No. 19-783

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE ELEVENTH CIRCUIT

BRIEF OF *AMICI CURIAE* KYRATSO KARAHALIOS, ALAN MISLOVE, CHRISTIAN W. SANDVIG, CHRISTOPHER WILSON, FIRST LOOK MEDIA WORKS, THE AMERICAN CIVIL LIBERTIES UNION, THE AMERICAN CIVIL LIBERTIES UNION OF THE DISTRICT OF COLUMBIA, UPTURN, AND THE KNIGHT FIRST AMENDMENT INSTITUTE IN SUPPORT OF PETITIONER

DAVID COLE
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 5th Street, NW
Washington, D.C. 20005

ARTHUR B. SPITZER
AMERICAN CIVIL LIBERTIES UNION OF THE DISTRICT OF COLUMBIA
915 15th Street, N.W., Second Floor
Washington, D.C. 20005

ESHA BHANDARI
Counsel of Record
BEN WIZNER
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004
(212) 549-2500
ebhandari@aclu.org

Attorneys for Amici Curiae

July 7, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

LEGISLATIVE MATERIALS

INTEREST OF *AMICI CURIAE*[1]

Kyratso "Karrie" Karahalios, Alan Mislove, Christian W. Sandvig, and Christopher "Christo" Wilson are computer scientists and professors at U.S. universities whose academic research includes audit testing and related investigative work to determine whether online platforms and websites treat users differently on the basis of race, age, gender, or other protected class status under civil rights laws.[2] Their research methods may require violating websites' terms of service. Federal prosecutors and some courts have interpreted the Computer Fraud and Abuse Act's prohibition on "exceed[ing] authorized access," 18 U.S.C. § 1030(a)(2)(C), to make it a crime to visit a website in a manner that violates its terms of service or terms of use. *Amici* are therefore concerned that their research, which serves the public interest, could

---

[1] Pursuant to this Court's Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici* and their counsel made a monetary contribution intended to fund the preparation or submission of this brief. Counsel for each party has consented in writing to the filing of this brief of *amici curiae*.

[2] Karrie Karahalios is a Professor of Computer Science, Electrical and Computer Engineering, Information Sciences, Criticism & Interpretive Theory, and Co-director of the Center for People and Infrastructures at the University of Illinois at Urbana-Champaign and a University Scholar there. Alan Mislove is Professor and Associate Dean for Faculty Affairs in the Khoury College of Computer Sciences at Northeastern University. Christian W. Sandvig is the Director of the Center for Ethics, Society, and Computing and the H. Marshall McLuhan Collegiate Professor of Information, Communication and Media at the University of Michigan. Christo Wilson is an Associate Professor in the Khoury College of Computer Sciences at Northeastern University. *Amici*'s affiliations are provided for identification purposes only.

render them criminally liable under the CFAA for violating website terms of service. All four individual *amici* are plaintiffs in a lawsuit against the U.S. Department of Justice in which they challenge the constitutionality of the CFAA to the extent it criminalizes violations of website terms of service. *See Sandvig v. Barr*, No. 16-1368 (JDB), 2020 WL 1494065, at *1 (D.D.C. Mar. 27, 2020).

First Look Media Works, Inc. ("Media Works") is the non-profit journalism arm of First Look Media. First Look Media is a new-model media company devoted to supporting independent voices across all platforms. Media Works, a federally-recognized 501(c)(3) tax-exempt organization, publishes The Intercept, an online news and journalism platform. Its sister company, First Look Productions, Inc., produces and finances content for all screens and platforms including feature films, television, digital series, and podcasts. Media Works is a plaintiff in *Sandvig v. Barr*. Media Works has an interest in ensuring that its journalism, which includes online data journalism, can continue unimpeded by the threat of legal liability under the CFAA.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with nearly two million members and supporters dedicated to defending the principles of liberty and equality embodied in the Constitution. The ACLU is counsel for the plaintiffs in *Sandvig v. Barr*, a lawsuit claiming that the CFAA violates the First Amendment if it criminalizes the plaintiffs' research for violating website terms of service. The ACLU has an interest in ensuring that the nation's civil rights laws, which include protections against discrimination in housing,

employment, and credit, are enforced online, particularly in an era of algorithmic or automated decision-making. The ACLU also has an interest in ensuring that the First Amendment rights of academic researchers and data journalists are not eroded by a construction of the CFAA that would chill critical investigative work about online platforms that is essential to inform the public. The American Civil Liberties Union of the District of Columbia is an affiliate of the national ACLU.

