

## Uncovering Online Discrimination When Faced with Legal Uncertainty and Corporate Power

Esha Bhandari

Imagine an increasingly common scenario: you apply for a job through an online platform that connects employers to jobseekers. You send your materials into the void and then never hear back. You might assume this was because you didn't meet the criteria for the job or because the company was overwhelmed with applicants who did. You might be perturbed to learn that a human never reviewed your application—a computer determined you weren't qualified—but perhaps you're resigned to that reality. But how would you react if you knew that the jobs platform used a ranking algorithm that systematically ranked women lower than equally qualified men applying for the job, and that's why the employer never interviewed you?<sup>1</sup>

As upsetting as it would be to learn that you were discriminated against in the job-seeking process, it is in fact more likely that you would never find that information out at all. Most people using websites and mobile applications have no information about the hidden automated processes that are used to determine who gets certain opportunities online. Companies that run platforms don't generally reveal details about the algorithms they use or whether those algorithms discriminate on the basis of race, gender, age, disability, or other protected class status under civil rights laws—including because they have self-interested reasons not to voluntarily provide information that could render them liable for discrimination. Uncovering this type of discrimination therefore often requires some form of adversarial testing by researchers or journalists, using techniques designed to assess the workings of automated processes online.

But there is a barrier to a robust environment of online accountability research and journalism. The United States continues to have an uncertain legal environment for adversarial civil rights testing and research online due to outdated computer crime laws that fail to accommodate and encourage digital-era research techniques.<sup>2</sup> These laws are focused on antiquated notions of “hacking” into closed computer systems and do not map neatly onto the online environment of today. Furthermore, the legal environment has given outsize power to corporations to control how and when their actions are evaluated for discrimination. Corporate terms of service, which are one-sided and drafted with the company’s interests in mind, often prohibit using the techniques necessary for adversarial testing. The US Supreme Court’s recent decision in *Van Buren v. United States* has gone a long way to clearing the threat posed by the federal Computer Fraud and Abuse Act (CFAA), a computer crime law that had long created the risk of federal criminal prosecution for those engaged in civil rights testing online in violation of website terms of service.<sup>3</sup> But even with that welcome advance, there remain state laws on the books that could pose a barrier to robust research. And corporate terms of service that are hostile to independent testing and research continue to create ambiguity in a legal landscape sorely in need of clarity.

For every researcher or journalist willing to conduct important research in the face of such uncertainty, there are likely untold numbers of others who would engage in such work but cannot in light of the risks attached—including those very members of communities most likely to be harmed by online discrimination, such as people of color. Others who may be deterred are researchers without tenure or graduate students on student visas, or independent journalists without the backing of a large newsroom with a legal team. Anyone potentially revealing wrongdoing by powerful corporations online must contend with the legal tools that could be used against them. Despite these concerns, there are promising developments in the law. Courts are increasingly recognizing the legitimacy of certain common online research techniques. And federal regulatory bodies are stepping up enforcement of civil rights laws online, which serves to encourage even more research into online discrimination.

This chapter argues that independent research and journalism is needed to address the growing problem of unchecked online discrimination, which is often invisible to the people affected by it. The chapter then examines the legal barriers that computer crime laws such as the CFAA have posed to independent testing of online platforms. It argues that while there have been promising legal developments, further clarity in the law is needed to assure researchers and journalists that they need not fear liability for their work. Lastly, the chapter notes that there are privacy considerations that should inform online research and journalism, and that efforts to address privacy concerns should proceed

alongside efforts to clear away the legal hurdles to independent, adversarial online testing.

