A CASE AGAINST BAD MATH

Peggy Bruner[*]

INTRODUCTION

If you google[1] any of one your favorite Tech News blogs, you will likely see at least one of the following phrases on the homepage: "artificial intelligence," "machine learning," or "algorithm." An algorithm, the basis of this fast-growing area of computer science, is a sequence of instructions telling a computer what to do.[2] Machine learning uses algorithms to "learn" by "minimizing error or maximizing the

* J.D., University of Florida Levin College of Law; B.A. 2015, Auburn University. I would like to thank my friends and family for their constant support. I would also like to thank Adam Curry and John C. Dvorak of the No Agenda Podcast for drawing my attention to this important topic. Lastly, thank you to all of the members of the *Journal of Technology Law and Policy* for their hard work and dedication.

1. *Google*, MERRIAM-WEBSTER, 2017, https://www.merriam-webster.com/dictionary/google (last updated Dec. 21, 2017).

2. Jacob Brogan, *What's the Deal With Algorithms?*, SLATE, http://www.slate.com/articles/technology/future_tense/2016/02/what_is_an_algorithm_an_explainer.html (last updated Feb. 2, 2016).

likelihood of their predictions becoming true."[3] Artificial Intelligence uses algorithms to perform tasks that would otherwise require human behavior, such as visual or audio recognition.[4] Over the last few years, big data companies like Netflix, Amazon, and Facebook have introduced algorithms to suggest movies you might like, products you might want to purchase, or people you may know based on the inputs you give each algorithm.

I. THE PROBLEM WITH ALGORITHMS

I never would have guessed that this type of math was responsible for advancing systemic discrimination until I watched a TED Talk by Cathy O'Neil.[5] O'Neil explained how algorithms are used by big data companies to determine who fills an open job position, who gets an interview, or who pays more for their insurance.[6] She highlighted how the public does not get to see the magic formulas that make these decisions.[7] Cathy O'Neil has been investigating these secret formulas and dedicated the last few years writing a book about them. In her cleverly titled book, *Weapons of Math Destruction*, she explains the problems with these secret formulas and our inability to question and change them.[8] Throughout her book and speeches, she makes a call for action, asking society to accept fairness over accuracy.

O'Neil describes how this type of discrimination, hidden deep in source code, is typically invisible to the public.[9] Just because discrimination is hidden does not mean it is insignificant. Often times, this type of discrimination is illegal.[10] In other situations, biased algorithms perpetuate negative and harmful stereotypes. For example, a study in 2013 found that Google's results for searches of common African-American names would often show suggestions that the person had an arrest record, even if he or she did not.[11] Many people might not

3. DEEPLEARNING4J DEVELOPMENT TEAM, *Artificial Intelligence, Machine Learning and Deep Learning*, https://deeplearning4j.org/ai-machinelearning-deeplearning (last visited Dec. 7, 2017).

4. *Id.*

5. Cathy O'Neil, *The Era of Blind Faith in Big Data Must End*, TED, https://www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end/ transcript (last visited Dec. 6, 2017).

6. *Id.*

7. *Id.*

8. CATHY O'NEIL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND THREATENS DEMOCRACY 13 (1st ed. 2016).

9. *Id.*

10. *E.g.*, Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-2 (2012); 42 U.S.C. § 3604.

11. Latanya Sweeney, *Discrimination in Online Ad Delivery*, 56 COMM. ACM 44–54 (2013).

initially understand the implications of an individual's negative Google search results. Therefore, imagine applying for a job where the employer's first step in a background check is to search the individual's name on an online search engine such as Google. When pages of results are suggestions for another similarly named individual's potential arrest records, an employer is likely to end his or her preliminary background check, and potentially the individual's application process altogether.

This problem has been detected, investigated, and reported many times over several years. Corporations and government organizations have exponentially continued, however, to develop new algorithms. Our institutions place blind faith in mathematical formulas, hoping for maximized efficiency and profits.

II. LEGAL APPROACHES TO INVESTIGATING DISCRIMINATORY ALGORITHMS

The success of O'Neil's speech and book has shone a light on insidious discrimination hidden deep inside mathematical formulas that falsely appear objective. The public's demand to hold big data companies accountable is critical to finding and fighting bias deep within the source code. Legally speaking, computer scientists, academic researchers, and journalists face many hurdles when investigating this problem. The criminal justice system continues to use software to predict the likelihood that a criminal will commit a crime in the future, despite vast research showing the software makes racially discriminatory assumptions. On the consumer protection front, researchers have identified discriminatory business practices and successfully pressured corporations into changing those practices. But a suit filed by the ACLU on behalf of researchers investigating potential housing and employment discrimination online shows there are additional legal hurdles researchers have to overcome when tackling algorithmic discrimination.[12]

A. *Algorithms in the Criminal Justice System*

The criminal justice system uses algorithms in crime prediction software and "risk assessment" tools.[13] Crime prediction software programs, like PredPol, CompStat, and HunchLab, are software programs that process past data to predict where crimes are likely to occur.[14] Police departments benefit from these programs when faced with

12. Complaint at 1–3, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

13. Justin Jouvenal, *Police Are Using Software to Predict Crime. Is it a 'Holy Grail' or Biased Against Minorities?*, WASH. POST (Nov, 16, 2016), https://www.washingtonpost.com/local/public-safety/police-are-using-software-to-predict-crime-is-it-a-holy-grail-or-biased-against-minorities/2016/11/17/525a6649-0472-440a-aae1-b283aa8e5de8_story.html?utm_term=.89350e3abb78.

