Law360

Ruling On Anti-Hacking Law May Guide Fair Lending Tests

By **Jeffrey Naimon, Joshua Kotin and Frida Alim** (May 5, 2020)

Jeffrey Naimon

Joshua Kotin

Frida Alim

Regulators, consumer groups, academics and private litigants are grappling with the fair lending implications of the credit models powering the explosive growth in online lending by banks and financial technology firms.

The U.S. District Court for the District of Columbia in late March concluded that creating fake online profiles to test proprietary algorithms for discrimination does not violate the Computer Fraud and Abuse Act, or CFAA, even if the creation of such accounts violates the terms of service on the host's website.[1]

The holding in Sandvig v. Barr may encourage some constituencies to update the old-school strategy of deploying human testers into the online credit arena. In addition, the U.S. Supreme Court is reviewing a case that may shed further light on whether a violation of terms of service implicates the notoriously vague CFAA, which was enacted in 1984 when floppy disks were cutting-edge technology.[2]

Sandvig Implications for Fair Lending Testing

The Sandvig court held that academic researchers testing whether various hiring websites' proprietary algorithms discriminated against online users based on characteristics such as race and gender did not violate the CFAA when they created fake profiles, even though doing so violated websites' terms of service.[3]

The CFAA's so-called access provision prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information from any protected computer."[4] In avoiding the constitutional question of whether the CFAA violates the First Amendment, the court found that terms of service did not constitute permission requirements, the violation of which would trigger criminal liability under the CFAA.[5] However, the court acknowledged that agreeing to terms of service may have consequences for civil liability under other federal and state laws.[6]

While the Sandvig case is not the first to hold that a violation of terms of service does not constitute a violation of the CFAA, it is the most recent.[7] In addition, the holding is not a complete safe harbor for researchers seeking to use similar tactics in the fair lending world. For example, creating fake accounts to apply for credit may run afoul of federal or state law prohibiting the making of false statements on credit applications.[8]

Use of Alternative Data, Algorithms and Machine Learning Continues to Receive Scrutiny

Government agencies, watchdog groups and researchers continue to analyze the fair lending implications of using alternative data, algorithms and machine learning in consumer lending. On April 8, the Federal Trade Commission posted guidance, encouraging entities using automated tools to be transparent on the type of information the entity collects and the factors they consider in algorithmic decision-making.[9]

This follows lengthy earlier reports by the FTC and Federal Reserve similarly outlining risks of discrimination.[10] In particular, entities relying on algorithmic decision-making for credit decisions should rigorously test algorithms both before use and periodically thereafter to ensure that the algorithms do not have a disparate impact on protected classes.[11]

Some entities have begun to utilize testers to detect discrimination by online platforms. In February, the Student Borrower Protection Center issued a widely publicized report claiming to have found discrimination based only on results generated by an employee submitting false inquiries to lending platforms.[12] Another recent study analyzed potentially disparate outcomes along gender and racial lines on a social media's advertising system by creating mock advertisements.[13]

The use of testers — real or fictionalized — can create headline-grabbing results. However, reliance on results from testers — such as those in the Student Borrower Protection Center report — will also ignore critical aspects of the credit decision process that underpin whether a credit model or practice actually has an impermissible disparate impact.

Steps Lenders Can Take to Mitigate Fair Lending Risk

Lenders should ensure that alternative data is used appropriately and algorithmic decision-making is primed before researchers and government agencies have the opportunity to review and critique these models by:

Evaluating Inputs and Outputs in Algorithms

The FTC advises that an operator of an algorithm ask four key questions prior to use of an algorithm: (1) How representative is the data set; (2) does the data model account for biases; (3) how accurate are predictions based on big data; and (4) does reliance on big data raise ethical or fairness concerns? For example, a lender should consider whether algorithms used to determine credit cost or allocation use ethnically based inputs or proxies, such as census tract. A lender should also evaluate whether the algorithm's outputs result in disparate impacts on protected classes. Conducting this true evaluation should enable a lending platform to better respond to tester-driven criticism.

Comparing the Alternative Underwriting and Pricing Model With a Traditional Model

Continuous monitoring and testing of outcomes is integral to ensure equitable outcomes in the use of alternative data and algorithmic decision-making. This may involve comparing outcomes from the alternative underwriting and pricing model with a hypothetical, non-machine-learning model that uses traditional applicable and credit file variables. Conducting such testing enables the lender to rebut claims of discrimination by consumer groups or researchers.