### ADDRESSING THE PROBLEM OF ONLINE DISCRIMINATION

The online world, for all its promise of greater access to knowledge and economic opportunities, has also ushered in a new era of discrimination. The structural inequalities of the real world are being replicated online, turbocharged by ubiquitous data collection and surveillance practices. Private companies have amassed vast amounts of data about online user behavior, much of it using methods that have given users no meaningful control over their information. The data can reveal particularly sensitive information about people, including their race, gender, sexual orientation, or disability status. And this sensitive information can, in turn, be used to determine which opportunities people are given.<sup>4</sup> Increasingly, some of the most important decisions that shape people's lives are mediated by algorithms and data in online settings.<sup>5</sup> Long-standing 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 physically went to a bank, a rental company, or a job fair. But today, these activities have largely migrated online. Accordingly, if the promise of our civil rights laws are to be realized, we must understand how these online services—including websites and mobile applications—operate. Only by first uncovering discrimination online can we do something about it, including by robustly enforcing existing federal and state antidiscrimination laws in the digital realm, and designing additional laws and regulations to target new forms of digital-era discrimination.

We are a long way from the time when the internet held the promise of mitigating certain long-standing and persistent structural inequities in society. While early studies of the internet suggested that the anonymity of online transactions would close the gap for women and other groups who were historically discriminated against in the “real world” marketplace, that promise has faded away.<sup>6</sup> Now, corporations have amassed vast amounts of data about individuals, much of it through tracking our online activities. Online interactions are losing much of their anonymity, as tracking technologies allow websites and platforms to access all kinds of information about visitors, including information that may reveal race, gender, age, and sexual orientation.<sup>7</sup> Companies that operate commercial websites have access to massive amounts of data about internet users and can employ algorithms to analyze that data. Such “big data analytics” enables behavioral targeting, meaning that websites can steer individuals toward viewing different content on the internet.<sup>8</sup> Most critically for purposes of civil rights concerns, online targeting allows platforms to steer housing or credit offers or jobs on the basis of protected

class status, such as race, age, or gender.<sup>9</sup> Behavioral targeting opens up vast potential for discrimination against marginalized communities.

The risks of discrimination can arise in a variety of contexts. Online ad targeting, for example, can be used to exclude users from seeing certain ads on the basis of race, gender, age, or other protected characteristics, as well as on the basis of proxies for those categories. Sometimes the ad targeting is done through choices on the part of the advertiser or the platform to select (or exclude) users with particular characteristics.<sup>10</sup> But other times the ad targeting occurs through an ad delivery algorithm or automated system that determines which users should see which ads—and those delivery systems can end up discriminating on the basis of protected characteristics. In the latter cases, ad delivery algorithms can discriminate in who sees an ad because of large skews in underlying metrics that inform the algorithm.<sup>11</sup> For example, an ad delivery system that shows ads to users based on whether they share characteristics with existing employees in a certain industry could replicate the bias in that industry—systematically showing the ad to fewer women and nonbinary people, for example, for technology or engineering jobs because of long-standing underrepresentation in those fields.<sup>12</sup> This discrimination in ad delivery might occur even if the employer is not aware of and does not want such discriminatory ad delivery.<sup>13</sup>

Discrimination in ads online is particularly pernicious because users will rarely, if ever, be aware of what ads they were not shown. In the offline world, a woman might see a job ad for “Men Only” and be able to raise a complaint of discrimination. But online, that same woman might never see the job opportunity that an advertising platform showed only to men, and never know she was discriminated against. After all, we seldom have a way to identify the ads we’re *not* seeing online.<sup>14</sup> That this discrimination is invisible to the excluded user makes it all the more difficult to stop.

Another example of online discrimination is when hiring platforms serve a matching function between employers and jobseekers. These platforms can use automated systems, or algorithms, to rank candidates for jobs, or even to eliminate candidates from eligibility.<sup>15</sup> Individual applicants using such a system might never know why they didn’t get the job, let alone whether the ranking algorithm systematically discriminates against people on the basis of a protected class status. In such cases, even the employers might not know that the platform they are using is discriminating in the candidates it highlights for them.