14. O'NEIL, *supra* note 8, at 85.

substantial financial restraints and a limited number of officers available for patrolling a given community.[15]

Risk assessment software is employed to predict a defendant's recidivism rate, or the likelihood a defendant will commit a crime again; it's used to set bail and determine sentences.[16] This software uses algorithms to calculate risk based on factors such as a defendant's age, sex, location, family background, and employment.[17] One example of this software is the Level of Service Inventory-Revised (LSI-R), which is a quantitative survey of offender attributes and their situations relevant to the level of supervision and treatment decisions.[18] The LSI–R helps predict parole outcomes, success in correctional halfway houses, institutional misconducts, and recidivism.[19]

Another example of risk assessment software is COMPAS (Correctional Offender Management Profiling for Alternative Sanctions), which is used for decisional support in the Department of Corrections when making placement decisions, managing offenders, and planning treatment.[20] COMPAS uses information gathered from a defendant's criminal file and an interview with the defendant to produce a report that consists of predicted recidivism and potential needs related to substance abuse, housing, and employment.[21] The COMPAS assessment calculates pre-trial, general, and violent recidivism risks on a one to ten scale.[22] COMPAS predicts the general likelihood that a criminal is either more or less likely to commit another crime following release from custody based on those with a similar history of offending.[23]

1. State v. Loomis

The Wisconsin Supreme Court reviewed the constitutionality of the algorithm used by COMPAS in *State v. Loomis*.[24] Loomis was the driver in a drive-by shooting.[25] He was charged with five counts, including first-degree recklessly endangering safety, operating a motor vehicle without the owner's consent, attempting to flee a traffic officer, possession of a firearm by a felon, and possession of a short-barreled shotgun or rifle.[26]

---

15. *Id.*
16. *Id.* at 25.
17. *Id.*
18. *LSI-R*, MHS ASSESSMENTS, https://www.mhs.com/MHS-Publicsafety?prodname=lsi-r (last visited Dec. 7, 2017).
19. *Id.*
20. State v. Loomis, 881 N.W.2d 749, 754 (Wisc. 2016).
21. *Id*.
22. *Id.*
23. *Id.*
24. *Id.* at 753.
25. *Id*. at 754.
26. *Id.*

Loomis denied any involvement with the crime, and pleaded to two of the less severe charges: attempting to flee a traffic officer and operating a motor vehicle without the owner's consent.[27] The plea agreement dismissed the other counts but included the following[28]:

> The other counts will be dismissed and read in for sentencing, although the defendant denies he had any role in the shooting, and only drove the car after the shooting occurred. The State believes he was the driver of the car when the shooting happened. The State will leave any appropriate sentence to the court's discretion, but will argue aggravating and mitigating factors.

After Loomis accepted the plea, he was subjected to a presentence investigation which included a COMPAS risk assessment.[29] The COMPAS scores predicted that Loomis was highly likely to commit another crime before trial, another crime in general, and a violent crime.[30] Although the COMPAS report stated that its scores "should not be used to determine the severity of the sentence or whether the offender is incarcerated," the State argued that the court should consider the report in determining Loomis's sentence.[31] The court used the COMPAS scores among other factors in excluding the possibility of probation.[32] The court sentenced Loomis to six years in prison and five years of supervised parole.[33] After sentencing, Loomis filed a motion for post-conviction relief requesting a new sentencing hearing, alleging the court's use of the COMPAS risk assessment violated his due process rights.[34]

At the due process hearing, expert witness Dr. David Thompson testified for the defense, explaining that the court's consideration of the COMPAS risk assessment runs a serious risk of overestimating an individual's risk.[35] Dr. Thompson also pointed out how little information courts have about how the COMPAS software analyzes the recidivism risks of each defendant; he stated, "[t]he Court does not know how the COMPAS compares that individual's history with the population that it's comparing them with. The Court doesn't even know whether that population is a Wisconsin population."[36] The court denied the post-conviction motion, explaining that it used the COMPAS report to

27. *Id.*
28. *Id.*
29. *Id.*
30. *Id*. at 755.
31. *Id.*
32. *Id.*
33. *Id.* at 756 n.18.
34. *Id.* at 756.
35. *Id.*
36. *Id.* at 756.

corroborate its findings and that it would have imposed the same sentence regardless.[37]

On appeal, the court considered whether the circuit court's consideration of the COMPAS risk assessment report violated Loomis's constitutional right to due process as a question of law.[38] The court found that a sentencing court may consider a COMPAS risk assessment report at sentencing but not to incarcerate an offender or to determine the severity of the sentence.[39] The court restricted the use of the report, holding that it "may not be considered as the determinative factor in deciding whether an offender can be supervised safely and effectively in the community."[40]

2. ProPublica's Algorithm Audit

In May 2016, ProPublica released a report on a number of states and their use of the COMPAS recidivism algorithm.[41] As a part of the report, ProPublica studied 10,000 criminal defendants in Broward County, Florida and compared their predicted recidivism to their actual rates over a two-year period.[42] They found that African-American defendants were predicted to be riskier than they actually were, and white defendants less risky than they were.[43] Black defendants were also twice as likely as white defendants to be misclassified as having a higher risk for violent recidivism.[44] Compared with violent black recidivists, violent white recidivists were 63% more likely to be misclassified as having a low risk of violent recidivism.[45] The violent recidivism analysis also showed that even when controlling for prior crimes, future recidivism, age, and gender, black defendants were 77% more likely to be assigned higher risk scores than white defendants.[46]

While the ProPublica report shows that risk assessment software is substantially discriminatory, the ruling in *Loomis* demonstrates how difficult it can be for a court to make a legal determination that the software is so substantially discriminatory that it should not be used as a

---

37. *Id.* at 757.