Upturn is a nonprofit organization based in Washington, D.C. that seeks to advance equity and justice in the design, governance, and use of technology. Upturn conducts original research on issues related to technology and civil rights, including in partnership with other *amici* in this brief. Upturn staff are regularly quoted in the national press, and frequently present their research to the U.S. Congress, regulatory agencies, and courts. Upturn has an interest in ensuring that its research, which is essential to fulfilling its mission, is not prohibited by the CFAA for violating terms of service.

The Knight First Amendment Institute at Columbia University ("Institute") is a non-partisan, not-for-profit organization that works to defend the freedoms of speech and the press in the digital age through strategic litigation, research, and public education. The Institute's aim is to promote a system of free expression that is open and inclusive, that broadens and elevates public discourse, and that fosters creativity, accountability, and effective self-government. The Institute is particularly committed to illuminating the forces that are shaping public discourse online. It represents journalists and

researchers who fear legal liability for violating the terms of service of Facebook and other major social media platforms in the course of studying the ways in which these platforms influence public discourse. In an effort to mitigate these fears, the Knight Institute proposed to Facebook that it amend its terms of service to make clear that it will not seek to hold liable under the CFAA those engaged in socially valuable and bona fide journalism and research on the platform. Facebook has rejected that proposal.

SUMMARY OF THE ARGUMENT

The Computer Fraud and Abuse Act ("CFAA") is an anti-hacking law meant to address theft of information, and it should not be construed to prohibit mere violations of written computer use policies, including violations of website terms of service. Any construction of the CFAA that leaves open the possibility of criminal or civil liability when users violate website terms of service will chill critical research and data journalism necessary to hold powerful platforms and websites accountable to the public, including for violations of anti-discrimination laws.

Many important studies that have increased public and governmental understanding of the actions of private companies have required researchers to violate website terms of service. Civil rights enforcement in the twenty-first century relies on audit techniques and basic research methods that bear no resemblance to hacking, but are nonetheless commonly prohibited by exceptionally broad terms of service. Many of these methods are akin to techniques used in offline auditing to enforce civil rights laws. It

will often be necessary for data journalism and research to violate terms of service in order to uncover novel forms of discrimination involving algorithms so as to inform public debate. Researchers and journalists who violate terms of service should not face the threat of criminal and civil liability under the CFAA. To hold otherwise would raise serious constitutional concerns, including due process and First Amendment concerns.

The CFAA makes it a federal crime to "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). Under the Act, to "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter . . . ." *Id.* § 1030(e)(6). Even though the text and purpose of the CFAA, and principles of constitutional avoidance, compel otherwise, courts and federal prosecutors have interpreted the CFAA's prohibition on "exceed[ing] authorized access," *id.* § 1030(a)(2)(C), to make it a crime to visit a website in a manner that violates the terms of service or terms of use (hereinafter "terms of service") established by that website. While this case involves an employee's violation of an employer's computer use policy, the government's reading of the statute necessarily implicates computer use policies that apply to the general public, such as website terms of service. Thus, in *United States v. Nosal*, 676 F.3d 854, 856-58 (9th Cir. 2012) (en banc), the Ninth Circuit declined to read Section 1030(a)(2) to cover violations of an employer's

computer use policy in part because of the implications for millions of internet users subject to website terms of service if it held otherwise.

The government contends that this Court and the public need not fear application of the CFAA to website terms-of-service violations. *See* Brief for the United States in Opposition at 17–18, *Van Buren v. United States*, No. 19-783 (U.S. Mar. 10, 2020). But the Department of Justice has declined to disavow such an interpretation of the CFAA. Notably, the court in *Sandvig* held that the plaintiffs had standing to bring a pre-enforcement challenge to Section 1030(a)(2) as applied to their research, because of the credible threat of prosecution by the federal government for violations of website terms of service. *See Sandvig v. Barr*, No. 16-1368 (JDB), 2020 WL 1494065, at *4–5 (D.D.C. Mar. 27, 2020. The court noted that the Attorney General's 2014 charging guidance does not disavow prosecutions for website terms-of-service violations, and that the DOJ has brought prosecutions for terms-of-service violations in the past. *See id.* at *5 (citing *United States v. Stevens*, 559 U.S. 460, 480 (2010), for the proposition that the Constitution "does not leave us at the mercy of noblesse oblige" on the part of prosecutors).