These examples are not exhaustive, but illustrative of the larger problem of identifying discrimination online, where individual users may not even be aware of the systems that are operating to deny them opportunities. And all of this discrimination has been fueled by business practices in which individuals have had no meaningful choice in the information they give up to online services, nor any control over whether that information ends up in the hands of other companies or potential landlords, realtors, or employers.<sup>16</sup>

These discriminatory practices persist despite increasing enforcement of antidiscrimination laws against online platforms in recent years. Meta (formerly Facebook), for example, has faced multiple lawsuits and federal enforcement action regarding its online ad targeting and delivery system, for violating the federal Fair Housing Act and other civil rights laws, leading to major changes to its ad platform.<sup>17</sup> These lawsuits were enabled by the work of journalists and researchers who uncovered discrimination in the platform's ad system.<sup>18</sup> But despite such recent enforcement actions raising the prospect of potential liability, the industry is slow to change, and there is a need for much more research into a wider variety of platforms and actors in the online ecosystem.<sup>19</sup>

### PROGRESS IN RESOLVING LEGAL BARRIERS TO CIVIL RIGHTS TESTING ONLINE

The problem of rampant and unchecked online discrimination requires robust accountability research and journalism to hold platforms accountable. This type of civil rights testing has long been common in the offline world, and yet online civil rights testing faces unjustified barriers because of an uncertain legal environment. These barriers include open questions about how computer crime laws intersect with common online research techniques, including creating tester accounts with fictitious user information or scraping data. Scraping is a method of collecting information from the internet that generally involves programming automated queries to retrieve content, without using a web browser or application programming interface. Scraping allows for efficient collection of large amounts of information that might be impracticable for someone to record manually.<sup>20</sup>

In the offline world, adversarial testing has long been used to enforce the guarantees of civil rights laws, such as the federal Fair Housing Act, Title VII of the Civil Rights Act (which prohibits discrimination in employment), the Age Discrimination in Employment Act, and the Equal Credit Opportunity Act. A method called audit testing, for example, has long been recognized as a crucial way to uncover racial discrimination in housing and employment. This technique involves pairing individuals of different races to pose as home- or job-seekers to determine whether they are treated differently.<sup>21</sup> A correspondence test can involve auditors submitting two job applications for fictional applicants who vary only with respect to racial or gender signifiers, and comparing results.<sup>22</sup> The law has protected the ability to engage in such misrepresentation in the offline world during the course of civil rights testing, regardless of whether businesses would rather not deal with applicants who are not real.<sup>23</sup>

In the online world, however, conducting the same kind of audit testing generally violates websites' terms of service, which often prohibit providing false information, creating multiple user profiles, or using automated methods of recording the information displayed for different users, such as scraping. Yet there

is often no way to conduct systematic testing of online platforms for discrimination without doing these things—such as creating tester accounts with fictitious user information that varies by gender or race, searching for jobs online through those accounts to see how results differ for each fictional user, and recording those results efficiently through scraping. Some terms of service simply prohibit any uses not specifically allowed by the platform, thereby targeting not any one particular technique but effectively banning all testing whatsoever.<sup>24</sup>

Computer crime laws, most notably the CFAA, have long served as a deterrent to such testing because they could render violations of website terms of service into criminal violations. The CFAA is a federal anti-hacking law from the 1980s that has proven ill-suited to the modern internet. For many years, the federal government and some courts interpreted its prohibition on “exceed[ing] authorized access” to a computer to prohibit visiting a website and violating its terms of service—even though such terms are unilaterally imposed, self-serving conditions written by companies (and largely unread by most internet users).<sup>25</sup> This interpretation risked turning everyday internet behavior, such as using a pseudonym on social media, into a crime.<sup>26</sup> And it meant that anyone conducting adversarial research, journalism, or testing of a platform for discrimination had to worry about whether they could be subject to prosecution or civil liability for going against a company’s terms of service in doing so. Unsurprisingly, some researchers, especially those who are themselves marginalized or vulnerable in the face of legal threats, understandably chose to forgo investigations they might have otherwise undertaken.<sup>27</sup>

