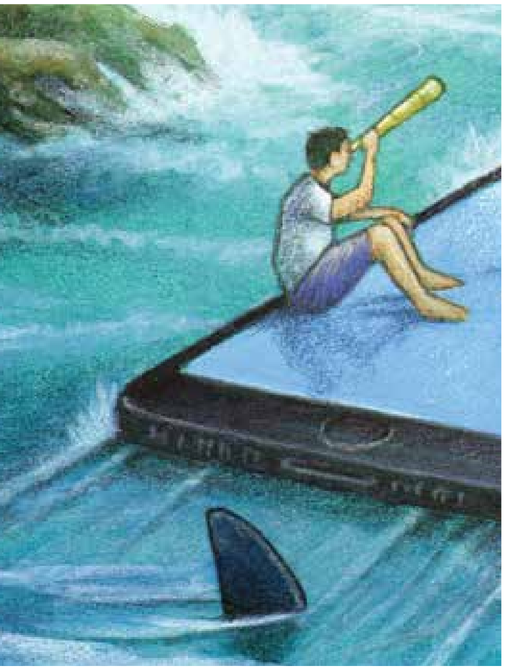
One in a Series of Working Papers from the Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression



An Examination of the Algorithmic Accountability Act of 2019

Mark MacCarthy
Georgetown University

October 24, 2019

TRANSATLANTIC WORKING GROUP

The Transatlantic Working Group Papers Series

Co-Chairs Reports

Co-Chairs Reports from TWG's Three Sessions: Ditchley Park, Santa Monica, and Bellagio.

Freedom of Expression and Intermediary Liability

Freedom of Expression: A Comparative Summary of United States and European Law
B. Heller & J. van Hoboken, May 3, 2019.

Design Principles for Intermediary Liability Laws
J. van Hoboken & D. Keller, October 8, 2019.

Existing Legislative Initiatives

An Analysis of Germany's NetzDG Law
H. Tworek & P. Leerssen, April 15, 2019.

The Proposed EU Terrorism Content Regulation: Analysis and Recommendations with Respect to Freedom of Expression Implications
J. van Hoboken, May 3, 2019.

Combating Terrorist-Related Content Through AI and Information Sharing
B. Heller, April 26, 2019.

The European Commission's Code of Conduct for Countering Illegal Hate Speech Online: An Analysis of Freedom of Expression Implications
B. Bukovská, May 7, 2019.

The EU Code of Practice on Disinformation: The Difficulty of Regulating a Nebulous Problem
P.H. Chase, August 29, 2019.

A Cycle of Censorship: The UK White Paper on Online Harms and the Dangers of Regulating Disinformation
P. Pomerantsev, October 1, 2019.

U.S. Initiatives to Counter Harmful Speech and Disinformation on Social Media
A. Shahbaz, June 11, 2019.

ABC Framework to Address Disinformation

Actors, Behaviors, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses
C. François, September 20, 2019.

Transparency and Accountability Solutions

Transparency Requirements for Digital Social Media Platforms: Recommendations for Policy Makers and Industry
M. MacCarthy, February 12, 2020.

Dispute Resolution and Content Moderation: Fair, Accountable, Independent, Transparent, and Effective
H. Tworek, R. Ó Fathaigh, L. Bruggeman & C. Tenove, January 14, 2020.

Algorithms and Artificial Intelligence

An Examination of the Algorithmic Accountability Act of 2019
M. MacCarthy, October 24, 2019.

Artificial Intelligence, Content Moderation, and Freedom of Expression
E. Llansó, J. van Hoboken, P. Leerssen & J. Harambam, February 26, 2020.

www.annenbergpublicpolicycenter.org/twg

A project of the Annenberg Public Policy Center of the University of Pennsylvania in partnership with
The Annenberg Foundation Trust at Sunnylands and the Institute for Information Law of the University of Amsterdam,
with support from the Embassy of the Kingdom of the Netherlands in Washington, D.C.

