CS 182: Ethics, Public Policy, and Technological Change

Rob Reich
Mehran Sahami
Jeremy Weinstein
Ece Korkmaz (Co-Head TA)
Alena Smith (Co-Head TA)
Today’s Agenda

1. Navigating trade-offs
2. Mapping policy and legal approaches
3. Making them work: technical considerations
4. Making them work: social scientific considerations
5. Should we be satisfied with tweaking the system?
New York City Council

OPEN THE CODE
epic.org/algorithmic-transparency

Source: Craig Warga, New York Daily News, Electronic Privacy Information Center
An Ambitious Proposal

The proposed Algorithmic Accountability bill would:

- Require city agencies to publically release the source code of all algorithms they use to make their decisions
- Allow members of the public to “self-test” the algorithms by submitting their own data and getting the results

In committee, the bill was watered down to:

- Establish a task force that would examine exactly what algorithms are in use and whether any appear to discriminate
- It would also make recommendations on how to help New Yorkers understand algorithms and challenge their results.
A Glass Half Full? Or Half Empty?

The NYC task force recommended that NYC:

- Establish org. structure and guidance for overseeing use of ADS; provide resources and support to agencies
- Broaden public discussion of ADS
- Formalize agency reporting on ADS, establish single point of inquiry, create process for assessing harm

The critics argue that more ambition was needed including:

- Process for public consultation before ADS is designed/acquired
- Clear standard and process for regularly assessing disproportional impact, responding if discovered (incl. right of private action)
- Formal procedures for explanation of decisions within 20 days
- Transparency requirements
Put Yourself in Their Shoes

Now imagine you are the Mayor having received the task force recommendations. What position would you take?

• Would you accept the recommendations as is? Why or why not?
• If not, what would you prioritize in terms of strengthening the recommendations?
• Why would you prioritize these things?
• What gives you confidence that these mechanisms would be effective?
Criteria

1. Does it work? (Efficiency to achieve public safety)
2. Is it fair? (Fairness)
3. Can people understand how it works? (Transparency)
4. Can people appeal its judgment? (Due Process)
5. Does it use information that an individual might reasonably expect to remain private? (Privacy)

Today we are going to focus on how we balance the value of an algorithm in terms of achieving public safety against other values beyond fairness.

It means asking: What else do we value? How do we encode that in law or policy?
Today’s Agenda

1. Navigating trade-offs
2. Mapping policy and legal approaches
3. Making them work: technical considerations
4. Making them work: social scientific considerations
5. Should we be satisfied with tweaking the system?
What Should We Do About Algorithms?

Substantive fairness is context-dependent. It depends on some social understanding of what fairness requires.

- That’s a hard problem to solve. But it isn’t a technical problem. It demands engagement in politics.

Procedural fairness is distinct from substantive fairness. We can envision what we might want a process to look like, especially from an “original position” (e.g. without knowing our own characteristics).

- This is what a lot of policy efforts are focused on. But the devil is still in the details.
Who Should be Governing?

If algorithms are doing (or have the potential to do) harm, who should we rely on to fix the problem?

- The workers who create the algorithms
- The companies that hire the workers
- The industries in which companies are organized
- The consumers who use the technologies
- The non-users impacted by new technologies
- The government which sets and enforces rules in the place where the new technologies are built/deployed

How does your answer differ depending on whether the algorithm is being used by a company or a government agency?
Relying on Companies

How dominant?
Global market share
April 2018, %

Search
- Google 91%
- Smartphone web traffic
  - Apple 45%

Social media
- Facebook 66%
- Online retail
  - Amazon 37%

Source: Global Stats Counter

How confident are you in relying on companies to...

- To regulate themselves?
- To self-regulate as an industry?
- To be responsive to user pressure?
- To be responsive to their own employees?

“Governments should intervene, at a minimum, when private action has negative public consequences; when shortsighted actions threaten to cause long-term harm; when failure to intervene undermines significant constitutional values and important individual rights; when a form of life emerges that may threaten values we believe to be fundamental; and when we can see that failing to intervene on the side of right will simply strengthen the interventions on the side of wrong.”

-- Larry Lessig, *Code 2.0*
Relying on Democratic Politics


Source: Kleptocracy Now
Maybe the Courts Will Save Us?

• The proprietary nature of COMPAS has been invoked to prevent disclosure of information relating to how factors are weighed or how risk scores are determined.
• Because COMPAS risk assessment scores are based on group data, they are able to identify groups of high-risk offenders – not a particular high-risk individual.
• Some studies of COMPAS risk assessment scores have raised questions about whether they disproportionately classify minority offenders as having a higher risk of recidivism.
• A COMPAS risk assessment compares defendants to a national sample, but no cross-validation study for a Wisconsin population has yet been completed.
• COMPAS was not developed for use at sentencing, but... for determinations regarding treatment, supervision, and parole.