This is why the Supreme Court’s decision in 2021 in *Van Buren v. United States* was a welcome step in easing one of the major hurdles to such research. At first glance, the case does not seem obviously related to civil rights enforcement. It concerned a police officer who searched for information about a license plate in a law enforcement database in exchange for money.<sup>28</sup> The officer was criminally charged with “exceed[ing] authorized access” under the CFAA because he violated his employer’s computer use policies. The Supreme Court held that the CFAA should not be read to criminalize violations of computer use policies alone. Instead it should be read to prohibit behavior that is akin to breaking and entering—such as in the course of accessing parts of a computer that someone does not have authority to access at all.<sup>29</sup> By narrowing the scope of the CFAA, the decision has cleared the way for researchers and journalists to use common investigative techniques online without worrying that violating terms of service alone will subject them to liability under the CFAA.

The *Van Buren* decision came after a lower court decision that had explicitly considered the claims of civil rights researchers. The federal district court in *Sandvig v. Barr* held that the CFAA should not be read to criminalize terms of service violations, in a lawsuit brought by academic researchers who argued that they had a First Amendment right to conduct their discrimination testing online, including through creating fictitious tester accounts. Such fictitious accounts would allow the

researchers to test how platforms treat similar users who vary only by a controlled variable, such as race, gender, or age.<sup>30</sup> The court concluded that the CFAA did not apply to barring the researchers' proposed online testing activities, and thus did not need to reach their claim that the First Amendment protected those activities.

Even with the Supreme Court's decision in *Van Buren*, however, questions remain about various legal issues affecting adversarial online discrimination testing. All fifty states have computer crime laws, many of which are analogous to their federal counterpart and have been interpreted consistently with the CFAA.<sup>31</sup> While *Van Buren* should prove persuasive in similarly limiting application of those computer crime laws to violations of terms of service, there remains ambiguity absent definitive constructions of those laws in state courts. And the courts have also been inconsistent on the enforceability of website terms of service in contract, which can also act as a deterrent to research.<sup>32</sup>

There also remain questions about the application of the CFAA and other computer crime laws to research techniques where the threatened liability does not stem from violations of terms of service, but rather from whether the particular research technique might be deemed the equivalent of "breaking and entering" a system (for example, through the use of password sharing for user accounts or bypassing Internet Protocol [IP] address barriers).<sup>33</sup> One of the challenges of adversarial testing online is that platforms may implement technical barriers to prohibit scraping and other common research methods. Platforms might also suspend or remove specific accounts they identify as researcher accounts.<sup>34</sup> While these challenges might inhibit or prevent testing of certain platforms, in other cases they may spur innovation in research techniques, as a result of the adversarial back-and-forth between independent testers and the platforms that seek to shut them out. For this reason, it is important that courts provide more definitive guidance on the types of technical barriers that researchers can bypass without running afoul of computer crime laws that are focused on notions of trespass.

And yet, courts have been slow to address the legality of particular research methods online even as data journalism, online auditing, and other digital-era research methods have adapted to keep pace with the systems they are studying. A recent decision by a federal district court, for example, held that the South Carolina State Conference of the NAACP had stated a First Amendment claim to scrape public housing court records in order to efficiently reach tenants in eviction proceedings to provide them with services to fight those evictions.<sup>35</sup> That decision denying a motion to dismiss the case is one of the few in which courts have explicitly considered the legality of scraping as a research technique, despite the fact that the practice is exceedingly common, both for research and commercial purposes.<sup>36</sup>

Recent caselaw concerning the First Amendment limitations on laws restricting access to agricultural facilities for the purpose of undercover investigations—so called "ag-gag" laws—may prove relevant to securing the right to engage in

online research. Courts have struck down some laws that restrict the ability to record in agricultural facilities, or to provide misleading information about one's intent in gaining access to such facilities, in part because they are targeted only at critics of those facilities.<sup>37</sup> These cases may provide support for the claims of online civil rights testers, particularly because platforms (in a manner similar to agricultural facility owners) often assert rights of property ownership or control to prohibit adversarial researchers from accessing or recording information on their platforms that is available to other users.

