

Creation of Fake Online Accounts to Study Algorithmic Bias Does Not Violate the Computer Fraud and Abuse Act, D.C. Court Rules

Law and the Workplace Blog on April 10, 2020

A federal judge recently held that researchers who violate a website's terms of service by creating fake online accounts in order to study algorithmic bias in artificial intelligence software do not violate the Computer Fraud and Abuse Act ("CFAA") (decision available [here](#)).

Brief Background

The decision resulted from a lawsuit filed by the American Civil Liberties Union ("ACLU") against the Department of Justice ("DOJ") on behalf of researchers and a nonprofit journalism group. Several of the researchers had created fake employer and employee accounts in order to study the algorithms used by various websites (such as LinkedIn). The researchers were particularly interested in determining whether the algorithms discriminated against applicants on the basis of protected characteristics, such as sex, age, or race.

Realizing that the use of fake accounts violated the terms of service of many of the websites, the ACLU filed suit on behalf of the plaintiffs in order to seek a declaration that their conduct did not violate the CFAA's "Access Provision," which criminalizes the "intentional access [of] a computer without authorization or exceeding authorized access, and thereby obtaining . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). The suit contended that the Access Provision unconstitutionally restricted the researchers' First Amendment right to free speech "by criminalizing their research plans and journalistic activities that involve violating websites' terms of service."

After determining that plaintiffs had standing, the Court adopted a narrow interpretation of the “exceeds authorized access” language of the CFAA. Although the Court held that the conduct in question could expose a party to civil liability under other federal and state laws (e.g., lawsuits by website owners against individual violators to enforce their terms of service), it ultimately found that agreeing to terms of service “is not sufficient to trigger criminal liability under the CFAA.”

Finding that the conduct in question was not criminal in the first instance, the Court did not weigh in on the First Amendment concerns raised by plaintiffs.

Takeaways

While the Court’s decision permits researchers to create fake accounts to study algorithmic bias without concern of criminal liability under the CFAA, it does not absolve individuals of liability arising under other federal and state laws (let alone attorney ethics rules), or shield them from suits by website owners.

This decision further underscores the need for employers to continue to heed caution and consult counsel before unleashing “AI” software in their workplace as individuals and organizations actively seek to covertly assess possible algorithmic bias in AI platforms.

[View Original](#)