38. *Id.*

39. *Id.* at 759.

40. *Id.*

41. Julia Angwin et al., *Machine Bias*, PROPUBLICA, (May 23, 2016), https://www.propublica. org/article/machine-bias-risk-assessments-in-criminal-sentencing.

42. *Id.*

43. Julia Angwin et al., *How We Analyzed the COMPAS Recidivism Algorithm*, PROPUBLICA, (May 23, 2016), https://www.propublica.org/ article/how-we-analyzed-the-compas-recidivism-algorithm.

44. *Id.*

45. *Id.*

46. *Id.*

single factor when a judge determines a criminal sentence.[47] Perhaps if the *Loomis* court had the ProPublica report prior to the due process hearing, the outcome would have been different. *Loomis* sets a tricky precedent for future cases against bad math and discriminatory algorithms.

In *Loomis*, the risk assessment software did not determine the defendant's guilt, and the risk report was one factor in the court's sentencing decision.[48] The court did not have to use the report at all to determine Loomis's sentence if it did not wish to. The software was likely not strongly discredited or prohibited because of the court's role in deciding the defendant's sentence. Indeed, judges across the country handle increasingly overwhelming caseloads and risk assessment software can contribute to judicial efficiency.

Risk assessment software, if created properly, can also give judges objective recommendations for criminal sentencing, in which case an outright ban on these types of software might further perpetuate biased decision-making in the criminal justice system. It is possible to create unbiased risk assessment software, but to do so, like Cathy O'Neil has advocated time and again, we need to see the source code. We also need independent researchers, like ProPublica, to continue testing this software and probing these algorithms we place our blind trust in to see if they are as objective as we want them to be.

B. *Amazon Same-Day Delivery Dilemma*

In April 2016, after Amazon.com launched their same-day delivery program in twenty-seven metropolitan areas across the United States, Bloomberg News published a report showing that Amazon excluded predominantly black neighborhoods from same-day services within some six of those cities.[49] The researchers used Amazon's publicly available data showing what zip codes were offered same-day delivery and racial demographic data from the American Community Survey to determine whether Amazon was prioritizing services to white neighborhoods over predominantly black neighborhoods.[50]

In Atlanta, Boston, Chicago, Dallas, New York City, and Washington, D.C., black residents were just half as likely as white residents to live in a neighborhood Amazon provided same-day delivery service to.[51] Amazon's Vice President of Global Communications, Craig Berman,

47. State v. Loomis, 881 N.W.2d 749, 767 (Wisc. 2016).

48. *Id.*

49. David Ingold & Spencer Soper, *Amazon Doesn't Consider the Race of Its Customers. Should It?*, BLOOMBERG (Apr. 21, 2016), https://www.bloomberg.com/graphics/2016-amazon-same-day/.

50. *Id.*

51. *Id.*

responded to the Bloomberg reporters, explaining that Amazon does not use ethnic composition of neighborhoods to draw up their maps.[52] Berman explained that Amazon's plan is to focus its same-day service in areas where there is a high concentration of Prime members and continue to fill the gaps in the future.[53]

Amazon offers same-day delivery service to Amazon Prime members, who pay a yearly membership fee of $99.[54] A study from investment bank Piper Jaffray found that in 2016, around 71% of households with an average income of $112,000 and over had Amazon Prime memberships, while 43% of households with an average income between $21,000–$41,000 had memberships.[55] Berman suggested that income inequality could likely play a role in drawing the maps, although some predominantly black neighborhoods were not given same-day delivery access despite having higher average annual household incomes than whiter neighborhoods with same-day delivery.[56] The Amazon representative explained that too few Prime members in each area, the distance between serviced areas, the location of the closest Amazon warehouse, and the cost of the carriers create diminishing returns for certain ZIP codes.[57] Amazon, however, does not provide the locations of the Amazon Warehouses.

Interestingly, in Boston, the Roxbury area was not offered same-day delivery, although it is surrounded by neighborhoods that have access to the service.[58] Berman stressed that Amazon does not use race to calculate what areas are offered same-day service and that reaching the maximum number of customers is the top priority.[59] For customers who live in neighborhoods without same-day service, Amazon's secret formula or their intent behind it does not matter.[60] The impact reinforces inequality in access to goods, services, and job opportunities since Amazon employs drivers and carriers within the same-day delivery communities. Moreover, these discriminatory practices could violate federal law.[61]

---

52. *Id.*

53. *Id.*

54. *See* Ingold & Soper, *supra* note 49.

55. *Id.*; *see* Rani Molla, *For the Wealthiest Americans, Amazon Prime Has Become the Norm*, RECODE (June 8, 2017, 10:27 AM), https://www.recode.net/2017/6/8/15759354/amazon-prime-low-income-discount-piper-jaffray-demographics.

56. *Id.*

57. *Id.*

58. *See* Ingold & Soper, *supra* note 49.

59. *Id.*

60. *Id.*

61. *Amazon Urged to Serve Minority Areas in Chicago, New York*, CHI. BUS. (Apr. 29, 2016), http://www.chicagobusiness.com/article/20160429/NEWS10/160429782/amazon-urged-to-serve-minority-areas-in-chicago-new-york.