Finally, there are, of course, privacy considerations that online civil rights testing, research, or journalism in the public interest must consider. This tension is not new to the digital era—even offline efforts at antidiscrimination testing and research have privacy implications, particularly when they involve collecting sensitive data on protected class status such as race, sexual orientation, or disability. The tensions between individual privacy considerations and the need for research data to advance equality have existed for a long time, and merit special consideration in the digital era. Never before has so much data about so many people been potentially available. With the mission to advance the public good through adversarial platform research also comes a heavy responsibility for the people doing that work. It is beyond the scope of this piece to outline specific policies, ethical guidelines, or security best practices that should be adopted by online civil rights researchers. But others are engaged in that endeavor, which should proceed simultaneously with efforts to clear away legal barriers to such research.<sup>38</sup>

## CONCLUSION

Much of what we know about the world of online discrimination today is thanks to researchers, academics, and journalists who have conducted online testing and research to which the subject companies did not consent. This critically important work must continue in order for the promise of our civil rights laws to be realized online, and in order for us to adapt our laws and policies to the new world of discrimination enabled by the digital era. While the Computer Fraud and Abuse Act has long posed a significant hurdle to online civil rights testing by creating the risk of criminal prosecution for necessary research techniques, the legal environment is shifting slowly in the direction of greater clarity, so that researchers don't have to bear the burden of potential liability for their work that serves the public good.

## NOTES

Thank you to Rachel Goodman and Galen Sherwin for collaborating on developing the ideas reflected in this piece, to Mitra Ebadolahi for her comments, and to Amanda Levendowski for shepherding the project.



1. Such a hypothetical is not fanciful. Amazon stopped developing an automated hiring tool that was demonstrating bias against female job candidates. See Jeffrey Dastin, *Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women*, REUTERS (Oct. 18, 2018), <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>.

2. See, e.g., 18 U.S.C. § 1030 *et seq.* (Computer Fraud and Abuse Act); see generally Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143 (2016) (arguing that courts have struggled to interpret computer trespass laws, with some imposing liability for trivial wrongs such as violating website terms of service).

3. *Van Buren v. United States*, 141 S. Ct. 1648 (2021).

4. See generally Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671 (2016).

5. See generally Safiya Umoja Noble, *ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM* (2018); Virginia Eubanks, *AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR* (2018).

6. See, e.g., Fiona Scott Morton, et al., *Consumer Information and Discrimination: Does the Internet Affect the Pricing of New Cars to Women and Minorities?*, 1 QUANTITATIVE MARKETING AND ECONOMICS 65–92 (2003), <https://doi.org/10.1023/A:1023529910567>.

7. Characteristics such as race, or perceived race, can be inferred even when users do not explicitly provide that information. Pioneering early studies have demonstrated the persistence of racial bias online. See, e.g., Latanya Sweeney, *Discrimination in Online Ad Delivery*, 11 ACM QUEUE 1 (2013); Benjamin Edelman, et al., *Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment*, 9 AM. ECON. J. APPLIED ECON. 1 (2017).

8. Beginning as far back as 2014, the federal government released a series of reports highlighting the discriminatory potential in the era of “big data.” See Exec. Office of the President, *Big Data: Seizing Opportunities, Preserving Values* (2014); Fed. Trade Comm’n, *Big Data: A Tool for Inclusion or Exclusion?* (2014); Exec. Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (2016).

9. See, e.g., Samuel Gibbs, *Women Less Likely to Be Shown Ads for High-Paid Jobs on Google, Study Shows*, THE GUARDIAN (July 8, 2015), <https://www.theguardian.com/technology/2015/jul/08/women-less-likely-ads-high-paid-jobs-google-study>; Byron Spice, *Questioning the Fairness of Targeting Ads Online*, CARNEGIE MELLON UNIVERSITY NEWS (July 7, 2015), <https://www.cmu.edu/news/stories/archives/2015/july/online-ads-research.html>.

10. See Julia Angwin, et al., *Facebook (Still) Letting Housing Advertisers Exclude Users by Race*, PROPUBLICA (Nov. 21, 2017).