Researchers and data journalists have reason to fear CFAA liability for violations of website terms of service. While some have taken on that risk to conduct important studies, the CFAA has made this work more difficult, and other researchers have undoubtedly been chilled by the threat of federal criminal liability. This Court should make clear that

the CFAA does not cover violations of website terms of service, thereby enabling critical research in the public interest.

ARGUMENT

I. ONLINE AUDIT TESTING AND RESEARCH ARE NECESSARY TO UNCOVER DISCRIMINATION, ENFORCE CIVIL RIGHTS LAWS, AND INFORM THE PUBLIC ABOUT THE ACTIONS OF POWERFUL PLATFORMS.

A. The need for online civil rights testing and research.

Increasingly, some of the most important decisions that shape people's lives are mediated by algorithms and data in online settings. Discriminatory practices in housing, credit, and employment are often replicated, and in some instances exacerbated, by internet services. Not long ago, many of these discriminatory decisions were made only after someone went physically to a bank, a realtor, or a job fair. Today, these activities have largely migrated online. Accordingly, if the promise of our civil rights laws are to be realized, we must understand how such online services operate.

Consumers routinely apply for loans online, which are often underwritten using nontraditional sources of data. Job-seekers apply for employment using a range of websites and mobile applications, which may use algorithms to rank candidates who are shown to employers. Prospective tenants are regularly evaluated by screening software programs. And sophisticated advertising technology can skew political and other messages that are shown to users along race and

gender lines, even without an advertiser's knowledge. *See infra* note 10. In each of these realms, sophisticated algorithms and analytics fundamentally shape people's access to important life opportunities.

There is ample evidence that algorithms enable intentional and unintentional discrimination. *See infra* notes 6–19; *see, e.g.*, Charge of Discrimination, *Sec'y, HUD v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (HUD Mar. 28, 2019. The federal government has repeatedly acknowledged the potential for analytics or algorithmic targeting to result in discrimination against individuals on the basis of their protected class status, such as race, gender, or age. *See* Plaintiffs' Statement of Undisputed Material Facts at ¶ 55, *Sandvig v. Barr*, No. 1:16-cv-1368 (JDB) (D.D.C. March 7, 2019) [hereinafter "SOF"].[3]

In the offline world, researchers and enforcement agencies have long used audit testing to investigate discrimination in housing and employment, and such evidence has facilitated the enforcement of anti-discrimination laws, such as the Fair Housing Act ("FHA"), 42 U.S.C. § 3601 *et seq*., and Title VII of the

---

[3] *See* Exec. Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* 7–10, 13, 15 (2016), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf; Fed. Trade Comm'n, *Big Data: A Tool for Inclusion or Exclusion?*, at iv, 8, 27–28 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Exec. Office of the President, B*ig Data: Seizing Opportunities, Preserving Values*, 45–47, 51–53 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

Civil Rights Act of 1964 ("Title VII"), 42 U.S.C. § 2000e *et seq*., which prohibits discrimination in employment. SOF, *supra* Section I.A, at ¶ 26.[4] One common way to identify discrimination is to pair individuals of different races or genders to pose as similarly situated home- or job-seekers to determine whether they are treated differently. *See* SOF, *supra* Section I.A, at ¶ 28.

In one approach, known as a correspondence test, auditors submit job applications for fictional applicants that vary only with respect to racial or gender signifiers or other protected characteristics. In another approach, the in-person audit study, pairs of real testers apply for jobs, presenting credentials that have been made equal for the purpose of the study. *See* SOF, *supra* Section I.A, at ¶ 33. Both the U.S. Department of Housing and Urban Development ("HUD") and the Equal Employment Opportunity Commission ("EEOC") have long recognized the

[4] U.S. Dep't. of Justice, *Fair Housing Testing Program* (March 5, 2019), https://www.justice.gov/crt/fair-housing-testing-program-1; *Data & Methods: Paired Testing*, Urban Inst., https://www.urbafn.org/research/data-methods/data-analysis/quantitative-data-analysis/impact-analysis/paired-testing (last visited July 2, 2020); *see also, e.g.*, Diane K. Levy et al., *A Paired-Testing Pilot Study of Housing Discrimination Against Same-Sex Couples and Transgender Individuals*, Urban Inst., at ix (2017), https://www.urban.org/sites/default/files/publication/91486/2017.06.27_hds_lgt_final_report_report_finalized_0.pdf.

importance of studies and audit tests to test housing providers and employers for discrimination.[5]

As more housing, employment, and credit-related transactions have moved online, journalists, academics, and other researchers have sought to apply similar methods of testing for bias to online transactions. For example, outcomes-based audit testing examines the outputs or outcomes of decision-making systems governed by an algorithm, and enables researchers to compare the content that is shown to different users. *See* SOF, *supra* Section I.A, at ¶¶ 57–58. Outcomes-based audit testing is a way to determine whether users are experiencing discrimination in transactions covered by civil rights laws on the basis of their protected class status; without such testing, there may be no way to determine whether such discrimination is occurring. *See* SOF, *supra* Section I.A, at ¶¶ 59–60.