Following the Bloomberg report, several media companies picked up the story, and politicians from Boston, New York, and Chicago called for action. United States Representative Bobby Rush, from Illinois, urged the Federal Trade Commission to investigate Amazon's same-day delivery boundaries to determine if they violated the Civil Rights Act of 1964, for inequitable distribution services.[62] In New York, State Assemblyman Jeffrey Dinowitz also called for state and federal investigations into Amazon's same-day maps, calling the exclusion "a real slap in the face."[63] Bronx Borough President, Ruben Diaz, Jr., wrote a letter to Amazon's CEO, Jeff Bezos, addressing the unacceptable "level of insensitivity, if not hostility" of the company's business practice.[64] In Boston, former state treasurer Steven Grossman called for residents to petition Amazon, calling the exclusion of the Roxbury neighborhood, "insensitive, unjust, and unwise."[65] Shortly following the backlash, Amazon extended same-day delivery to all zip codes in Boston, Chicago, and the Bronx borough in New York.[66]

Amazon never released the method used for determining what areas would receive same-day delivery.[67] Instead, Berman described multiple factors that could explain the disparate impact in select cities.[68] Berman pointed to examples of predominantly minority race neighborhoods with same-day delivery in other metropolitan areas to explain that Amazon does not use race as a variable to draw up boundaries.[69] Although some of the excluded neighborhoods had higher crime rates, Amazon would not say whether that was a factor involved in its decision.[70] While Amazon has not given more insight into its decision-making process, Berman's comments indicate that an algorithm, making blind assumptions based on profits and efficiency, was at play here. If humans at Amazon decided which neighborhoods to include in each metropolitan area—and perhaps that decision was reviewed by a public relations

62. *Id.*

63. *Id.*

64. Dan Adams et al., *Why Doesn't Amazon Offer Same-Day Delivery in Roxbury?*, BOS. GLOBE (Apr. 21, 2016), https://www.bostonglobe.com/business/2016/04/21/why-doesn-amazon-offer-same-day-delivery-roxbury/09m1fLx69trWXWAk3UNgcK/story.html.

65. *Id.*

66. *See* Spencer Soper, *Amazon to Bring Same-Day Delivery to Bronx, Chicago After Outcry*, BLOOMBERG (May 1, 2016), https://www.bloomberg.com/news/articles/2016-05-01/amazon-pledges-to-bring-same-day-delivery-to-bronx-after-outcry; *see also* Eugene Kim, *Amazon Expands Same-Day Delivery to All of Boston Following Reports of it Excluding Black Neighborhoods*, BUS. INSIDER (Apr. 26, 2016), http://www.businessinsider.com/amazon-same-day-delivery-now-available-in-all-of-boston-2016-4.

67. *See* Ingold & Soper*, supra* note 49.

68. *Id.*

69. *Id.*

70. *Id.*

team—the retail giant could have avoided possibly violating federal regulations.

Certainly, Amazon has no financial interest in engaging in discriminatory practices. Berman told Bloomberg, "with the math involved, we can't make it work."[71] Amazon made the math work, however, and within weeks of the Bloomberg report. As of December 2017, Amazon offers Prime members same-day delivery in thirty-two cities.[72] Amazon likely created a formula based on variables Berman discussed and other factors "the competition would kill for," and let that algorithm dictate which ZIP codes receive same-day services.[73] Amazon did not factor in "human" variables into their algorithm; rather, it skipped the last step human-review that the *Loomis* court exercised.[74] Amazon's "math" overlooked the importance of extending access to goods and services, as well as providing economic opportunities in these neighborhoods still struggling with economic inequality.

Like ProPublica did with the risk-assessment software used in *Loomis*, the analysts at Bloomberg took publicly available information straight from Amazon to detect Bloomberg's own discriminatory algorithm.[75] Bloomberg used its media platform to expose the disparate impact, and luckily for Amazon, it had the opportunity to right the wrong before facing legal action. Bloomberg's report is incredibly important because it exposes how corporations may be intentionally or unintentionally practicing discrimination and how we can use data to question those practices. There is plenty of silent and invisible discrimination going on that is much more difficult to detect. Some is even illegal to detect.[76]

C. *The ACLU Takes on the CFAA in* Sandvig v. Sessions

In 2016, the American Civil Liberties Union filed a suit on behalf of academic researchers, computer scientists, and journalists who wish to investigate discriminatory practices by companies on the internet.[77] The suit challenges the constitutionality of the Computer Fraud and Abuse Act (CFAA), also known as the most hated internet law.[78] Section

71. *Id.*

72. AMAZON, https://primenow.amazon.com/onboard (last visited Dec. 7, 2017).

73. *See Amazon Urged to Serve Minority Areas in Chicago, New York*, *supra* note 61.

74. State v. Loomis, 881 N.W.2d 749, 759 (Wisc. 2016).

75. Ingold & Soper, *supra* note 49.

76. *See* 18 U.S.C. § 1030(a)(2)(C) (2012); Esha Bhandari & Rachel Goodman, *ACLU Challenges Computer Crimes Law That is Thwarting Research on Discrimination Online,* ACLU (June 29, 2016, 10:00 AM), https://www.aclu.org/blog/racial-justice/race-and-economic-justice/aclu-challenges-computer-crimes-law-thwarting-research?redirect=blog/free-future/aclu-challenges-computer-crimes-law-thwarting-research-discrimination-online.