11. See Muhammad Ali, et al., *Discrimination through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes*, Proceedings of the ACM on Human-Computer Interaction (2019), available at arXiv:1904.02095.

12. See Rachel Goodman, *Why Amazon's Automated Hiring Tool Discriminated against Women*, ACLU NEWS AND COMMENTARY (Oct. 12, 2018), <https://www.aclu.org/blog/womens-rights/womens-rights-workplace/why-amazons-automated-hiring-tool-discriminated-against>.

13. Piotr Sapiezynski, et al., *Algorithms That “Don't See Color”: Comparing Biases in Lookalike and Special Ad Audiences*, Proceedings of the 2022 AAAI/ACM Conference on AI, Ethics, and Society (Dec. 17, 2019), <https://arxiv.org/abs/1912.07579>.

14. Aaron Rieke and Miranda Bogen, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, UPTURN (Dec. 10, 2018), <https://www.upturn.org/work/help-wanted/> (“The complexity and opacity of digital advertising tools make it difficult, if not impossible, for aggrieved jobseekers to spot discriminatory patterns of advertising in the first place”).

15. *Id.*

16. See Rick Edmonds, *People Don't Want to Trade Privacy for Targeted Ads*, POYNTER (Jan. 14, 2016), <https://www.poynter.org/business-work/2016/people-dont-want-to-trade-privacy-for-targeted-ads>.

17. See US Dep't of Justice, *Justice Department and Meta Platforms Inc. Reach Key Agreement as They Implement Groundbreaking Resolution to Address Discriminatory Delivery of Housing Advertisements* (Jan. 9, 2023), <https://www.justice.gov/opa/pr/justice-department-and-meta-platforms-inc-reach-key-agreement-they-implement-groundbreaking>; Ariana Tobin & Ava Kofman, *Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising*, PROPUBLICA (June 22, 2022), <https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement>; US Dep't of Justice, *Justice Department Secures Groundbreaking Settlement Agreement with Meta Platforms, Formerly Known as Facebook, to Resolve Allegations of Discriminatory Advertising* (June 21, 2022), <https://www.justice.gov/opa/pr/justice-department-secures-groundbreaking-settlement-agreement-meta-platforms-formerly-known>; Esha Bhandari & Galen Sherwin, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU NEWS AND COMMENTARY (Mar. 19, 2019), <https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping>.

18. Ariana Tobin & Ava Kofman, *Facebook Finally Agrees to Eliminate Tool That Enabled Discriminatory Advertising*, PROPUBLICA (June 22, 2022), <https://www.propublica.org/article/facebook-doj-advertising-discrimination-settlement>.

19. See Jeremy B. Merrill, *Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads*, THE MARKUP (Feb. 11, 2021), <https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads>.

20. See Andrew Sellers, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 4 B.U. J. Sci. & Tech. L. 372, 372, 381–88 (2018).

21. See, e.g., US Dep't of Housing and Urban Development, Office of Policy Development and Research, *Housing Discrimination against Racial and Ethnic Minorities* 2012 xi, [http://www.huduser.gov/portal/Publications/pdf/HUD-514\\_HDS2012.pdf](http://www.huduser.gov/portal/Publications/pdf/HUD-514_HDS2012.pdf) (government-sponsored study used paired-testing methodology in twenty-eight metropolitan areas and found that Black, Latino, and Asian testers were told about and shown fewer homes than white testers); US Dep't. of Justice, *Fair Housing Testing Program* (Mar. 5, 2019), <https://www.justice.gov/crt/fair-housing-testing-program-1>; Diane K. Levy, et al., *A Paired-Testing Pilot Study of Housing Discrimination against Same-Sex Couples and Transgender Individuals*, URBAN INST. (2017), [https://www.urban.org/sites/default/files/publication/91486/2017.06.27\\_hds\\_lgt\\_final\\_report\\_report\\_finalized\\_o.pdf](https://www.urban.org/sites/default/files/publication/91486/2017.06.27_hds_lgt_final_report_report_finalized_o.pdf).