Engaging a Third Party to Independently Evaluate a Fair Lending Program

This may provide a valuable comparison against claims from consumer groups or researchers. Such a review should include an evaluation of alternative lending models, including the results of such models.

Seeking a No-Action Letter

The Consumer Financial Protection Bureau created its Office of Innovation to engage stakeholders interested in promoting consumer-beneficial innovation and provide measured regulatory protections for financial market participants testing new ideas.[14] Entities aiming to deploy novel marketing and credit models that can expand and improve access to credit can apply for a no-action letter or for participation in the compliance assistance sandbox to reduce regulatory risk while responsibly taking on new and exciting strategies.

Jeffrey Naimon and Joshua Kotin are partners, and Frida Alim is an associate, at Buckley LLP.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] Sandvig v. Barr, No. 16-1368, 2020 WL 1494065 (D.D.C. Mar. 27, 2020).

[2] In Van Buren, petitioner, a police officer, accessed the Georgia Crime Information Center database, which contains license plate and vehicle registration information, to run a search on behalf of a third party. Van Buren v. United States, Petition for Writ of Certiorari at 1 (Dec. 18, 2019), available at https://www.supremecourt.gov/DocketPDF/19/19-783/125972/20191218121814446_No.%2019-__%20Van%20Buren%20Cert%20Petition-2.pdf. The Eleventh Circuit affirmed petitioner's felony computer fraud conviction. Id. at 5-6. Van Buren asks the Supreme Court to consider whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the CFAA if he accesses the same information for an improper purpose. The Supreme Court's holding may impact whether a breach of terms of service, employer policies, or other third-party restrictions would constitute access without authorization under the CFAA. Similar issues of authorized persons accessing sensitive data for unauthorized purposes (i.e., so-called "insider threats") are an increasing focus in data security.

[3] Sandvig, 2020 WL 1494065 at *1.

[4] 18 U.S.C. § 1030(a)(2). The term "protected computer" refers to any computer "used in or affecting interstate or foreign commerce or communication." Id. § 1030(e)(2)(B).

[5] Sandvig, 2020 WL 1494065 at *9-11.

[6] Id. at *10.

[7] See, e.g., United States v. Drew, 259 F.R.D. 449, 464 (C.D. Cal. 2009) (declining to find CFAA liability based on a violation of terms of service because it would render section 1030(a)(2)(C) "unacceptably vague because it is unclear whether any or all violations of terms of service will render the access unauthorized, or whether only certain ones will."); Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016) (a violation of terms of service, alone, "cannot establish liability under the CFAA."); Bittman v. Fox, 107 F. Supp. 3d 896, 900–01 (N.D. Ill. 2015) (creation of fake social media accounts did not result in defendants exceeding authorized access in contravention of the CFAA); United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (holding that the phrase

"exceeds authorized access" in the CFAA "does not extend to violations of use restrictions."); but see United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010) (Social Security Administration employee "exceed[ed] authorized access," in contravention of the CFAA, when he violated a Social Security Administration policy prohibiting access of personal records for nonbusiness purposes).

[8] See, e.g., 18 U.S.C. § 1014.

[9] FTC, Using Artificial Intelligence and Algorithms (Apr. 8, 2020), https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms.

[10] FTC, Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues (Jan. 2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf; Fed. Reserve, Consumer Compliance Supervision Bulletin (Dec. 2019), https://www.federalreserve.gov/publications/2019-december-consumer-compliance-supervision-bulletin.htm.

[11] Id.

[12] Student Borrower Protection Center, Educational Redlining (Feb. 2020); Sen. Kamala Harris, Harris, Senate Democrats Press Upstart, Lenders for Answers Following Reports of Higher Interest Rates for Students of Minority-Serving Institutions (Feb. 13, 2020), https://www.harris.senate.gov/news/press-releases/harris-senate-democrats-press-upstart-lenders-for-answers-following-reports-of-higher-interest-rates-for-students-of-minority-serving-institutions.

[13] Muhammad Ali et al., Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Skewed Outcomes Proceedings of the ACM on Human-Computer Interaction, Vol. 3, CSCW, Article 199 (November 2019) .

[14] CFPB, Final Rule: Policy on No-Action Letters (Sept. 6, 2019), https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-no-action-letters.pdf.