TRANSATLANTIC WORKING GROUP

An Examination of the Algorithmic Accountability Act of 2019[†]

Mark MacCarthy, Georgetown University[1]

October 24, 2019

Contents

Introduction

The Algorithmic Accountability Act of 2019, sponsored by Senators Cory Booker (D-NJ) and Ron Wyden (D-OR), with a House equivalent sponsored by Rep. Yvette Clarke (D-NY), requires companies to assess their automatic decision systems for risks to "privacy and security of personal information" and risks of "inaccurate, unfair, biased, or discriminatory decisions." They must also "reasonably address" the results of their assessments. The bill empowers the Federal Trade Commission (FTC) to resolve by regulation the crucial details of these requirements. It is not likely to pass Congress on its own, but it might become part of a new national privacy law currently under consideration in Congress. If passed, it would apply to the AI systems that platforms increasingly deploy to detect and counter hate speech, terrorist material and disinformation campaigns and would require the platforms to conduct fairness assessments of these AI systems and fix issues of bias uncovered in these studies. Even without a legislative mandate, however, platforms should rigorously review algorithmic content moderation systems for fairness and accuracy and should establish and

[†] One in a series: A working paper of the Transatlantic Working Group on Content Moderation Online and Freedom of Expression. Read about the TWG: https://www.ivir.nl/twg/.

maintain effective, easy-to-use complaint mechanisms whereby people wrongly labeled as purveyors of harmful material can obtain redress.

Summary of the Bill

On April 10, 2019, Senators Booker and Wyden introduced S. 1108, the Algorithmic Accountability Act of 2019.[2] Rep. Clarke introduced an identical companion bill, H.R. 2231, in the House.[3] The Senate bill was referred to the Senate Commerce Committee while the House bill went to the House Energy and Commerce Committee, the committees that will deal with privacy legislation later this year.

The bill contains an exemption for small businesses. It would apply to companies under the FTC's jurisdiction that make more than $50 million per year in gross receipts or have data for at least 1 million people or devices. It would also apply to "data brokers" (a company that "collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell or trade the information or provide third-party access to the information") regardless of their revenue or the number of people whose data they hold.

The bill would direct the Federal Trade Commission to pass regulations within two years to require these companies to conduct studies of their high-risk automated decision systems "for impacts on accuracy, fairness, bias, discrimination, privacy, and security." Companies must conduct an assessment for new systems "prior to implementation" and for existing systems "as frequently as the Commission (FTC) thinks is necessary." These impact assessments may be made public, but need not be, at the "sole discretion" of the company. They must conduct these assessments "if reasonably possible, in consultation with external third parties, including independent auditors and independent technology experts" and must "reasonably address in a timely manner the results of the impact assessments."

An automated decision system is a "computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers."

Companies must conduct assessments only for their "high-risk" automated decision systems. An automated decision system is high-risk if it satisfies *any* of the following conditions:

- It poses "a significant risk to the privacy or security of personal information ... or of resulting in or contributing to inaccurate, unfair, biased, or discriminatory decisions impacting consumers."
- It "makes decisions, or facilitates human decision making" that "alter legal rights of consumers … or otherwise significantly impact consumers" when these decisions are based on "attempts to analyze or predict sensitive aspects of their lives, such as their work performance, economic situation, health, personal preferences, interests, behavior, location, or movements."
- It "involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests."

- It "systematically monitors a large, publicly accessible physical place."
- It "meets any other criteria established by the Commission in regulations…"

The bill also requires companies to conduct a "data protection impact assessment" for "high risk information systems." An information system is a database that "involves personal information, such as the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, sharing, disclosure, dissemination, combination, restriction, erasure, or destruction of personal information." An information system is high risk when it poses significant risks to the privacy or security of personal information, or as above when it collects sensitive information, monitors a large, public space, or meets other criteria established by the commission. A data protection impact assessment is narrower than an automated data system impact assessment, focusing only on "the extent to which an information system protects the privacy and security of personal information the system processes."