Amici Professors Karahalios, Mislove, Sandvig, and Wilson conduct such audits of online platforms to uncover potential discrimination, as does *amicus* Upturn. One example of such a study is the research plan that was considered by the *Sandvig* court.

---

[5] *See, e.g.*, Margery Austin Turner et al., U.S. Dep't of Hous. and Urban Dev., *Housing Discrimination Against Racial and Ethnic Minorities 2012*, at xi, xii (2013), http://www.huduser.gov/portal//Publications/pdf/HUD-514_HDS2012.pdf; U.S. Equal Emp't Opportunity Comm'n, Notice No. 915.002, *Enforcement Guidance: Whether "Testers" Can File Charges and Litigate Claims of Employment Discrimination* (1996), https://www.eeoc.gov/laws/guidance/enforcement-guidance-whether-testers-can-file-charges-and-litigate-claims-employment.

Professors Mislove and Wilson designed a study to determine whether the algorithms used by some hiring websites produce results that discriminate against job seekers by race, gender, or other characteristics. SOF, *supra* Section I.A, at ¶ 62. For example, a hiring website could rank job candidates in search results in a racially disparate manner if the algorithm that determines which results are displayed takes into account factors—gleaned from a user's resume, browsing history, or social networking profiles—that correlate with race. In order to control for confounding variables, the study requires creating fictitious profiles for fictitious job seekers, who vary along the attributes of race, gender, or age, and comparing their rankings in a list of candidates for fictitious jobs. If the study shows that candidates with specific attributes are consistently ranked lower (when controlling for other variables), this may indicate that the algorithm being used is discriminatory. SOF, *supra* Section I.A, at ¶¶ 62–83.

These types of studies are necessary to ensure that the move from offline to online transactions does not erode civil rights protections. Researchers who study discrimination online have helped the public, lawmakers, regulators, and companies themselves understand how new technologies and uses of data can result in discrimination. They have measured racial gaps in rental acceptances on a major housing

website,[6] prompting lawsuits and reforms.[7] They have exposed biases in facial recognition technologies,[8] paving the way for new policies and temporary bans on the sale of such technology to the police.[9] They have measured racial discrimination in the targeting and delivery of online advertisements,[10] influencing legal settlements and prompting new corporate practices.[11]

---

[6] *See, e.g.*, Benjamin Edelman et al., *Racial Discrimination in the Sharing Economy: Evidence From a Field Experiment*, 9 Am. Econ. J. Applied Econ. 1, 1-3 (2017), https://www.aeaweb.org/articles?id=10.1257/app.20160213.

[7] *An Update on Airbnb's Work to Fight Discrimination*, Airbnb Newsroom (Sep. 10, 2019), https://news.airbnb.com/an-update-on-airbnbs-work-to-fight-discrimination/; Olivia Carville, *Airbnb Agrees to Give Host Data to NYC in Settlement*, Bloomberg (June 12, 2020), https://www.bloomberg.com/news/articles/2020-06-12/airbnb-settles-lawsuit-with-nyc-over-providing-host-data (updated June 15, 2020).

[8] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparaties in Commercial Gender Classification*, 81 Proc. Machine Learning Res. 1, 1–2 (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[9] *State Facial Recognition Policy*, Electronic Privacy Info. Ctr., https://epic.org/state-policy/facialrecognition/ (last visited July 2, 2020).

[10] Latanya Sweeney, *Discrimination in Online Ad Delivery*, 11 ACM Queue 1, 10–13 (2013), https://dl.acm.org/doi/pdf/10.1145/2460276.2460278?download=true; Muhammad Ali et al., Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging 1 (Dec. 17, 2019) (unpublished manuscript) https://arxiv.org/abs/1912.04255; Piotr Sapiezynski et al., Algorithms That "Don't See Color": Comparing Biases in Lookalike and Special Ad Audiences 1–2 (Dec. 17, 2019) (unpublished manuscript), https://arxiv.org/abs/1912.07579.