22. See Devah Pager & Bruce Western, *Identifying Discrimination at Work: The Use of Field Experiments*, 68 J. OF SOCIAL ISSUES 221, 223 (2012).

23. See *Havens Realty Corp v. Coleman*, 455 U.S. 363, 373 (1982) (testers have standing to sue for Fair Housing Act violations). Courts regularly acknowledge the importance of testing to enforce the Fair Housing Act, see, e.g., *Smith v. Pac. Properties & Dev. Corp.*, 358 F.3d 1097, 1102 (9th Cir. 2004); *Richardson v. Howard*, 712 F.2d 319, 321 (7th Cir. 1983); and Title VII, see, e.g., *Kyles v. J.K. Guardian Sec. Servs., Inc.*, 222 F.3d 289, 292 (7th Cir. 2000); *Fair Employment Council of Greater Washington, Inc. v. BMC Marketing Corp.*, 28 F.3d 1268, 1277–78 (D.C. Cir. 1994).

24. See, e.g., Esha Bhandari & Rachel Goodman, *Data Journalism and the Computer Fraud and Abuse Act: Tips for Moving Forward in an Uncertain Landscape*, Northwestern Computation and Journalism Symposium (2017), <https://cj2017.northwestern.edu/documents/data-journalism-cj2017-paper-23.pdf>; Alex Abdo, *Facebook Is Shaping Public Discourse. We Need to Understand How*, THE GUARDIAN (Sept. 15, 2018), <https://www.theguardian.com/commentisfree/2018/sep/15/facebook-twitter-social-media-public-discourse> (discussing terms of service restrictions on Facebook and Twitter that impede digital journalism and research).

25. The Ninth Circuit Court of Appeals was one notable court to hold that the CFAA does not encompass mere violations of computer use policies. See *United States v. Nosal*, 676 F.3d 854 (9th Cir.

2012); see also Uri Benoliel & Shmuel I. Becher, *The Duty to Read the Unreadable*, 60 B.C. L. REV. 2255, 2296 (2019) (noting that the unilaterally imposed terms of most online services “permit online firms to contract with millions of users, with no negotiation, and without verifying that the contract was read [let alone understood]”).

26. The federal government prosecuted someone under the CFAA for lying about her age to create a fictitious account on MySpace, in violation of that website’s terms of service. Although the defendant allegedly used the account to cyberbully a minor, who subsequently died by suicide, the CFAA misdemeanor charges were for terms of service violations alone. The district court overturned the jury’s guilty verdicts on those charges. See *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). For a critique of CFAA reform advocacy for failing to recognize that overcriminalization of everyday behavior is not a phenomenon limited to the Internet, see Kendra Albert, *Not a Crime: The CFAA and Respectability Politics*, TECH POLICY PRESS (Jan. 3, 2022), <https://techpolicy.press/not-a-crime-the-cfaa-and-respectability-politics>.

27. D. Victoria Baranetsky, *Data Journalism and the Law*, TOW CENTER FOR DIG. JOURNALISM (Sept. 19, 2018), [https://www.cjr.org/tow\\_center\\_reports/data-journalism-and-the-law.php](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*, WASHINGTON POST (Aug. 7, 2018), [https://www.washingtonpost.com/world/national-security/first-amendment-advocates-urge-change-in-facebook-platform-rules/2018/08/06/ddaa4180-99dc-11e8-8d5e-c6c594024954\\_story.html](https://www.washingtonpost.com/world/national-security/first-amendment-advocates-urge-change-in-facebook-platform-rules/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](https://www.eff.org/files/dc_bh_letter_f4.pdf) (“The 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”).

28. *Van Buren v. United States*, 141 S. Ct. 1648, 1653 (2021). Although the police officer was the subject of a sting operation, he believed he was conducting the search for a friend to be able to identify a woman he had recently met, with no seeming regard for her safety.

29. *Id.*, at 1661–62.