The bill's basic requirement to conduct impact assessments systems appears to be modeled on several provisions of the European General Data Protection Regulation (GDPR). Article 22 of the GDPR provides for a right for a data subject "not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."[4] Article 35 requires companies to conduct "data impact assessments" of the risks of data processing operations "to the rights and freedoms of natural persons" and their effect "on the protection of personal data."[5]

The FTC is provided substantial authority to enforce the provisions of the bill, treating violations as if they were violations of rules defining "unfair and deceptive practices" under its authorizing statute. The bill does not allow the FTC to exceed its current authority in drafting implementing rules or its enforcement actions.

Despite much discussion of the need for companies to disclose the source code or the formula of their algorithms and to provide explanations of machine learning algorithms,[6] the bill makes no such demand on companies. The bill requires companies to assess their algorithms for conformity to various standards such as privacy, security, and fairness. But under the proposed bill, they can keep their formulas and source code secret, and they need not provide explanations of how they work. It would not be too hard, however, to add transparency and explainability requirements to the bill if it began to move through the congressional process.

Interpretation of the Bill

Under the proposed bill, the FTC has broad authority to define the key terms in the requirement to conduct impact assessments – discrimination, bias, unfairness, privacy and security. It is likely that the FTC would think of the requirement to avoid unfairness in terms of its current authority to prevent companies from engaging in an unfair act or practice, that is, an act or practice that "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[7]

The FTC has brought cases under its unfairness authority in connection with several types of informational injury including financial harm, physical injury, reputational harm and unwanted intrusion.[8] Companies conducting algorithmic assessments covered by the FTC's rules developed under the new law would likely have to include whether the use of the algorithms in company decisions would cause or be likely to cause harms of this nature.

The mandate for companies to conduct analyses for bias and discrimination is different. It would be new to the FTC, but it is not new for companies that already need to comply with a range of U.S. laws forbidding discrimination against protected classes in a variety of contexts. The current anti-discrimination laws prohibit discrimination against protected groups in employment,[9] credit,[10] housing,[11] use of genetic information,[12] and health care and health insurance.[13]

The use of disparate impact analyses in anti-discrimination law is complex and controversial.[14] But companies often conduct these analyses to assess and control legal risk of non-compliance with current anti-discrimination laws. In general a disparate impact assessment analysis has three stages: evidence of a disproportionate impact caused by a policy or procedure; assessment of whether and to what extent the policy or procedure serves a valid purpose; and assessment of whether there are alternative policies or procedures that would achieve the legitimate objective with a less disparate impact.

For instance, a potential legal risk in the employment context would be the presence of a disproportionate adverse effect on a protected class that takes place unintentionally through a policy, procedure or decision algorithm that does not base a hiring or promotion decision explicitly on protected class status. Potential violations of statistical parity in employment contexts can be detected by a company study assessing compliance with the 80% rule of thumb, which suggests, for instance, that if a company hires 10% of white applicants then it should hire no less than 8% of African American applicants.[15]

Companies frequently conduct disparate impact analyses to determine if their decisions depart from statistical parity among protected groups, and if so, whether there are legitimate reasons for this departure and alternative decisions procedures that would create less impact. This is what happened with Amazon's attempt to develop a hiring algorithm for software engineers. It experimented with using historical data to train an automated method of selecting promising applicants, did disparate impact analyses, found that these algorithmic results disproportionately rejected women, and fixed the factors that were leading to this disparate impact but encountered others it could not fix. Aware of the legal risk under current laws that bar discrimination on the basis of sex, the company wisely used the conclusions of its disparate impact analysis to abandon that attempt at recruitment automation. [16]

The FTC is likely to interpret the mandate in the proposed law for companies to review an algorithm for bias and discrimination as similar to the way in which companies currently conduct disparate impact analysis under existing anti-discrimination law. This would mean an extension of the range of areas in which companies might be required to conduct these analyses beyond what is already required under current law.

