmaster is de minimus. Plaintiff Mislove testified that "it is not clear that Ticketmaster was being harmed in that case and if they were selling the tickets they probably would have sold them anyways. But there may be non de minimus harm to third parties who would have been able to buy tickets and now in aggregate have not been able to do so. If there was a sufficiently large number of tickets bought to cause the amount of harm." He also testified, with respect to Ticketmaster's exclusive right to sell tickets, "[I]t seems a harder case to make that that Ticketmaster has been harmed in that they got all the money they would have gotten in the end regardless of actually who bought the tickets." Mislove Depo. at 151, 153 (Def. Ex. 3, ECF No. 53-3).

110. Plaintiff Wilson believes that displacing a real user from the top position in an employer's search results, so that the real user now appears in the third position—below two fake users—is not a substantive harm. *See* Wilson Depo. Tr. (Exh. 4) at 165.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinion expressed by Plaintiff Wilson. Plaintiff Wilson testified as follows: "So, somebody, let's say, who could have been the top result is now all of a sudden the third result. I mean, it depends on how many resumes recruiters are looking at. It would be difficult to argue that that is a substantive harm. But . . . we did try to engineer these such that they would not appear at the top of search results displacing the top candidates." Wilson Depo. at 165 (Def. Ex. 4, ECF No. 53-4).

111. Plaintiff Mislove believes that some cyber attacks where an attacker creates many fake accounts with the intention of obtaining more privileges than they would otherwise get may involve only de minimis harm. *See* Mislove Depo. Tr. (Exh. 3) at 184–85.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinion expressed by Plaintiff Mislove. Plaintiff Mislove testified as follows:

Q: What is a Sybil attack?

A: That is an attack where an attacker creates many fake accounts with the intention of obtaining more privileges than they would otherwise get.

Q: Would you agree that that is more than de minimus harm?

A: Not necessarily. It depends upon what they did with the accounts.

Q: . . . What is a circumstance where a Sybil attack is de minimus harm?

A: Again, if I go to one of these services and create a number of accounts but don't do anything with them, I would argue that is de minimus harm.

Mislove Depo. at 184 (Def. Ex. 3, ECF No. 53-3).

112. Plaintiffs have never worked at an online employment company. *See* Wilson Depo. Tr. (Exh. 4) at 98; Mislove Depo. Tr. (Exh. 3) at 104.

**PL. RESPONSE:** Undisputed.

113. Plaintiffs have never been privy to internal deliberations within an online employment company. *See* Wilson Depo. Tr. (Exh. 4) at 98; Mislove Depo. Tr. (Exh. 3) at 105.

**PL. RESPONSE:** Undisputed.

114. Plaintiffs are unable to assess whether their research undermines companies' private property rights. *See* Mislove Depo. Tr. (Exh. 3) at 153–54.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinion expressed by Plaintiff Mislove. Plaintiff Mislove testified as follows: "I feel capable of making a determination of the harms of the kinds of research that I do. And I feel capable of understanding, not in the legal level because I'm not a lawyer, what other risks that kinds of users that I entail [sic]. I don't know if that answers your question. If it is asking specifically about property rights." Mislove Depo. at 153 (Def. Ex. 3, ECF No. 53-3).

115. Aside from the technical concepts associated with their research design (e.g., burden on the companies' servers, storage space, etc.), Plaintiffs can only speculate as to whether their conduct causes harm to companies from the companies' perspective. *See* Wilson Depo. Tr. (Exh. 4) at 102–04; Mislove Depo. Tr. (Exh. 3) at 105–07, 110.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinions expressed by Plaintiffs Mislove and Wilson. On the pages of his deposition cited by Defendant, Plaintiff Mislove testified in detail as to the considerations he takes into account regarding potential harms to a company from research, and, specifically, testified , "We are not privy to [a company's] internal inclination. But having experience as a computer scientist for a number of years and having experience knowing how these services operate . . . I can make an informed guess as to the impact that whatever number we are talking about of fake accounts would have."