30. See *Sandvig v. Barr*, 451 F. Supp. 3d 73 (D.D.C. 2020). The author of this piece was counsel for the plaintiffs in *Sandvig*.

31. See National Conference of State Legislatures, *Computer Crime Statutes* (May 4, 2022), <https://www.ncsl.org/technology-and-communication/computer-crime-statutes#:~:text=All%2050%20states%2C%20Puerto%20Rico,and%20ransomware%2C%20as%20shown%20below>; see also *Facebook, Inc. v. Power Ventures*, 844 F.3d 1058, 1069 (9th Cir. 2016) (noting that the analysis of the reach of California’s computer crimes law, the Comprehensive Computer Data Access and Fraud Act, Penal Code § 502, is similar to the CFAA).

32. See *hiQ Labs v. LinkedIn*, No. 17-cv-03301-EMC (N.D. Cal. Nov. 4, 2022) (finding hiQ Labs liable for breach of contract when it scraped LinkedIn’s public facing site in violation of LinkedIn’s terms of service).

33. See, e.g., *Facebook v. Power Ventures*, 844 F.3d 1058 (9th Cir. 2016); see also Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1167–69 (2016).

34. In August 2021, Facebook suspended the accounts of NYU researcher Laura Edelson and two colleagues after the NYU team’s research revealed that over half of the US political ads on Facebook in a particular period violated the platform’s own rules on transparency. See Mark Scott, *Facebook’s Attempt to Ban Academics Runs Into Trouble*, POLITICO (Aug. 5, 2021), <https://www.politico.eu/article/facebook-nyu-laura-edelson-political-ads>. This incident led to the formation of the Coalition for Independent Technology Research, a group of organizations and individuals across civil society,

journalism, and academia committed to advancing independent research into technology companies. See Coalition for Independent Technology Research, *Founding Document* (Oct. 12, 2022), <https://independenttechresearch.org/coalition-for-independent-technology-research-founding-document>.

35. *NAACP v. Kohn*, No.: 3:22–01007–MGL (D.S.C. Jan. 10, 2023). The author of this piece is counsel for the plaintiff in *Kohn*.

36. The litigation between LinkedIn and hiQ has been significant in developing the law around scraping, albeit in a context involving commercial scraping for business purposes. The Ninth Circuit held, in the posture of a preliminary injunction, that scraping a public website does not likely violate the CFAA. See *hiQ Labs v. LinkedIn*, 31 F.4th 1180 (9th Cir. 2022). But following that decision, the district court held that hiQ had committed breach of contract in scraping LinkedIn's website in violation of terms of service. See *hiQ Labs v. LinkedIn*, No. 17-cv-03301-EMC (N.D. Cal. Nov. 4, 2022).

37. See, e.g., *Animal Legal Def. Fund v. Kelly*, 9 F.4th 1219 (10th Cir. 2021), *cert. denied*, 142 S. Ct. 2647 (2022) (holding that Kansas' ag-gag law was viewpoint discriminatory in violation of the First Amendment because it operated only to restrict critics of agricultural facilities from gaining access and recording there); *Animal Legal Defense Fund v. Wasden*, 878 F.3d 1184 (9th Cir. 2018) (concluding that Idaho's criminalization of using misrepresentations to enter a production facility and ban on audio and video recordings of a production facility's operations violated the First Amendment); see also *People for the Ethical Treatment of Animals, Inc. v. N. Carolina Farm Bureau Fed'n, Inc.*, 60 F.4th 815 (4th Cir. 2023) (enjoining North Carolina from enforcing its law prohibiting, among other things, employees from surreptitiously recording information to breach their duty of loyalty to their employer, but only insofar as the law would interfere with newsgathering activities).

38. Caitlin Vogus & Emma Llansó, Center for Democracy and Technology, *Making Transparency Meaningful: A Framework for Policymakers* (Dec. 14, 2021), <https://cdt.org/insights/new-cdt-report-provides-guide-for-policymakers-on-making-transparency-meaningful> (including guidance on protecting researcher data from law enforcement access).