It is possible that the law is intended to remedy a purported exemption from these laws for algorithms. The press statement accompanying the introduction of the bill suggests this, saying, "Algorithms shouldn't have an exemption from our anti-discrimination laws."[17] But algorithms do not have such an exemption. Current anti-discrimination laws cover the use of old-fashioned statistical methods such as regression analysis to assess people, as well as the most up-to-date machine learning techniques.[18]

The press release also cites action brought against Facebook for discrimination in housing ads. But that action was brought under the Fair Housing Act and clearly demonstrates that the Fair Housing Act covers discriminatory housing ads that use targeting algorithms. In announcing the action against Facebook, Ben Carson, Secretary of Housing and Urban Development, said, "Using a computer to limit a person's housing choices can be just as discriminatory as slamming a door in someone's face."[19]

So it is most likely that the bill is aimed at uses of algorithms that are close to the line in terms of current discrimination law, or are not covered at all under current law.[20] Is it illegal for a financial institution to tailor its online website so that the best credit card offers appear to people who seem to be the best credit risks? Is it a violation of employment discrimination law when women are less likely than men to be shown ads for high-paying jobs? Is a facial recognition program that is less accurate for blacks than for whites discriminatory? The law is less than clear in these areas, and the proposed bill might best be interpreted as a directive to the Federal Trade Commission to provide clarity.

But such clarifications are not in the bill itself. The proposal does not specify that any particular uses of algorithms are discriminatory. Its definitions are broad enough to include such common uses of algorithms as ad targeting, facial recognition, search engines, fraud detection systems, and identity verification systems. But its key terms of bias, discrimination and unfairness are left up to the FTC to define.

There are other matters that the FTC will have to clarify in implementing regulations. For instance, what will define whether consultation with external third parties in the conduct of assessments is "reasonably possible?" Will the FTC define the circumstances or leave it up to the companies?

Probably most important is the unresolved question of what companies might have to do to "reasonably address … the results of the impact assessments." In the case of an ad for high-paying jobs that target men, the agency could conclude that the only way to "reasonably address" the harm of employment ads targeted at men would be to alter them so that they preserved statistical parity for men and women – the chances of a man getting the ad have to be approximately the same as the chances of a woman getting the same ad. This would be a substantial intrusion into the ad marketplace, but it seems to be clearly within the authority granted to the FTC under the proposed legislation.

Effect on Content Moderation Programs

The bill does not directly affect content moderation programs and their content rules regarding hate speech, terrorist material and disinformation campaigns. But platforms increasingly rely on algorithms to identify and counter harmful speech. The proposed bill could indirectly affect the content moderation programs established by platforms through its requirement to conduct algorithmic assessments of these content moderation algorithms and its further authority to require unspecified fixes based on the results of these assessments.

These content moderation algorithms clearly fit the bill's definition of high-risk automated decision systems. These algorithms might make or contribute to a decision that certain people are likely to be part of a hate group, disinformation campaign or terrorist plot through a computerized analysis of their "interests, behavior, location or movements." Such a determination could certainly "significantly impact" these people, for instance, through barring them from access to the platform, and might even alter their "legal rights" if their identifying information was turned over to law enforcement. A platform's automated methods of detecting harmful content might also affect the privacy of platform users by collecting large amounts of information and making inferences to sensitive attributes.

FTC regulations under the new law are likely to require assessments of the accuracy, fairness and disparate impact of content moderation algorithms. They will not require disclosure of the source code or the formula, or a requirement for explanation of the operation of these algorithms. Under the law, these assessments can be made public only with the consent of the platforms conducting them, but it is highly likely that the FTC will require access to the results of the studies and maybe even to the studies themselves.

It is not clear what the FTC will require in terms of the results of these assessments. They will at minimum examine whether the data gathered as part of the development of these algorithms is consistent with FTC privacy guidelines and conformity to the requirements of the new privacy law Congress is considering, which would likely provide FTC with new enforcement authority.

The commission will also likely examine whether a particular use of an algorithm in content moderation decisions is an unfair practice and whether it causes or is likely to cause substantial injury to consumers that they cannot reasonably avoid and has no compensating benefit. In doing this, it is likely to consider the various informational injuries – financial harm, physical injury, reputational harm and unwanted intrusion – that it has considered in past cases.