77. Complaint at 4, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

78. *Id.* at 1; G. Burningham, *The Most Hated Law on the Internet and its Many Problems*, NEWSWEEK (Apr. 16, 2016, 2:20 PM), http://www.newsweek.com/most-hated-law-internet-and-

1030(a)(2)(C) of the CFAA makes anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" criminally liable by fine, imprisonment, or both.[79] The small phrase, "exceeds authorized access," experts argue, effectively makes any website's terms of service law because any violation of a website's terms of service is punishable under the CFAA.[80]

The CFAA was first drafted in 1986 and has been amended nine times as computer crimes have grown in complexity and sophistication.[81] Critics of the CFAA argue that Congress has refused with each additional amendment to narrow and define the meaning of the "authorized access" provision, create additional private rights of action, and turn misdemeanors into felonies.[82] Most recently, following the Sony Pictures Entertainment hack, the Obama administration promised to ensure that "insignificant conduct does not fall within the scope of the statute," but the revision instead created harsher penalties for hacking crimes and broadened the definition of hacking.[83]

Some courts interpret the phrases "without authorization" and "exceeds authorized access" broadly enough to cover violations of corporate computer use restrictions or violations of a duty of loyalty.[84] Other courts have concluded that the CFAA does not expressly forbid the misuse of confidential and proprietary computer-stored information and is limited to violations of restrictions on access to such information.[85]

---

its-many-problems-cfaa-448567 (The CFAA was used to prosecute Aaron Swartz after he entered a closed network closet at MIT and mass downloaded millions of academic journals; Swartz committed suicide after prosecutors rejected a plea deal).

79. 18 U.S.C. § 1030(a)(2)(C).

80. *Id.*; Esha Bhandari & Rachel Goodman, *supra* note 76.

81. PROSECUTING COMPUTER CRIMES, OFFICE OF LEGAL EDUCATION EXECUTIVE OFFICE FOR UNITED STATES ATTORNEYS (2d ed. 2007).

82. Tim Wu, *Fixing the Worst Law in Technology,* NEW YORKER (Mar. 18, 2013) https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

83. Dana Liebelson, *Democrats, Tech Experts Slam Obama's Anti-Hacking Proposal*, HUFFINGTON POST (Jan. 20, 2015, 8:27 PM), https://www.huffingtonpost.com/2015/01/20/obama-hackers_ n_6511700.html.

84. *See, e.g.*, United States v. John, 597 F.3d 263, 271–72 (5th Cir. 2010) (finding employee "exceed[ed] authorized access" when she used employer information, to which she had access for other purposes, to perpetrate a fraud); Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (applying principles of agency, employee's authorization to use employer's laptop ended once he violated duty of loyalty to employer, and thus finding employee accessed computer "without authorization"); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579–80, 583 (1st Cir. 2001) (interpreting "exceeds authorized access" to encompass breach of an employer confidentiality agreement where disloyal employee allegedly helped competitor obtain proprietary information).

85. *See, e.g.*, United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012) (affirming dismissal of Section 1030(a)(4) charge against a defendant who resigned and then induced his former colleagues to download confidential customer information and transfer that information to him,

A broad interpretation of the CFAA's "exceeds authorization access" provision could render activities like recording public information, providing false information, and creating multiple accounts criminal offenses. These are exactly the types of activities that researchers, journalists, and computer scientists need to do to study discrimination in big data. Christian Sandvig, one of the plaintiffs represented by the ACLU in the pending suit challenging the CFAA, explains why researchers in computing and social science need to break websites' terms of service to investigate into potential discriminatory practices.[86] They use various techniques, like writing scripts, bots, or scrapers that collect online data, to bombard closed algorithms with various inputs to study their hidden biases.[87]

The ACLU represents Sandvig, three additional professors, and First Look Media Works.[88] These specialists in algorithmic research want to deploy bots and use fake profiles to investigate possible racial and gender discrimination in online advertising for employment and housing.[89] They also want to use automated methods of recording publicly available data from websites, also known as "scraping."[90] The websites the researchers have targeted forbid these techniques in their "terms of service," thus the researchers cannot go forward because their actions could be prosecutable crimes under the CFAA.[91]

The ACLU points out that offline audit testing, which involves pairing people of different races to pose as home- or job-seekers, has been encouraged by courts[92] and Congress to uncover racial discrimination in

---

in violation of company's policy prohibiting disclosure of confidential information; "the CFAA 'targets the unauthorized procurement or alteration of information, not its misuse or misappropriation'"); Scottrade, Inc. v. BroCo Invs., Inc., 774 F. Supp. 2d 573, 583–84 (S.D.N.Y. 2011) (dismissing a CFAA claim against investment firm where plaintiff conceded that defendant had not accessed plaintiff's computer systems without authorization); Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 381, 383–84 (S.D.N.Y. 2010) (finding that where defendant employee conspired with former employee to steal confidential client information from employer's database, CFAA claim could not be premised on acts of system administrator, because he had "full access" to the database at issue).

86. Christian Sandvig, *Why I Am Suing the Government*, SOCIAL MEDIA COLLECTIVE, (July 1, 2016), https://socialmediacollective.org/ 2016/07/01/why-i-am-suing-the-government/.

87. *Id.*

88. Complaint at 1, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

89. Cyrus Farivar, *To Study Possibly Racist Algorithms, Professors Have to Sue the US,* ARSTECHNICA (June 29, 2016, 10:00 AM), https://arstechnica.com/tech-policy/2016/06/do-housing-jobs-sites-have-racist-algorithms-academics-sue-to-find-out/.

90. Esha Bhandari & Rachel Goodman, *supra* note 76.

91. *See* 18 U.S.C. § 1030(a)(2)(C) (2012).