He further testified that he would take into account "how many users they have on their platform, how many resumes and so forth. And . . . we have some estimate of . . . what fraction our study is going to be relative to their entire user population." Mislove Depo. at 110 (Def. Ex. 3, ECF No. 53-3); *see also id*. at 105–07.

On the pages of his deposition cited by Defendant, Plaintiff Wilson testified in detail as to the considerations he takes into account regarding potential harms to a company from research. *See* Wilson Depo. at 102 (Def. Ex. 4, ECF No. 53-4) (testifying that "based on my experience and knowledge as a computer scientist and my understanding of how platforms are constructed, I believe I am able to determine what would be de minimus"). In response to a question asking whether, "setting aside the infrastructure technological side and the things about the user accounts that you control . . . and setting aside the reputational harm . . . [a]re you able to determine whether the creation of a fake account harms a company's business?," Plaintiff Wilson testified, "I would say yes." *Id*. at 103; *see also id.* at 104 (testifying that "based on my understanding of how these systems are built, how they are managed, my vague understanding of how investors assess the companies and the things that they disclose, the way they manage their operations, I don't see the potential for harm" and "no, I'm not a businessman" and "I don't run these companies").

116. The Access Provision does not prohibit Plaintiffs from conducting algorithm audits that do not require the creation of false or misleading accounts. *See* ¶¶ 1–4, *supra* (Plaintiffs previously conducted algorithm audits without creating fake accounts); Mislove Depo. Tr. (Exh. 3) at 92 (not all algorithm audits require creation of fake accounts); Wilson Depo. Tr. (Exh. 4) at 59–60.

**PL. RESPONSE:** Disputed to the extent this calls for a legal conclusion as to whether the Access Provision would prohibit the activities required to conduct algorithm audits that do not require the creation of false or misleading accounts, which depends on whether the terms of service of a target website would prohibit those activities at the time the research is conducted. Undisputed that Plaintiffs have conducted previous research without creating false accounts.

117. Even if Plaintiffs' algorithm audit did require creating false or misleading accounts, the Access Provision does not prohibit Plaintiffs from conducting audits on websites that do not have ToS requiring truthful information, and/or ToS that are not genuine access restrictions. *See* MTD Op. at 34; Lynch Depo. Tr. (Exh. 8) at 45–46.

**PL. RESPONSE:** Disputed to the extent that it calls for a legal conclusion regarding when a term of service is a "genuine access restriction."

118. Even if Plaintiffs' algorithm audit required creating user accounts and websites genuinely conditioned access on the provision of truthful information, the Access Provision does not prohibit Plaintiffs from conducting algorithm audits using real-world individuals who possess the necessary characteristics (i.e., who are sufficiently similar but for the protected class being tested). *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 11 (noting that "[u]se of real-world individuals is a standard research method" in investigating potential online discrimination); *see also* P-SMF ¶¶ 28, 30 (noting that real individuals are used in audit testing); Mislove Depo. Tr. (Exh. 3) at 87–88 (algorithm audits are the equivalent of offline audit studies, which involve real people); Wilson Depo. Tr. (Exh. 4) at 89–90 (same); *id.* at 137 (acknowledging that "I could get two people, I guess, who are very similar to sign up" and "that would also accomplish the same thing").

**PL. RESPONSE:** Disputed. The Access Provision can prohibit Plaintiffs from conducting algorithm audits using real-world individuals when such individuals would have to provide false or misleading information to a website to conduct the audit in violating of such a website's ToS prohibiting false or misleading information. The testimony of Plaintiff Wilson cited by Defendant was, in full, as follows:

Q: Do you believe in using real-world individuals would have allowed you to accomplish the experimental phase of [the CHI 2018] paper?

A: Okay, so what do you mean by "accomplish." I could tell someone to go make fake accounts on my behalf. Or I could get two people, I guess, who are very similar to sign up. And that would also accomplish the same thing. It is not entirely clear to me how that is fundamentally different than what we did. Telling two people to make two accounts on the service if they didn't have any intention of doing so anyway, I mean that sounds exactly like what we did. Is two inauthentic accounts.

