# Big Data and Security

**Jeffrey Borowitz, PhD**

*Lecturer*

Sam Nunn School of International Affairs

Implications of AI Decision-Making

# There are Always Errors

- Think about the wage model:
  - Some people earn more than you would expect, given their education, experience, IQ, and knowledge of the world of work
  - Others earn less
- What does it mean when someone makes more than we think?
  - This depends on exactly how you think of the model
  - It might just be pure good luck
  - It might also be because there are aspects of wage determination that we can't measure: perseverance, interpersonal skills, intelligence not measured by IQ, etc.
- If our goal is to predict wages of an individual, we have two types of errors:
  - Under predicting wage
  - Over predicting wage

# Implications of Model Errors: Commercial Targeting

- Macy's offers discounts to some people and not others
  - Think about a situation where there are "high" and "low" demand customers, who would pay different amounts for a good
  - With no targeting, Macy's can either use a high price and sell only to high demand customers, or use a low price and sell to both kinds.
  - With targeting, (of e.g. a coupon for some people) Macy's can set a high price to high demand customers and a low price for low demand customers
  - This creates some inequality between customers - some pay more and some pay less
- But what about errors here?
  - Low types with no coupon: these people lose out on getting the goods at an affordable price. They look to Macy's like they have high demand, but will end up not getting an attainable offer for the good
  - High types with a coupon: these people are big winners, since they would have purchased at a high price, and thus get a better deal.
- Realistically, Macy's might target based on social media profiles (the drunk looking under the street lamp)
  - So benefits will come to customers who use social media, which is not everyone

Georgia Tech

# Implications of Model Errors: College Admissions

- Imagine a college admission committee looks at outcomes of their students, and links them to their initial applications
  - They try to decide what characteristics predict “good” alumni
- Some students will have better outcomes than predicted, while others will have worse
- But now admissions decisions are made based on predicted outcomes
- Who wins and who loses?
  - We can’t know without knowing what characteristics are the most important for “good” alumni status, compared to what is measured
  - But it’s likely the fact that students with easily measurable qualities associated with good outcomes will do better (e.g. SAT scores?)
  - Or perhaps those who are “late bloomers” and can’t tell a coherent life story when they are 17?
- Another big problem: you’ve defined “good” alumni in some way

Georgia Tech

# Implications of Model Errors: Border Screening

- Imagine looking at some sort of dossier for each individual crossing a border into the US
  - Each crosser could be looked up in a range of databases (commercial purchases, social media, terrorist watch lists, etc.) can be scored according to likely risks:
    - Chances of being a terrorist
    - Chances of being involved in smuggling
    - Chances of committing a crime in the US
- Individuals can be selected for additional screening
  - Some terrorists will be missed: those who look less typical of the people who are normally threats of interest, along observable characteristics
  - Other innocent individuals will be detained or subjected to screening when they have observable characteristics like people of interest
- Here, a “data driven approach” could easily be used as a guise for an ethically undesirable profiling strategy

Georgia Tech

# Implications of Modeling: Other Concepts of Fairness

- Health Insurance:
  - Women (during childbearing age) have higher average health care costs than men, and older people have higher average costs than younger people
  - But we have regulations which force insurance premia for men and women to be the same
  - Sick people mostly pay the same premia as healthy people (especially without exclusions due to “pre-existing conditions”)
- This is certainly an old problem, and not limited to “big data”
- It’s instructive that in an old but important area where data has been available for a long time, we have some some controls on how models can be used to make decisions.

# Implications of Model Errors: Loans

- Imagine banks using “big data” to develop models to predict who will repay loans, and hence use a model to decide who should receive loans and how much they should pay in interest for them
  - This could have a huge impact
    - You won’t be able to start a business without getting a loan
    - Or buy a house or car
- This is so important that there are very strict regulations on how information related to credit decisions can be transmitted, used, and kept.
  - The Fair Credit Reporting Act provides a variety of restrictions on how banks can use various information to make loan-related decisions, what controls individuals have over the veracity of the information, etc.

# More About Loans

- Loans are so important
- FCRA says that people have a right to know:
  - Their credit score
  - The pieces of information which go into the score: credit accounts of various types outstanding and repayment history
- But let's imagine a new big data financial technique which looks at your public twitter posting history, and who you follow
  - These factors might have no ability to predict your credit score, but then again they might
- Currently your Twitter isn't regulated under FCRA, and wouldn't be.
  - While there's some modest guidance provided by credit bureaus on how credit scores are formed from credit events, this might be more complicated with Twitter
  - Clearly the fact that your tweets and who you follow could affect your credit could have a chilling effect on your use of Twitter

Georgia Tech

# Lesson Summary

- Implications of AI and Big Data are not new - when you select any decision criteria, you end up creating cutoffs and making errors
- Any time there is a change in how decisions are made, there will be different “winners” and “losers”.
- When organizations make decisions which affect people’s lives, we as a society want to ensure concepts around “fairness”. This is already codified in many related laws and processes.

Georgia Tech