Source: Public Domain
FAccT to the Rescue!

ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT)

A computer science conference with a cross-disciplinary focus that brings together researchers and practitioners interested in fairness, accountability, and transparency in socio-technical systems.

Three Critical Levers

Transparency.
What data is used? What results are generated? What is the underlying source code? What is the logic for the result?

Auditing.
Can independent experts test the algorithm? Who chooses them? What happens to their input? Is it made public?

Due process.
What results were generated for me? What data of mine was used? What if the algorithm is wrong? To whom can I appeal the algorithmic decision?
Running Into Tradeoffs

- Accuracy vs. fairness
- Accuracy vs. interpretability
- Accuracy vs. privacy
- Safety vs. transparency
- Safety vs. autonomy
- Etc...
Today’s Agenda

1. Navigating trade-offs
2. Mapping policy and legal approaches
3. Making them work: technical considerations
4. Making them work: social scientific considerations
5. Should we be satisfied with tweaking the system?
Algorithm Interpretability

• What makes an algorithm *interpretable*?
  • Ability to scrutinize source code?
  • Understanding results from algorithm?
  • Understanding general “logic” of the algorithm?

• Consider initial version of NYC Council bill
  • Required city agencies to publicly release the source code of algorithms they use to make their decision
  • In Assignment #1, we start by asking you to consider potential bias of algorithm by just scrutinizing the code
  • How feasible do you think that is?

• And now, it’s *Possibly Apocryphal Story Time*!
  • Show me the tanks!
Zech et al (2018) examine deep learning models for making disease diagnoses from chest x-rays
- Neural network is weighting features of x-ray machine
- Portable machines are more likely to be used with sick patients (who can't come to the hospital)
- This creates a confound for trying to deploy real systems and can lead to misleading results

Source: John Zech (2018), “What are radiological deep learning models actually learning?”, Medium, pictures on the left altered by adding red boxes for emphasis. Picture on the right altered by creating heat maps. “To create the heatmaps, [Zech] use[s] the activations of Zhou et al 2015 and convert them into a probability for each of the 7x7 subregions as described in [his] preprint. I then calculate ln(p_subregion / p_baseline) for each of the 7x7 subregions, where p_subregion is the probability of disease based on that subregion and p_baseline is the population baseline probability of the disease.” See this pre-print for reference: https://arxiv.org/pdf/1807.00431.pdf
Interpretability vs. Accuracy

• How do we trade-off interpretability vs. accuracy?
  • Generally, more complicated model can be more accurate
  • Some models are more interpretable than others (e.g., a linear function, versus a set of rules, versus a neural network)
  • Hard/impossible for human to understand sufficiently complex models
    • It’s essentially a “opaque box” even if we have access to the code
  • Sometimes, we learn a simpler (or more readily understood) model to approximate the function in a complex model

• How should we weigh interpretability?
  • Importance of transparency and due process
  • E.g., decisions in the legal system

• How should we weigh accuracy?
  • Importance of outcomes
  • E.g., product recommendations
Interpretability via Outcomes

• Accounting for outcomes (outcome-based explanation)
  • How particular inputs lead to particular outputs

• Legal requirement for credit scoring by Fair Credit Reporting Act (FCRA)
  • E.g., You have a right to know factors that impact your FICO score

• Adverse action notice
  • When credit denied, you must be given specific reason for denial
  • Idea is to alert and educate the consumer about credit

• Can’t make credit decision based on protected attributes
  • But, proxy attributes can still be possible inputs (even in explanation)
Interpretability via Logic

• Logic of decision-making (logical explanation of result)
  • Need to provide description of “rules” in the system

• European General Data Protection Regulation (GDPR) requires access to “meaningful information about the logic involved” in automated decision-making that impact data subject
  • In case you were wondering, you are the “data subject”
  • More about GDPR later

• Seems more transparent, but potentially more problematic
  • What is suitable “logic” for decision?
  • Can someone explain who can see my Facebook post if I post a picture tagging a friend who only allows her friends to see posts on her feed, but I let anyone see mine?
  • How about why Google showed me a particular set of search results?
Auditing Algorithms

• Basic idea of audit: field study to diagnose harmful discrimination/impacts from a decision-making process
  • E.g., Send the same resume with “male” or “female” name to see if there is a difference in interview rates

• Note: algorithms are embedded in software systems/platforms
  • In many cases, we are really auditing the platform, not just a single algorithm in it, which can create more complexity

• Auditing of algorithms/platforms can take different forms
  • We’ll consider five from Sandvig et al (2014): “Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms”
1. Code Audit

- Platform makes underlying algorithm available to auditor
  - Could open source code (i.e., everyone is auditor)
  - Could put algorithm in safe escrow (i.e., designated auditors)