92. *See* Shaver v. Indep. Stave Co., 350 F.3d 716, 723–25 (8th Cir. 2003) (supporting "the so-called 'tester' cases, where minority applicants apply for jobs or housing that they have no intention of accepting for the sole purpose of determining whether the employer or landlord is unlawfully discriminating" to conclude that terminated employee's claims were actionable).

housing and employment.[93] Audit testing vindicated civil rights laws, including Title VII's prohibition on discrimination in employment and the Fair Housing Act.[94]

Specifically, the ACLU claims that the CFAA unconstitutionally prohibits the researchers' methods of posing as online users of different races and recording information they receive, conduct the ACLU says is speech and expressive activity protected by the First Amendment.[95] They further claim that the overbroad provisions within the CFAA are unconstitutionally vague under the Fifth Amendment and chill a range of speech and expressive activity by preventing private individuals from researching issues of public concern.[96]

The government responded to the ACLU's arguments in several ways. The government first argued that the plaintiffs failed to establish standing.[97] It next argued that the ACLU failed to state its claims.[98] It argued that the meaning of the CFAA is clear and the plaintiffs' harm is theoretical.[99]

The harm suffered from discrimination is not theoretical, however. Many of those who experience actual discrimination from an algorithmic program are not data or algorithm research specialists. It is unreasonable to expect that an average internet user has scripts, bots, and scraping tools available to audit an algorithm he or she suspects is biased. Even if a person believes an algorithm discriminated against him or her, that person likely has no avenue to request an explanation for the decision made against him or her.

III. POTENTIAL PLAINTIFFS

From where we now stand, in an era racing to apply artificial intelligence and machine learning processes in as many ways as possible, it can be difficult to imagine just how often an algorithm would be wired to discriminate against protected classes. *Loomis*, the Amazon same-day dilemma, and *Sandvig* provide examples of suspicious algorithms that needed auditing.

A. *Artificial Intelligence & Image Recognition Software*

Machine learning and artificial intelligence create more significant room for error because of their unique mechanism of "training" a data

93. Complaint at 2, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

94. *Shaver*, 350 F.3d at 723–25.

95. Complaint at 4, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

96. *Id.*

97. Memorandum of Points and Authorities in Support of Defendant's Motion to Dismiss at 2–3, 8–9, Sandvig v. Sessions, 315 F. Supp. 3d 1 (D.D.C. 2018) (No. 16-1368).

98. *Id.* at 2–3.

99. *Id.*

set. Take, for example, how a computer science professor discovered that image-recognition software "learned" to associate images of shopping, cooking, and cleaning with women; and pictures of coaching, shooting, and sports with men.[100] This image-recognition software used machine learning, taking a seemingly unbiased dataset, "learned" about those datasets, and amplified that training on future datasets.[101] The image-recognition software took collections of pictures of both men and women and identified various other items in the background of those pictures.[102] The software found that within the dataset, women were in more pictures with items found in the kitchen, and men were in more pictures with sporting equipment.[103] After the image-recognition software was "trained" on these datasets, it amplified gender bias in future data sets, misidentifying a picture of a man cooking on a stovetop as a woman.[104]

In 2015, Google's image recognition software mistakenly labeled photos of black people as "gorillas."[105] Google swiftly updated the malfunction. After Apple introduced iOS 10 in 2016, a twitter user found that the iPhone Photos application was capable of recognizing photos containing "brassieres," a keyword included in the object and scene detection software.[106] A list of the searchable keywords in Apple's scene and object detecting software update contains words including, "bra," "brassiere," "corset," and "girdle;" but does not include "underwear," "boxers," or "briefs."[107]

If the researchers who created the initial dataset selected more photographs of women in undergarments than men in theirs, the object-detecting software will prioritize, categorize, and "learn" more about the objects that appear most often in the initial dataset.[108] Recent

---

100. Tom Simonite, *Machines Taught by Photos Learn a Sexist View of Women*, WIRED (Aug. 21, 2017, 9:00 AM), https://www.wired.com/story/machines-taught-by-photos-learn-a-sexist-view-of-women/.

101. *Id.*

102. *Id.*

103. *Id.*

104. Jieyu Zhao et al., *Men Also Like Shopping: Reducing Gender Bias Amplification Using Corpus-level Constraints*, https://homes.cs.washington.edu/~my89/publications/bias.pdf (last visited Dec. 7, 2017).

105. Conor Dougherty, *Google Photos Mistakenly Labels Black People 'Gorillas'*, N.Y. TIMES (July 1, 2015, 7:01 PM), https://bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/?_r=1.

106. Dami Lee, *Apple Has Been Categorizing All Your 'Brassiere' Photos for Over a Year Now*, VERGE (Oct. 30, 2017, 5:19 PM), https://www.theverge.com/2017/10/30/16575600/apple-iphone-photos-brassiere-machine-learning.

107. Kenny Yin, *Apple's Updated Photos App Recognizes Thousands of Objects, Scenes and Facial Expressions*, MEDIUM (June 19, 2016), https://medium.com/@iosight/behind-apples-advanced-computer-vision-for-photos-app-41f3f617d31c.

108. *See* Simonite, *supra* note 100.

studies showing that most job positions in the tech industry are filled with men might partially explain how more photos of "brassieres" slips into an initial dataset.[109] These examples of image-recognition software gone awry show us how easily bias can proliferate from a program's initial dataset and amplify that bias.