[11] *Facebook Settlement*, Nat'l Fair Housing Alliance, https://nationalfairhousing.org/facebook-settlement/ (last visited July 2, 2020); Erin Egan, *Improving Enforcement and Promoting*

They have tested voter registration systems,[12] helping to inform security improvements that will protect democratic processes.[13] And they have investigated and participated in policy discussions in a range of other areas, such as payday lending,[14] price discrimination,[15] educational redlining,[16] and insurance underwriting.[17] Regulatory bodies, including HUD, have brought enforcement actions against private parties for discrimination in online

---

Diversity: Updates to Ethnic Affinity Marketing, Facebook (Nov. 11, 2016), https://about.fb.com/news/2016/11/updates-to-ethnic-affinity-marketing/.

[12] Latanya Sweeney et al., *Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections*, Tech. Sci. (2017), https://techscience.org/a/2017090601/.

[13] Max Weiss, *Deepfake Bot Submissions to Federal Public Comment Websites Cannot Be Distinguished from Human Submissions*, Tech. Sci. (2019), https://techscience.org/a/2019121801/.

[14] Upturn, *Led Astray: Online Lead Generation and Payday Loans* 1–6 (2015), https://www.upturn.org/static/reports/2015/led-astray/files/Upturn_-_Led_Astray_v.1.01.pdf.

[15] Jennifer Valentino-DeVries et al., *Websites Vary Prices, Deals Based on Users' Information*, Wall Street J. (Dec. 24, 2012), https://www.wsj.com/articles/SB10001424127887323777204578189391813881534; Keyon Vafa et al., *Price Discrimination in The Princeton Review's Online SAT Tutoring Service*, Tech. Sci. (2015), https://techscience.org/a/2015090102/.

[16] Student Borrower's Prot. Ctr., *Educational Redlining* 6–7 (Feb. 2020), https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf.

[17] Consumer Fed'n of Am., *Major Auto Insurers Charge Higher Rates to High School Graduates and Blue Collar Workers* (July 22, 2013), https://consumerfed.org/pdfs/auto-insurers-charge-higher-rates-high-school-grads-blue-collar-workers.pdf.

advertising,[18] after independent investigations revealed the problem.[19]

In short, online research and data journalism is critical to ensuring that discrimination can be detected so that employers, landlords, bankers, public agencies, and the general public are informed and can respond appropriately.

B. The chilling effect of restrictive terms of service.

The research and data journalism described above requires interacting with websites, mobile applications, and other kinds of internet services. As a result, researchers' efforts are almost always subject to various unilaterally imposed terms of service.[20] A snapshot survey of major recruiting websites, tenant screening services, digital financial services, and advertising platforms shows just how restrictive these terms can be. Many sites prohibit the use of "inaccurate or incomplete information"[21] (thus prohibiting the

---

[18] *See*, *e.g.*, Charge of Discrimination, *Sec'y, HUD v. Facebook, Inc.*, FHEO No. 01-18-0323-8 (HUD Mar. 28, 2019).

[19] Julia Angwin et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, ProPublica (Nov. 21, 2017), https://www.propublica.org/article/facebook-advertising-discrimination-housing-race-sex-national-origin.

[20] Although *amici* focus on website terms of service, they note that researchers and journalists are subject to terms of service on a host of internet-connected platforms, including mobile applications, for which the same concerns apply.

[21] *See*, *e.g.*, *User Agreement*, LinkedIn, https://www.linkedin.com/legal/user-agreement (last visited July 2, 2020) ("To use the Services, you agree that. . . you will only have only one LinkedIn

creation of tester accounts or fictitious user profiles that vary along one defined attribute); the sharing of log-in information (which is often necessary for collaboration among researchers);[22] the use of automated means to obtain information, such as scraping, critical to efficient testing;[23] or any attempt

---

account, which must be in your real name . . . ."); *Upstart Website Terms of Use*, Upstart, https://www.upstart.com/terms (last visited July 2, 2020) ("When you register, become an investor, or apply for a loan, you agree to provide current, complete, and accurate information about yourself."); *Indeed General Terms of Service*, Indeed, https://www.indeed.com/legal?hl=en&redirect=true#tos (last visited July 2, 2020) ("Using or providing any false, fake, or fictitious name or contact information in connection with the Site is grounds for immediate termination of your Indeed account and ability to use the Site.").