Wilson Depo. at 137 (Def. Ex. 4, ECF No. 53-4).

119. Two algorithm auditors—Christian Sandvig and Karrie Karahalios—believe that it is possible to perform algorithm audits using real-world individuals, either in the form of a "noninvasive user audit" or a "crowdosourced audit / collaborative audit." *See* Sandvig et al., Au*diting Algorithms: Research Methods for Detecting Discrimination on Internet Platforms* (May 2014) (attached hereto as Exh. 25) at PID00143-44, PID00146-48; *see also* Mislove Depo. Tr. (Exh. 3) at 119.

**PL. RESPONSE:** Disputed as an incomplete statement of the opinions expressed by Christian Sandvig and Karrie Karahalios in their paper, cited by Defendant. The paper speaks for itself. With respect to whether it is possible to perform algorithmic audits using real-world individuals,

the paper states the following with respect to a "noninvasive user audit": "it may be stretching a point to call it an audit," "*it might be possible to infer something useful* about the operation of a platform's algorithm" and "[y]et without the benefit of any manipulation or random assignment to conditions this is not an experimental design, and it may be quite difficult to infer causality from any particular results," it "introduces a serious sampling problem" that "is an extremely difficult one" requiring "great expense and effort when compared to other designs," and "a survey-based audit that relies upon any kind of self-report measure is likely to introduce significant validity problems that may be insurmountable" because "error rates as high as 50%" have been found when comparing self-reported behavior to measured behavior. *See* Sandvig et al., *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms* (May 2014) at 11 (Def. Ex. 25, ECF No. 53-25, at PID0143) (emphases added). In describing one design of a "crowdsourced audit/collaborative audit" the authors note the problem of "injecting false data into the [website or platform]" which is the same as for sock-puppet audits, or audits that rely on false or tester accounts. *See id*. at 14–16, PID0146-48.

120. Plaintiff Mislove has performed an algorithm audit in the past using real-world individuals. *See* Mislove Depo. Tr. (Exh. 3) at 92–94.

**PL. RESPONSE:** Undisputed.

121. Before proceeding with the portion of the CHI 2018 paper that involved the creation of fictitious user accounts, Plaintiff Wilson did not consider recruiting real-world individuals instead of creating fake accounts. *See* Wilson Depo. Tr. (Exh. 4) at 141.

**PL. RESPONSE:** Undisputed.

122. Plaintiffs have not considered trying to perform their potential future algorithm audits using real-world individuals. *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 9.

**PL. RESPONSE:** Undisputed.

123. Even if Plaintiffs' algorithm audit required creating fictitious user accounts on a website or platform that had a genuine access restriction prohibiting such conduct, the Access Provision would not prohibit Plaintiffs from conducting algorithm audits on websites or platforms that consent to such audits. *See* 18 U.S.C. § 1030(a)(2)(C) (prohibiting only access "without authorization" or "exceed[ing] authorized access").

**PL. RESPONSE:** Disputed, to the extent it calls for a legal conclusion regarding whether consent from a company, and what form of any such consent, to an algorithm audit would override any violation of terms of service prohibitions, for purposes of liability under the Access Provision.

124. Two algorithm auditors—Christian Sandvig and Karrie Karahalios—believe that it is possible to perform a scientifically valid algorithm audit with the consent of the company. *See Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms* (Exh. 25) at PID00146 ("[A] virtuous algorithm provider might consent to an independent sock puppet audit as a public relations or trust-building tactic."); *see also* Mislove Depo. Tr. (Exh. 3) at 119.

**PL. RESPONSE:** Disputed, as an inaccurate characterization of the opinions expressed by Christian Sandvig and Karrie Karahalios in their paper, cited by Defendant. The paper speaks for itself. The language quoted by Defendant, that a "*virtuous* algorithmic provider *might* consent to an independent sock puppet audit *as a public relations or trust-building tactic*" does not support

the statement that the authors believe "it is possible to perform a *scientifically valid* algorithm audit with the consent of the company." *See* Sandvig et al., *Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms* (May 2014) at 14 (Def. Ex. 25, ECF No. 53-25, at PID0146) (emphases added).