- Provides algorithmic transparency at source code level
  - Essentially, what question 1 of your assignment is about

- Doesn’t necessarily provide data algorithm was trained on
  - That’s why your assignment doesn’t stop after question 1
  - Providing training data can be a privacy concern
    - We’ll talk much more about data privacy in the next unit
Some Machine Learning Architectures

- Accessing algorithm ≠ understanding how decisions are made
  - High-dimensional, non-linear, non-monotonic, discontinuous functions

\[ x_1, w_1, x_2, w_2, x_3, w_3, x_4, w_4 \rightarrow d(X) \]

Perceptron

\[ \text{LeNet-5 Deep Neural Network architecture} \]

Proprietary Algorithms

- Algorithm can be core intellectual property of company
  - E.g., Email spam filter, Google ranking algorithm

- Release of algorithm could be untenable
  - Gaming/spamming of platform
  - Release of trade secrets to competition
  - Outright theft/copying

2. Noninvasive User Audit

- Auditors ask users to give them results of using platform
- Generally, not randomized in condition assignment
  - Difficult to focus on what you believe may be discriminatory
- Sampling bias
  - Which users you have access to
  - Which users agree to share results with you
  - (Very) limited sample size
- Results from platform may be too sensitive in some domains
  - Finance, healthcare, criminal justice, etc.
3. Scraping Audit

- Auditors scraps results from platform using program/script
- Potentially violates US Computer Fraud and Abuse Act (CFAA)
  - Criminalizes unauthorized access to computer systems
- Likely to violate platform’s “Terms of Service”
- Should platforms provide an API (or modify their terms of service) to enable this?
  - How do you protect the platform from abuse?
  - Was Cambridge Analytica just auditing Facebook?
4. Sock Puppet Audit

- Auditors create “false users” (sock puppets) to interact with platform
  - E.g., Has been used to test if there is bias in Facebook ad targeting
- Does it violate US Computer Fraud and Abuse Act (CFAA)?
  - Injecting “false” data into system (e.g., fake profiles in Facebook)
- Likely to violate platform’s “Terms of Service”
- Is this reasonable?
- Will it scale?

A federal judge recently held that researchers who violate a website’s terms of service by creating fake online accounts in order to study algorithmic bias in artificial intelligence software do not violate the Computer Fraud and Abuse Act (“CFAA”).

Several of the researchers had created fake employer and employee accounts in order to study the algorithms used by various websites (such as LinkedIn). The researchers were particularly interested in determining whether the algorithms discriminated against applicants on the basis of protected characteristics, such as sex, age, or race.

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

5. Crowdsourced Audit

- Auditors crowdsource real users to interact with platform
- Likely does **not** violate US Computer Fraud and Abuse Act
- Likely does **not** violate platform’s “Terms of Service”
- Does paying confederates change things?
- What if confederates were paid to click on ads?
Crowdsourced Auditing in Action

- TechCrunch, Jan 15, 2019
- Activists in Germany crowdsourcing credit scores (Schufa)
- OpenSchufa: project where users donate their financial data from Schufa
  - 3,000+ data donations


Source: re:pubica, Wikimedia Commons (CC-BY 2.0)
Canada has launched an Algorithmic Impact Assessment tool.

- Scorecard to highlight issues in design and deployment of automated decision-making (ADM).
- "Unspoken expectation... that any government entity is to use this tool... to supervise, control, and mitigate potential issues with the deployment of an ADM system."

Source: https://towardsdatascience.com/understanding-canadas-algorithmic-impact-assessment-tool-cd0d3c8cafab
Changes in the Law

Auditing algorithms. It’s not just a good idea...

It’s the law!

NYC Targets Artificial Intelligence Bias in Hiring Under New Law
By Erin Mulvaney
Bloomberg Law, Dec. 10, 2021

Employers in the city will be banned from using automated employment decision tools to screen job candidates, unless the technology has been subject to a “bias audit” conducted a year before the use of the tool.

Companies also will be required to notify employees or candidates if the tool was used to make job decisions.

Illinois previously passed a measure similar to New York City’s to crack down on the use of such technology in employment decisions.... The attorney general in the Washington, D.C. announced Thursday proposed legislation that would address “algorithmic discrimination” and require companies to submit to annual audits about their technology.

The Data & Trust Alliance, tapping corporate and outside experts, has devised a 55-question evaluation, which covers 13 topics, and a scoring system. The goal is to detect and combat algorithmic bias.

“This is not just adopting principles, but actually implementing something concrete,” said Kenneth Chenault, co-chairman of the group and a former chief executive of American Express, which has agreed to adopt the anti-bias tool kit.