[22] *See*, *e.g.*, *Use of the Services*, ZipRecruiter, https://www.ziprecruiter.com/terms#s1 (last visited July 2, 2020) ("Additionally, you agree that: (i) you will not share log-in credentials and account information with third parties . . . ."); *Terms of Use*, Monster, https://www.monster.com/inside/terms-of-use (last visited July 2, 2020) ("All Monster Users agree to not. . . share with a third party any login credentials to any Monster Site . . . ."). *Terms of Service*, Facebook, https://www.facebook.com/terms.php (last visited July 2, 2020) ("[Y]ou must . . . [n]ot share your password, give access to your Facebook account to others, or transfer your account to anyone else (without our permission).").

[23] *See*, *e.g.*, *Terms of Use*, LendingClub, https://www.lendingclub.com/legal/terms-of-use (last visited July 2, 2020) ("Without our prior consent, you may not. . . engage in the practices of 'screen scraping,' 'database scraping' or any other activity with the purpose of obtaining content or other information . . . ."); *Terms of Use*, Vigilant Biosciences, https://vigilantbiosciences.com/terms-of-use/ (last visited July 2, 2020) ("You agree not to engage in any of the following prohibited activities: (i) copying, distributing, or disclosing any part of the Website in any medium, including without limitation by any automated or non-

to understand the mechanisms underlying the service.[24] Some disallow any uses not specifically contemplated by the internet service.[25] These restrictions often amount to an effective prohibition of research. As a result, much internet civil rights research requires violations of terms of service.

Because of the potential for terms of service violations to be considered "exceed[ing] authorized

---

automated 'scraping'; (ii) using any automated system, including without limitation 'robots,' 'spiders,' 'offline readers,' etc. . . ."); *Service Agreement*, Hire Vue, https://www.hirevue.com/company/service-agreement (last visited July 2, 2020) ("Buyer shall not, and shall prevent its Authorized Users from using the Platform to. . . (vi) access all or any portion of the Platform by means of any crawler, scraper, bot, spider, or any other similar script or automated process . . . .").

[24] *See*, *e.g.*, *Legal*, Core Logic, https://www.corelogic.com/legal.aspx (last visited July 2, 2020) ("You agree that you will not attempt to modify, adapt, reverse engineer, decompile, translate or disassemble any portion of the Services or otherwise attempt to derive the source code or underlying ideas, programs or algorithms associated with the Services."); *Propertyware and On-Site Screening Services Agreement*, RealPage https://www.realpage.com/pw-screening-services/ (last visited July 2, 2020) ("Subscriber shall not use the Scores for model development or model calibration, and shall not reverse engineer the Scores.").

[25] *See*, *e.g.*, *Propertyware and On-Site Screening Services Agreement, supra* note 24 ("Subscriber certifies . . . that they shall order Information and shall use Information solely for the following permissible purposes: to determine the eligibility (a) for tenancy of persons or businesses from whom Subscriber has accepted a signed lease application relating to tenancy at the Property, or (b) of a person who has applied in writing to serve as a guarantor of such a lease transaction (collectively, the 'Permissible Purposes' and each, individually, a 'Permissible Purpose'); and (ii) solely for Subscriber's one-time use.").

access" under the CFAA, researchers and journalists who choose to undertake this important work must risk liability, even though their behavior does not constitute hacking or theft of information, the evils targeted by the CFAA. *Amicus* Upturn is acutely aware of this legal risk and has sought legal advice to manage it. It has struggled to secure research collaborations because of fears of legal liability. For example, one promising research opportunity with a major university about hiring technology recently fell through because of concerns about website terms of service. The *amici* who are plaintiffs in *Sandvig v. Barr* brought a pre-enforcement challenge to eliminate the threat of prosecution under the CFAA for violations of terms of service in the course of their proposed research. And, in some cases, the chilling effects of the CFAA have resulted in important research being left undone.[26]

II. THE CFAA SHOULD NOT BE CONSTRUED TO COVER VIOLATIONS OF COMPUTER USE POLICIES, INCLUDING WEBSITE TERMS OF SERVICE.

The text, purpose, and legislative history of the CFAA show that 18 U.S.C. § 1030(a)(2)(C) is properly