125. In Plaintiffs' view, it is possible for an algorithm audit conducted with the company's consent to be scientifically valid, assuming the audit was performed under the necessary conditions. *See* Mislove Depo. Tr. (Exh. 3) at 121–24; Wilson Depo. Tr. (Exh. 4) at 118–19, 121–22.

**PL. RESPONSE:** Disputed as an incomplete and misleading statement of the opinions expressed by Plaintiffs Mislove and Wilson.

The testimony of Plaintiff Mislove on the pages cited by Defendant, was as follows:

Q: Is a virtuous algorithm provider consenting to an independent sock puppet audit, would the results of that audit in your view be scientifically valid?

A: I would view such results very skeptically.

Q: Is it possible that it would be scientifically valid?

A: It may be possible, but it would raise many issues of exactly what they consented to, what their researchers had access to, how—what it meant for them to consent. . . . [D]id they fund[] the research? Was the research done by internal employees or some external employees? Were the people who were doing the audit under any sort of obligations or restrictions in terms of publication? So, I think it would be very unlikely that I would view such an algorithmic audit to have the same level of scientific validity that a non-consented one or one where they were not made aware of at the time.

Q: If all of the variables were worked out such that the audit was truly independent, would that audit be scientifically valid?

A: *If all of those were worked out*—and potentially I also need to think on it a little more, but if those were, yes.

Mislove Depo. at 121–22 (Pl. Ex. 20) (emphases added).

The testimony of Plaintiff Wilson on the pages cited by Defendant makes clear that Plaintiff Wilson speculated about a hypothetical set of circumstances under which an algorithm audit conducted with the company's consent might be valid, and that it was unclear to him whether such a set of circumstances could ever occur. Plaintiff Wilson testified that "[i]f I could imagine a bug bounty program that is truly restriction free in the sense that it says something like you can audit using whatever type of audit you want, *you don't have to tell us ahead of time*, that seems like it would be scientifically valid." Wilson Depo. at 118 (Def. Ex. 4, ECF No. 53-4) (emphasis added). He also testified, in response to a question about requesting advance permission from a company to conduct an audit, that doing so "would immediately raise questions about the ecological validity. I mean, the same could be said for an in-person audit. Do you tell the person ahead of time that you are going to be looking at civil rights and sending in fake people[;] you change your behavior when you know you are being watched." *Id*. at 119.

126. Plaintiff Wilson believes that companies should establish "algorithmic bug bounties," which would allow researchers to conduct scientifically valid audits with the company's consent. *See* Wilson Depo. Tr. (Exh. 4) at 114–19.

**PL. RESPONSE:** Disputed to the extent that the statement characterizes Plaintiff Wilson as having testified that an algorithmic bug bounty program would allow researchers to conduct scientifically valid audits with the company's consent. Plaintiff Wilson testified as to the

conditions for such a program that would be required for it to be scientifically valid, *see supra* (response to paragraph 125), which would include the requirement that a researcher not tell the company ahead of time of a planned audit. *See* Wilson Depo. at 119 (Def. Ex. 4, ECF No. 53-4). Undisputed to the extent that Plaintiff Wilson testified that he believes companies should establish algorithmic bug bounty programs, *id*. at 115, and that he is not aware of any company that has done so, *id*.

127. Online hiring websites already have a general awareness of Plaintiffs and their work. *See* Wilson Depo. Tr. (Exh. 4) at 110.

**PL. RESPONSE:** Undisputed to the extent that the full testimony provided by Plaintiff Wilson was as follows: "The employment companies—they have a general awareness of our existence that we do this work but in both cases they were not aware of any particular follow-on work we were doing or even whether we were conducting follow-on work period." Wilson Depo. at 110 (Def. Ex. 4, ECF No. 53-4).