The commission will examine whether the platforms' assessments of their content moderation algorithms reveal actionable disparate impact under new discrimination standards that the commission has developed. For instance, platforms using algorithms that disproportionately identify users from a protected class as more likely to post material violating platform content rules might need to engage in special scrutiny of these algorithms and justify their use both in terms of their accurate contribution to content moderation goals and the demonstrated lack of alternative algorithms that achieve that purpose with less impact on protected classes.

It might be possible for the FTC to examine the political neutrality of a content moderation program under the requirement for algorithmic fairness. For instance, the FTC might require platforms to examine their measures to address political disinformation campaigns to see whether they affected campaigns of Democrats and Republicans alike, and under its new regulations it might require demonstrating that any political disparate impact was the smallest consistent with an effective program to counter disinformation campaigns.

However, this is so far from the FTC's core mission that it is unlikely to do so under the bill as it is currently written. But a political neutrality requirement could be added in further consideration of the bill.

Political Assessment

In the one public reaction to the bill's introduction, law scholars Margot Kaminski and Andrew Selbst praised the bill, but suggested several improvements.[21] They suggest that the bill provide for additional enforcement and a clearer statement that algorithmic bias is illegal. They also argue that the bill needs greater public input and providing public audits only when "reasonably possible" is too narrow. Third, they suggest greater transparency in the assessments. They recognize that full transparency might jeopardize trade secrets and allow hostile actors to game the system and suggest an FTC report as one way to provide more openness while still allowing for more transparency.

These suggested improvements might be the enemy of the good. The chances that Congress will act on the bill as introduced are slim. The authors are all Democrats in a Senate controlled by Republicans. In the absence of a single Republican cosponsor, Republican committee chairs are unlikely to hold hearings on the bill or schedule it for a markup. Republican Senate leadership would not be likely to provide floor time for the bill without strong support by senior Republican senators. In the House, the lone sponsor is the Vice Chair of the House Energy and Commerce Committee, to which her bill was referred for action. She is thus well-positioned to encourage subcommittee and full committee chairs to hold hearings and markups on her bill. She cannot, however, schedule this on her own initiative.

As a result, the bill is unlikely to move on its own. It might however be an element of a larger privacy bill that is currently under consideration in both the House and Senate. The bill's focus on the bias, discrimination and unfairness in automated decision systems is mirrored in a draft bill proposed by Intel.[22] In addition, draft legislation from the privacy advocacy group the Center for Democracy and Technology instructs the FTC "to define and prohibit unfair targeted advertising practices," a specific use of an automated decision system that is also addressed in the algorithmic accountability proposal.[23] Finally, Congress is looking for guidance to Europe's GDPR, which, as previously noted, has a similar requirement as this bill with regard to automated decision systems.

Prospects are better in the House than in the Senate for attaching the bill to privacy legislation. The House bill has 26 cosponsors including Rep. Karen Bass (D-CA), the Chair of the Congressional Black Caucus, and a substantial number of caucus members have shown concern over algorithmic bias and the inadequacies of current law in dealing with it. This group has the political clout in the House to block movement on privacy legislation unless it includes measures addressing algorithmic bias.

In sum, Congress is considering the issues raised by the bill in regard to the fairness, accuracy and privacy of automated decision systems as it contemplates passage of a new national privacy law. The bill's most likely path to becoming law is by having significant elements of it become part of this larger privacy law. As mentioned earlier, additions to the bill requiring explanations, transparency and political neutrality might emerge during the political horse-trading that characterizes the movement of any complex legislation through Congress.

Conclusion and Recommendations

Platforms are properly focused on developing algorithms that can help them identify and counter harmful material on their systems. This is especially important for hate speech, disinformation campaigns and terrorist material that can have harmful effects on other platforms and in the real world.