Although patently offensive, many still underestimate the legal implications of image-recognition software misidentification or its malicious use. As artificial intelligence technology advances at such a high pace, so does the severity of its misapplication. In a recent study, researchers found that facial recognition software could detect a human's sexual orientation significantly better than a human could.[110] A misapplication of this "Gaydar" technology could allow advertisers to target specific products to a person based on his or her sexual orientation. But in a country where homosexuality is a punishable crime,[111] it could expose a substantial threat to the personal privacy and safety of gay men and women.[112]

B. *Advertising Left on Auto-Pilot*

Misidentifications and misapplications of face-recognition technologies illustrate how blind faith in algorithms threatens individual privacy. Although big data companies largely insulated themselves from discrimination claims via targeted advertisements, ProPublica found that Facebook gives advertisers the ability to exclude groups of individuals based on their "ethnic affinities."[113] While Facebook does not ask its members about their specific race, it mathematically assigns users an "ethnic affinity" based on pages, posts, and engagement with other users' content.[114]

Journalists at ProPublica purchased an advertisement for Facebook's housing categories and, in the Detailed Targeting feature provided,

---

109. Dina Bass, *Everyone Knows Tech Workers Are Mostly White Men—Except Tech Workers*, BLOOMBERG TECH. (Mar. 22, 2017, 11:00 AM), https://www.bloomberg.com/news/articles/2017-03-22/everyone-knows-tech-workers-are-mostly-white-men-except-tech-workers.

110. Yilun Wang & Michal Kosinski, *Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images* (last updated Oct. 16, 2017, 12:17 PM), https://osf.io/zn79k/.

111. Siobhan Fenton, *LGBT Relationships Are Illegal in 74 Countries, Research Finds*, INDEPENDENT (May 17, 2016, 11:28 AM), http://www.independent.co.uk/news/world/gay-lesbian-bisexual-relationships-illegal-in-74-countries-a7033666.html.

112. Alan Burdick, *The A.I. "Gaydar" Study and the Real Dangers of Big Data*, NEW YORKER (Sept. 15, 2017), https://www.newyorker.com/news/daily-comment/the-ai-gaydar-study-and-the-real-dangers-of-big-data.

113. Julia Angwin & Terry Parris Jr., *Facebook Lets Advertisers Exclude Users by Race*, PROPUBLICA (Oct. 28, 2016, 1:00 PM), https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race.

114. *Id.*

excluded anyone with an "ethnic affinity" for African-American, Asian-American, or Hispanic people.[115] The advertisement was approved within fifteen minutes of placing the order. This practice clearly violates the Fair Housing Act of 1968.[116] ProPublica went on to find 50,000 unique metrics Facebook measures its users by and uses for targeted advertising.[117] Although Facebook prohibits advertisers from using the targeting options for discrimination, harassment, disparagement, or predatory purposes, that policy did not prevent ProPublica's housing advertisement or ads that target people with interests such as "History of 'why jews ruin the world.'"[118] The social media giant reportedly made $26.89 billion in advertising revenue in 2016.[119]

While Facebook has continued to enhance its efforts to regulate content, its current policy—manually removing advertisements that violate its anti-discrimination policies—is borderline negligent. Facebook's advertising revenues continue to increase, just as the number of its advertising-related scandals.[120] While media organizations like ProPublica and Bloomberg have successfully investigated discriminatory-promoting algorithms, Facebook has taken more measures to obfuscate its advertising stats.[121] For a corporation capitalizing on its incomprehensible level of user engagement, concealing the secret formulas for targeted advertising seems like a C.Y.A. effort at best and fraudulent at worst.[122] Facebook, like other big data companies, does not want the liability of researchers finding bias and discrimination hidden in its algorithms because its monetized model depends on it. Moreover, if Facebook allowed researchers to examine its math for insidious bias, researchers might find out that Facebook's

115. *Id.*

116. 42 U.S.C. § 3604(c) (2012) ("it shall be unlawful . . . to make, print, or publish, or cause to be made, printed, or published any notice, statement, or advertisement, with respect to the sale or rental of a dwelling that indicates any preference, limitation, or discrimination based on race, color, religion, sex, handicap, familial status, or national origin . . . .").

117. *Id.*

118. Julia Angwin et al., *Facebook Enabled Advertisers to Reach 'Jew Haters'*, PROPUBLICA (Sept. 14, 2017, 4:00 PM), https://www.propublica.org/article/facebook-enabled-advertisers-to-reach-jew-haters.

119. *Facebook's Annualized Revenue per User from 2012 to 2016 (in U.S. Dollars)*, STATISTA, https://www.statista.com/statistics/234056/facebooks-average-advertising-revenue-per-user/ (last visited Dec. 6, 2017).

120. Julia Angwin et al., *Facebook Allowed Political Ads that Were Actually Scams and Malware*, PROPUBLICA (Dec. 5, 2017, 8:00 AM), https://www.propublica.org/article/facebook-political-ads-malware-scams-misleading.

121. *See* Lauren Johnson, *Facebook Is Shutting Down its API that Marketers Lean on for Research*, ADWEEK (Dec. 1, 2017), http://www.adweek.com/digital/facebook-is-shtting-down-its-api-that-marketers-lean-on-for-research/.

122. William Safire, *ON LANGUAGE; Glossary of a Scandal*, N.Y. TIMES (Aug. 16, 1987), http://www.nytimes.com/1987/08/16/magazine/on-language-glossary-of-a-scandal.html.

advertisements are not as valuable as businesses believe they are in the first place. Either way, Facebook has no financial incentive to be transparent—unless the public holds it accountable.