The companies are responding to concerns, backed by an ample body of research, that A.I. programs can inadvertently produce biased results.
Proposal From Microsoft President

• Brad Smith, President and Chief Legal Officer at Microsoft, has proposed a marketplace solution

• He claims that no one wants unfair algorithms

• Have companies evaluate their algorithms on a standard benchmark using a public dataset and report the results

• Consumers can choose to purchase/use the algorithm they deem best, given fairness results, price, etc.

• Do you think this is a reasonable proposal?
Today’s Agenda

1. Navigating trade-offs
2. Mapping policy and legal approaches
3. Making them work: technical considerations
4. Making them work: social scientific considerations
5. Should we be satisfied with tweaking the system?
The GDPR – A New Model

Better protection for personal data

- Clear consent required to process data
- Limits on the use of automated processing of data to make decisions, for example in the case of ‘profiling’
- Right to rectify and remove data, including the 'right to be forgotten' for data collected as a child
- Right to notification if data is compromised
- More and clearer information about processing
- Easier access to personal data
- Right to move data from one service provider to another
- Stricter safeguards for transfers of personal data outside the EU

Source: European Union/Council of the European Union (2015), “Infographic - Data protection regulation,” (Reproduction authorized as long as source is acknowledged). Modified by cropping to focus on a specific section.
The “Right to Explanation”

- Key GDPR provisions around algorithmic decision-making
  - A right not to be subject to algorithmic decision-making, except under specified circumstances
  - A right to obtain human intervention, to respond, and to contest any decision
  - A right to information about the data that is used, including one’s own personal information
  - A right to explanation about the logic involved in the decision
The Problem(s) with Transparency

It is simply one input into a complex decision-making process for individuals & groups.

Someone needs to pick up the information and run with it.

Who will do that, when, and why?

Making Audits Work

A ton of decisions are involved in making an auditing system work.

1. Who is the auditor?
2. How many are there?
3. Who selects them?
4. Who pays their salary?
5. Who do they report to and how?
6. Are there sufficient resources to get excellent auditors?
7. What happens to the findings of the auditor?
8. Who receives them?
9. What triggers a response and from whom?
“If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself.”

-- James Madison, Federalist Papers No. 51
Due Process for Whom?

Whites and blacks don’t see eye to eye on whether blacks are treated less fairly in a variety of settings

% of whites and blacks saying, in general in our country these days, blacks are treated less fairly than whites in each of the following situations

<table>
<thead>
<tr>
<th>Situation</th>
<th>White</th>
<th>Black</th>
</tr>
</thead>
<tbody>
<tr>
<td>In dealing with the police</td>
<td>63</td>
<td>84</td>
</tr>
<tr>
<td>By the criminal justice system</td>
<td>61</td>
<td>87</td>
</tr>
<tr>
<td>In hiring, pay and promotions</td>
<td>44</td>
<td>82</td>
</tr>
<tr>
<td>When applying for a loan or mortgage</td>
<td>38</td>
<td>74</td>
</tr>
<tr>
<td>In stores or restaurants</td>
<td>37</td>
<td>70</td>
</tr>
<tr>
<td>When voting in elections</td>
<td>30</td>
<td>58</td>
</tr>
<tr>
<td>When seeking medical treatment</td>
<td>26</td>
<td>59</td>
</tr>
</tbody>
</table>

Note: Whites and blacks include those who report being only one race and are non-Hispanic. “In dealing with the police” and “By the criminal justice system” were asked of separate random subsamples of respondents.
“Race in America 2019”

PEW RESEARCH CENTER

Today’s Agenda

1. Navigating trade-offs
2. Mapping policy and legal approaches
3. Making them work: technical considerations
4. Making them work: social scientific considerations
5. Should we be satisfied with tweaking the system?
Technology to the Rescue?

Benjamin warns about the dangers of discriminatory designs that:

“explicitly work to amplify hierarches...”

“ignore and thus replicate social divisions”

“aim to fix racial bias but end up doing the opposite”

She calls this: the New Jim Code.

Source: Anoushnajarian, CC-BY-4.0
What Really Matters

Should we be satisfied with tweaking an algorithm to make it more fair or taking steps to ensure transparency? Why not tackle the rigged system instead?

Where People Think the Economy is Rigged
Citizens of selected countries that think the economy is rigged in favor of the rich & powerful

- Mexico: most, 94%
- South Korea: 83%
- Russia: 80%
- United States: 78%
- Germany: 77%
- Great Britain: 76%
- Australia: 75%
- Canada: 71%
- Japan: 71%
- Sweden: least, 56%

Survey of 17,180 adults in 22 countries in September & October 2016
Source: Ipsos

Source (Top to Bottom, Left to Right): Mike Fleshman, Wikimedia Commons (CC-BY 2.0); Kelly (Pexel, Free to Use); Statista