The Algorithmic Accountability Act of 2019 should remind platforms, however, that decisions to remove content and to take action against people who post content in violation of their terms of service can pose significant risks of harm to people if they are based on inaccurate or unfair automated systems. As a result of content moderation decisions, users can be barred from platforms; their names might be entered into shared databases that could form the basis for widespread denial of platform services; and their personal information might be turned over to law enforcement or security officials for prosecution or further surveillance. If these actions are taken in error more often for users in a protected class, for instance, this might exacerbate already substantial disparate impacts experienced by members of vulnerable groups.

One recommendation that emerges from this consideration of the bill is that even if it does not become law, systematic assessments of the AI systems used to detect harmful content – to ensure the greatest possible fairness and accuracy – would be a valuable addition to platform content moderation programs. A further recommendation would be to assess the tradeoffs platforms have to make between taking down harmful material in error and leaving up harmful material in error, taking into account the damage that can be done to a person's reputation and opportunities by wrongfully designating that person as a member of a hate group, terrorist organization or disinformation campaign. Because such mistakes will inevitably occur in complex systems like social media platforms, there need to be robust redress mechanisms through which people wrongfully labeled as purveyors of harmful material can clear their names.

Notes

[1] Mark MacCarthy is adjunct professor at Georgetown University, where he teaches courses in the Graduate School's Communication, Culture, and Technology Program and in the Philosophy Department. He is also Senior Fellow at the Institute for Technology Law and Policy at Georgetown Law, Senior Policy Fellow at the Center for Business and Public Policy at Georgetown's McDonough School of Business and Senior Fellow with the Future of Privacy Forum.

[2] S. 1108 – 116th Congress: Algorithmic Accountability Act of 2019, https://www.congress.gov/bill/116th-congress/senate-bill/1108.

[3] H.R. 2231 – 116th Congress: Algorithmic Accountability Act of 2019, https://www.congress.gov/bill/116th-congress/house-bill/2231?q=%7B%22search%22%3A%5B%22yvette+clarke%22%5D%7D&s=5&r=12.

[4] See Article 22 of GDPR, available at https://gdpr-info.eu/art-22-gdpr/.

[5] See Article 35 of GDPR, available at https://gdpr-info.eu/art-35-gdpr/. A data impact study is "particularly required" in the case of "automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person" or sensitive information, or monitoring of a large public area. See also Article 29 Working Group, Guidelines on Data Protection Impact Assessment, October 13, 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236. I'm grateful to Joris van Hoboken for pointing out this connection to Article 35.

[6] For instance, Articles 13–15 of GDPR provide rights to "meaningful information about the logic involved" in automated decisions.

[7] 15 U.S.C. § 45(n). Section 3(d)(1) of the bill supports this interpretation by mandating the Commission to treat a failure to conduct an impact assessment required under the Commission's rule as "as a violation of a rule defining an unfair or deceptive act or practice" under the Federal Trade Commission Act.

[8] Federal Trade Commission, Staff Comments to NTIA on Consumer Privacy, November 13, 2018, pp. 8-9, https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-ntia-developing-administrations-approach-consumer-privacy/p195400_ftc_comment_to_ntia_112018.pdf.

[9] Title VII of the Civil Rights Act of 1964 makes it unlawful for employers and employment agencies to discriminate against an applicant or an employee because of such individual's "race color, religion, sex, or national origin." It is enforced by the Equal Employment Opportunity Commission and state fair employment practices agencies. See 42 U.S.C. §2000e-2 available at http://www.law.cornell.edu/uscode/text/42/2000e-2.

[10] The Equal Credit Opportunity Act makes it unlawful for any creditor to discriminate against any applicant for credit on the basis of "race, color, religion, national origin, sex or marital status, or age 15 U.S.C. § 1691 available at http://www.law.cornell.edu/uscode/text/15/1691. The Federal Reserve Board originally enforced the Equal Credit Opportunity Act, but the Dodd-Frank Act of 2011 transferred jurisdiction to CFPB. See Consumer Financial Protection Bureau, CFPB Consumer Protection Laws: ECOA, June 2013, p. 1 available at: https://files.consumerfinance.gov/f/201306_cfpb_laws-and-regulations_ecoa-combined-june-2013.pdf.