IV. CHALLENGING ALGORITHMS

Big data companies need constant public pressure to keep their practices transparent. Besides the third-party review of publicly available information provided by these corporations, there are substantial legal hurdles for researchers to overcome when they suspect algorithmic discrimination.

Limiting the scope of the CFAA so that academic researchers can violate websites "terms of service" to study potential discriminatory practices would substantially advance the cause. Following the filing of the complaint in *Sandvig*, ACLU Staff Attorney, Rachel Goodman, published an article outlining some suggestions for data journalists.[123] She explains that one way to circumvent the CFAA entirely would be to directly ask the company for permission to audit its algorithmic processes.[124] That would give the researcher "authorized access," but it might also legally implicate a researcher who chooses to go forward with the research without permission.[125] Goodman also recommends carefully choosing which technique to use before investigating so that a researcher can avoid damaging a target company's servers, computers, or interfering with its regular business operations.[126] An option of last resort for researchers who have been accused of violating the CFAA should be to draft a defense based on civil rights enforcement.[127]

Goodman illustrates how Congress and courts have encouraged and recognized audit testing in the offline fair housing and employment contexts, as they should in the online context.[128] While the ACLU attempts to tackle head-on the "exceeding authorized access" provision in the CFAA in the judicial system, there is support across the web for legislatively amending the Act to clearly define "authorization" and the penalties for violation.[129]

In the meantime, some algorithmic-justice warriors are challenging blind faith in algorithmic decision-making in their local communities.

---

123. Rachel Goodman, *Tips for Data Journalism in the Shadow of an Overbroad Anti-Hacking Law*, ACLU (Oct. 13, 2017), https://www.aclu.org/blog/privacy-technology/internet-privacy/tips-data-journalism-shadow-overbroad-anti-hacking-law.

124. *Id.*

125. *Id.*

126. *Id.*

127. *Id.*

128. *See id.*

129. *EFF CFAA Revisions—Penalties and Access,* ELEC. FRONTIER FOUND., https://www.eff.org/document/eff-cfaa-revisions-penalties-and-access (last visited Dec. 7, 2017).

This year, James Vacca, a Democratic City Councilman from the Bronx in New York City, introduced a bill that would require the city to make public any computer instructions or algorithms that the government uses for any type of automated decision-making.[130] Increasingly, city governments are applying algorithms to decide which neighborhoods receive the most policing, which schools students are zoned for, and where to conduct health and safety inspections.[131] Vacca's bill would require transparency with regards to the code used in any of the local government's decision-making algorithms as well as audits for any algorithm leased by the city from private companies.[132]

Abroad, the European Union has been more aggressive toward anonymous algorithms.[133] The General Data Protection Regulation is scheduled to take effect in 2018 and has been highly publicized for its establishment of a "right to be forgotten," but also includes a "right to explanation."[134] The law will restrict algorithms that make decisions based on user predictors which make decisions about them.[135] The "right to explanation" gives users an avenue to request an explanation of an algorithmic decision that was made about them.[136] Critics of the new law say that this will make it more difficult for tech companies to develop more complicated algorithmic systems, thereby hindering innovation in the field.[137] Oxford researchers Bryce Goodman and Seth Flaxman argue, however, that the implementation of the law gives computer scientists the opportunity to develop algorithms that avoid discrimination and enable explanation.[138]

---

130. Jim Dwyer, *Showing the Algorithms Behind New York City Services*, N.Y. TIMES (Aug. 24, 2017), https://www.nytimes.com/ 2017/08/24/nyregion/showing-the-algorithms-behind-new-york-city-services.html.

131. Michael Totty, *The Rise of the Smart City*, WALL ST. J. (Apr. 16, 2017, 10:12 PM), https://www.wsj.com/articles/the-rise-of-the-smart-city-1492395120.

132. Automated Decision Systems Used by Agencies, Int. No. 1696-A, N.Y. CITY COUNCIL LEGISLATIVE RESEARCH CTR. (Dec. 6, 2017), http://legistar.council.nyc.gov/Legislation Detail.aspx?ID=3137815&GUID=437A6A6D-62E1-47E2-9C42-461253F9C6D0.

133. Thomas Claburn, *EU Data Protection Law May End the Unknowable Algorithm*, INFORMATIONWEEK (July 18, 2016), https://www.informationweek.com/government/big-data-analytics/eu-data-protection-law-may-end-the-unknowable-algorithm/d/d-id/1326294.

134. Bryce Goodman & Seth Flaxman, *European Union Regulations on Algorithmic Decision-Making and a "Right to Explanation,"* OXFORD INTERNET INST. (Aug. 31, 2016), https://arxiv.org/pdf/1606.08813.pdf.

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.*

CONCLUSION

For many millennials, America has never felt as divided as it feels at the end of 2017. Academics have updated curricula in social science, history, and literature to reflect inclusivity and diversity; and to eliminate bias, stereotypes, and discrimination. Academia has mostly left mathematics, science, and technology out of discussions around race, color, nationality, sex, sexual orientation, and economic class. That needs to change now more than ever.

As big data companies continue to measure intimate human traits in every imaginable way, those companies desperately need to be engaged in meaningful ethical discussions on implicit and explicit bias. Debates will rage on over whether we have done enough to combat bias, hate, and bigotry. But it is time to hold the creators of discriminatory algorithms accountable. It is time to expose corporations' advancement of systemic prejudice and tackle it head-on. Whether we amend the CFAA, continue placing public pressure on discriminatory business practices, or create new laws requiring transparency of these hidden algorithms, we need to end the era of placing blind trust in big data and take control over the machines that are taking control over us.