---

[26] D. Victoria Baranetsky, *Data Journalism and the Law*, Tow Ctr. for Dig. Journalism (Sep. 19, 2018), https://www.cjr.org/tow_center_reports/data-journalism-and-the-law.php ("No journalists to date have been sued or prosecuted under the Computer Fraud and Abuse Act, but there's evidence that stories have been hindered or held from publication for the threat of penalty."); Ellen Nakashima, *First Amendment Advocates Urge Change in Facebook Platform Rules*, Wash. Post (Aug. 7, 2018), https://www.washingtonpost.com/world/national-security/first-amendment-advocates-urge-change-in-facebook-platform-rules/

read to prohibit specific forms of data theft. Congress initially meant to protect government and corporate computers from behavior that is analogous to breaking and entering and then stealing information—*i.e.*, hacking. *See* H.R. Rep. No. 98-894, at 20 (1984) (stating that "Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer" such that "the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense"); *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1000 (9th Cir. 2019), *petition for cert. filed*, No. 19-1116 (U.S. Mar. 9, 2020) ("The CFAA was enacted to prevent intentional intrusion onto someone else's computer—specifically, computer hacking."); *United States v. Valle*, 807 F.3d 508, 526 (2d Cir. 2015) (noting "statute's principal purpose of addressing the problem of hacking. . . .").

When enacted, the CFAA applied to only "a narrow range of computers—namely, those containing national security information or financial data and those operated by or on behalf of the government." *hiQ*

2018/08/06/ddaa4180-99dc-11e8-8d5e-c6c594024954_story.html; Surya Mattu & Kashmir Hill, *Facebook Wanted Us to Kill This Investigative Tool*, Gizmodo (Aug. 7, 2018), https://gizmodo.com/facebook-wanted-us-to-kill-this-investigative-tool-1826620111; Letter from Alex Stamos et al. to Congress and Members of the Senate and House Committees on the Judiciary (Aug. 1, 2013), https://www.eff.org/files/dc_bh_letter_f4.pdf ("[T]he mere risk of litigation or a federal prosecution is frequently sufficient to induce a researcher . . . to abandon or change a useful project. Some of us have jettisoned work due to legal threats or fears.").

Labs, 938 F.3d at 1001. In 1996, Congress expanded the CFAA to cover "protected computer[s]," S. Rep. 104-357, at 2 (1996), which includes websites designed for public interaction on the internet. *See Nosal*, 676 F.3d at 859–60. However, the development of the modern internet over time has led to applications of the CFAA that have unmoored it from its initial purpose and generated disagreement among courts and commentators. *See* Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1154 (2016) [hereinafter Kerr, *Norms*] (noting the CFAA interpretive problems stemming from the fact that the "[i]nternet and its technologies are new . . . ."). As a statute created to focus on theft from computers and back-end closed systems, it has become a poor fit for exchanges of information over the internet. Accordingly, the Ninth Circuit has held that there is a "serious question" whether access to public information on a website can ever be "without authorization." *hiQ Labs*, 938 F.3d at 1000 ("The 1984 House Report on the CFAA explicitly analogized the conduct prohibited by section 1030 to forced entry . . . ."); *see also* Kerr, *Norms* at 1164 ("[A] website owner necessarily assumes the risk that information published on the Web will be found.").

Section 1030(a)(2)(C) of the CFAA specifically deals with prohibited means of obtaining information from a protected computer. However, the prohibition on "exceed[ing] authorized access" to a protected computer is at best ambiguous as to whether it includes violations of written computer use policies, as opposed to violations of technological access barriers, such as authentication gates. *See Sandvig*, 2020 WL 1494065, at *12–13. Section 1030(a)(2)(C) does not on its face tell readers that visiting a website in a manner

that violates its terms of service is prohibited, for example.

Moreover, interpreting "exceeds authorized access" in Section 1030(a)(2) to cover violations of written computer use policies, including website terms of service, is contrary to Congress's purpose. The language is meant to cover situations where an insider, such as an employee, has access to certain information but improperly accesses other information through behavior that constitutes hacking to steal information—which could include bypassing authentication requirements or stealing someone else's authentication credentials. For the same reasons that the phrase "without authorization" should be construed as limited to hacking, so, too, "exceeds authorized access" should also be so limited. Similarly, "not entitled so to obtain" in the definition of "exceeds authorized access," 18 U.S.C. § 1030(e)(6), means "not entitled to steal," concomitant with the understanding of "authorized" in Section 1030. *See Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 194–95 (D.D.C. 2017) (the "most 'sensible reading of 'entitled' is as a synonym for 'authorized'") (quoting *Nosal*, 676 F.3d at 857). The Second Circuit, in *Valle*, quoted the Ninth Circuit in *Nosal* and stated "it is possible to read [Section 1030] as applying to hackers: '[W]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." 807 F.3d at 524 (alteration in original) (quoting *Nosal*, 676 F.3d at 858). The Ninth Circuit emphasized that "[i]f Congress wants to incorporate

misappropriation liability into the CFAA, it must speak more clearly." *Nosal*, 676 F.3d at 863. The CFAA is not a "sweeping Internet-policing mandate." *Id.* at 858.