128. After completing their past algorithm audits of companies, Plaintiffs disclosed their research findings to the companies. *See* Mislove Depo. Tr. (Exh. 3) at 62–66; Wilson Depo. Tr. (Exh. 4) at 72–78.

**PL. RESPONSE:** Undisputed.

129. After disclosing their past research to companies regarding potential online discrimination, none of those companies contacted Plaintiffs and informed Plaintiffs not to conduct algorithm audits in the future. *See* Mislove Depo. Tr. (Exh. 3) at 66; Wilson Depo. Tr. (Exh. 4) at 78.

**PL. RESPONSE:** Undisputed.

130. In both of Plaintiffs' past algorithm audit papers, Plaintiffs suggested future algorithm audits to be conducted. *See* CSCW 2017 Paper (Exh. 1) at PID0032 (Section 6.3, "Future Work"); CHI 2018 Paper (Exh. 2) at PID0010 ("Limitations and Future Work").

**PL. RESPONSE:** Undisputed.

131. Notwithstanding Plaintiffs' past disclosure of research to companies, Plaintiffs believe that future audits of those companies would remain scientifically valid. *See* Mislove Depo. Tr. (Exh. 3) at 125, 127–31; Wilson Depo. Tr. (Exh. 4) at 121–22.

**PL. RESPONSE:** Undisputed.

132. Plaintiffs have no reason to believe that, after they disclosed their past research to the companies, any of those companies took steps to frustrate Plaintiffs' future ability to perform research regarding the companies' websites and/or platforms. *See* Mislove Depo. Tr. (Exh. 3) at 131; Wilson Depo. Tr. (Exh. 4) at 128.

**PL. RESPONSE:** Undisputed.

133. Plaintiffs have not asked companies for permission to perform algorithm audits, and do not intend to do so for any future algorithm audits. *See* Pls.' Resps. to Def.'s First Interrogs. (Exh. 6), Interrog. No. 4; Mislove Decl. (ECF No. 48-2) ¶ 36; Wilson Decl. (ECF No. 48-1) ¶ 36.

**PL. RESPONSE:** Undisputed.

134. Plaintiffs can only speculate as to whether a company would give consent for Plaintiffs to perform an algorithm audit on the company's website and/or platform. *See* Mislove Depo. Tr. (Exh. 3) at 114–15; Wilson Depo. Tr. (Exh. 4) at 111–12.

**PL. RESPONSE:** Undisputed.

135. Private companies, including online employment companies, are willing to work with academics to allow researchers to perform studies using the companies' data, subject to appropriate safeguards. *See* LinkedIn Decl. (Exh. 11) ¶¶ 32–35; Glassdoor Decl. (Exh. 13) ¶¶ 23–27; Facebook Decl. (Exh. 12) ¶ 19; *see also* Pls.' Resp. to Def.'s Second Interrogs. (Exh. 19), Interrog. No. 19.

**PL. RESPONSE:** Disputed to the extent that it is a self-serving statement of opinion by third-party companies about their willingness to allow researchers to perform studies. Disputed to the extent that Defendants suggest any such "studies using the companies' data, subject to appropriate safeguards" are the equivalent of an algorithm audit, including of the type constituting Plaintiffs' research plan at issue in this case.

Dated: May 20, 2019

Respectfully submitted,

/s/ *Esha Bhandari*
Esha Bhandari
Rachel Goodman
Naomi Gilens
American Civil Liberties Union
Foundation
125 Broad St., 18th Floor
New York, NY 10004
Tel: 212-549-2500
Fax: 212-549-2654
ebhandari@aclu.org
rgoodman@aclu.org
ngilens@aclu.org

Arthur B. Spitzer (D.C. Bar No. 235960)
American Civil Liberties Union
of the Nation's Capital
915 15th Street, N.W., Second Floor
Washington, D.C. 20005
Tel: 202-457-0800
Fax: 202-457-0805
aspitzer@acludc.org

*Attorneys for Plaintiffs*