[11] Title VIII of the Civil Rights Act of 1968, the Fair Housing Act, prohibits discrimination in the sale, rental or financing of housing "because of race, color, religion, sex, familial status, or national origin." The act also protects people with disabilities and families with children. It is enforced by the Department of Housing and Urban Development. 42 U.S.C. 3604 available at http://www.law.cornell.edu/uscode/text/42/3604.

[12] The Genetic Information Nondiscrimination Act of 2008 prohibits U.S. health insurance companies and employers from discriminating on the basis of information derived from genetic tests. Pub. L. No. 110-233, 122 Stat. 881 available at https://www.govinfo.gov/content/pkg/PLAW-110publ233/pdf/PLAW-110publ233.pdf.

Enforcement is divided among a number of agencies including the Department of Health and Human Services (for health insurance) and the Equal Employment Opportunity Commission (for employment).

[13] Section 1557 of the Affordable Care Act of 2010 prohibits discrimination in health care and health insurance based on race, color, national origin, age, disability, or sex. 42 U.S.C. § 18116, available at https://www.law.cornell.edu/uscode/text/42/18116.

[14] For a discussion, see Software & Information Industry Association, Algorithmic Fairness, 2017, pp. 8-12.

[15] "A selection rate for any race, sex, or ethnic group which is less than four-fifths (or 80%) of the rate for the group with the highest rate will generally be regarded by the Federal enforcement agencies as evidence of adverse impact…" Uniform Guidelines on Employee Selection Procedures (1978), 29 C.F.R. § 1607.40 (1987), available at http://uniformguidelines.com/uniguideprint.html.

[16] Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," Reuters, October 9, 2018 at https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

[17] Wyden, Booker, "Clarke Introduce Bill Requiring Companies To Target Bias In Corporate Algorithms," April 10, 2019 at https://www.wyden.senate.gov/news/press-releases/wyden-booker-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms-.

[18] The Obama Administration recognized this when they recommended that regulatory agencies "should expand their technical expertise to be able to identify practices and outcomes facilitated by big data analytics that have a discriminatory impact on protected classes, and develop a plan for investigating and resolving violations of law in such cases." See Executive Office of the President, "Big Data: Seizing Opportunities, Preserving Values," May 2014, p. 60 available at https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. The Consumer Financial Protection Bureau claimed jurisdiction over the company Upstart that used alternative data and algorithms to assess lending decisions with respect to compliance with the Equal Credit Opportunity Act. See Consumer Financial Protection Bureau, CFPB Announces First No-Action Letter to Upstart Network Company to Regularly Report Lending and Compliance Information to the Bureau, September 14, 2017, https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-first-no-action-letter-upstart-network/.

[19] Katie Benner, Glenn Thrush and Mike Isaac, "Facebook Engages in Housing Discrimination With Its Ad Practices, U.S. Says" New York Times, March 28, 2019, at https://www.nytimes.com/2019/03/28/us/politics/facebook-housing-discrimination.html.

[20] The press release says the bill targets discrimination such as the "houses that you never know are for sale, job opportunities that never present themselves, and financing that you never become aware of – all due to biased algorithms."

[21] Margot E. Kaminski and Andrew D. Selbst, "The Legislation That Targets the Racist Impacts of Tech; A proposed law would make big companies determine whether their algorithms discriminate, but it's lacking in some big ways," New York Times, May 7, 2019, https://www.nytimes.com/2019/05/07/opinion/tech-racism-algorithms.html.

[22] Section 4 of the draft bill requires companies to conduct a study to ensure that their automated decision processes are "reasonably free of bias and error," https://usprivacybill.intel.com/wp-content/uploads/IntelPrivacyBill-01-28-19.pdf.

[23] Section 6 of the draft bill contains this instruction to the FTC, https://cdt.org/files/2018/12/2018-12-12-CDT-Privacy-Discussion-Draft-Final.pdf.