Given that Section 1030(a)(2)(C) is, at best, ambiguous regarding its application to violations of written terms, this Court should be guided by principles of constitutional avoidance in interpreting it. Several courts have considered the grave constitutional concerns that would arise were the CFAA interpreted to criminalize violations of every website's computer use policies. *Nosal* noted due process concerns regarding notice to users of which conduct is criminal if terms-of-service violations are covered, *see* 676 F.3d at 861, given the host of trivial terms-of-service violations that internet users commit regularly (such as letting close friends and relatives access their online accounts). Indeed, website terms of service are often arcane and voluminous, subject to change at any time, and without any requirement of notice to users. They are seldom read. *See Nosal*, 676 F. 3d at 860; *Sandvig*, 2020 WL 1494065, at *10. Construing the CFAA to criminalize violations of ever-shifting, private, unilaterally imposed terms of service that virtually no one reads would present serious due process problems, and supports a narrow construction of the statute here to exclude terms-of-service violations.

The court in *Sandvig* also weighed the "considerable nondelegation issues" that arise from criminalizing violations of website terms of service. *Sandvig*, 2020 WL 1494065, at *13. The court considered that because the analogy between the internet and real property is "not perfect," it is

therefore not appropriate to equate Section 1030(a)(2) to laws allowing property owners to exclude others. Rather, "[c]riminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature." *Id*. at *10. As the examples provided here show, *see supra* Section I.B., terms of service can be broad and vague, with no limiting principle on the behavior private parties can proscribe.

Construing the CFAA to cover violations of website terms of service would also raise First Amendment problems. For example, many websites prohibit providing any false information, but criminalizing any and all false information provided on the internet—including in the course of audit testing—would be unconstitutional. False speech cannot be criminalized where it does not cause harm. *United States v. Alvarez*, 567 U.S. 709, 722–23 (2012). But as courts have noted, many terms-of-service violations involving false information do not cause the types of legally cognizable harm identified in *Alvarez*. *See Nosal*, 676 F. 3d at 861–62 (discussing lies told on dating websites, such as describing yourself as "tall" when you are "short," that could be rendered criminal under the CFAA if terms-of-service violations are covered). Another consequence could be the criminalization of parody or pseudonymous social media profiles regardless of harm. There is no question that Section 1030(a)(2), if applied to terms-of-service violations, would not distinguish between online speech that causes harm and that which does not, because terms of service are not required to make such a distinction.

The court in *Sandvig* considered the plaintiffs' claims that the First Amendment protects their

misrepresentations in the course of online audit testing. It applied the canon of constitutional avoidance in interpreting the scope of Section 1030(a)(2), noting that "[i]f the Court were to conclude that plaintiffs' terms-of-service violations *do* violate the CFAA, then it would have to decide whether prosecuting them for such actions violates the First Amendment. As the Court previously observed, it 'need not determine whether plaintiffs' constitutional arguments would actually win the day,' but rather 'whether one reading presents a significant risk that [constitutional provisions] will be infringed.' Plaintiffs' First Amendment challenge raises such risks and thus weighs in favor of a narrow interpretation under the avoidance canon." *Sandvig*, 2020 WL 1494065, at *11 (citations and quotation marks omitted).

If the CFAA prohibits journalism and research when it violates terms of service, the public will be deprived of essential information about the ways in which increasingly powerful online platforms can contribute to discrimination. This will have dire consequences for the ability of public and private actors to enforce existing civil rights laws and to advocate for new ones. This chilling effect on protected journalism and research will also implicate First Amendment rights.

To avoid these constitutional concerns, and to interpret the text in line with Congressional purpose, this Court should hold that the CFAA does not impose liability for violations of computer use policies, including website terms of service.

CONCLUSION

The judgment of the Eleventh Circuit should be vacated because Section 1030(a)(2) of the Computer Fraud and Abuse Act should not be construed to criminalize violations of computer use policies alone, including website terms of service.

Respectfully submitted,

ESHA BHANDARI
Counsel of Record
BEN WIZNER
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street
New York, NY 10004
ebhandari@aclu.org
212-549-2500

DAVID D. COLE
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
915 5th Street, NW
Washington, D.C. 20005

ARTHUR B. SPITZER
AMERICAN CIVIL LIBERTIES UNION
OF THE DISTRICT OF COLUMBIA
915 15th Street, N.W., Second Floor
Washington, D.C. 20005

Attorneys for Amici Curiae

July 7, 2020