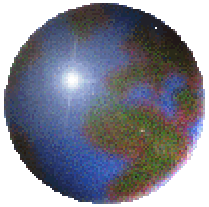

# *Machine Learning in Business*
# *John C. Hull*

## Chapter 11
## Issues for Society

# *Issues with Machine Learning*

- Data privacy
- Biases
- Ethics
- Transparency
- Adversarial machine learning
- Legal issues
- Man vs. machine

# *Data Privacy (EU), page 218*

- The Cambridge Analytica story has raised concerns about data privacy
- General Data Protection Regulation:
  - Recognizes that data is valuable
  - Companies need consent for using data for other than the purpose it was collected
  - Must provide data breach notifications
  - Citizen have a “right to explanation”
  - Safe handling across borders
  - Must appoint data protection officer

# Biases in Data

- Literary Digest predicted Landon (Republican) would beat Roosevelt (Democrat) by 57.1% to 42.9% in 1936 for U.S. president. This was based on polling 10 million people (2.4 million responding) consisting of its readers, telephone users, and those with car registrations
- Some facial recognition software was trained largely on images of white people which led to problems
- Data used to make loan decisions likely to reflect existing criteria
- Analysts may consciously or unconsciously incorporate their biases in the selection of features, the choice of models, the way data is cleaned, etc

# *Ethics (pages 220-221)*

- It is clearly unacceptable to base decisions on race, gender, or other sensitive inputs
- Including features that are highly correlated with the sensitive inputs should be avoided
- China’s social credit system which provides credit scores for citizens or businesses is controversial
- Other ethics considerations:
  - Use of ML in warfare
  - The trolley problem
  - Can machines be trained to be ethical in the data used

# *Transparency*

- Consumers have a right to know why a certain decision (e.g, a loan being refused)  was made.
- Predictions need to be explained. “Black box” algorithms are not likely to be acceptable.
- This means that in addition to making a prediction the algorithm must output the relative importance of different features in reaching conclusions
- It can do this by investigating the importance of a feature by changing its value or removing it from the analysis altogether
- The Hans story

# *Adversarial Machine Learning (page 221-222)*

- Machines are easier to fool than human beings
- Examples:
  - Avoiding spam filters
  - Spoofing financial markets
  - Confusing driverless cars

# *Legal issues*

- If a driverless car hits a pedestrian, who is liable:
  - The person who programmed the car?
  - The manufacturer of the car?
  - The owner of the car?

# *Technology interacting with humans*

- This can be dangerous
- An extreme example is Microsoft’s Tay chatbot
- This interacted with teenagers via Twitter and learned politically incorrect phrases
- It was shut down after only one day

# *Limitations of ML*

- It relies on historical data
- If there is a regime change so that historical data no longer applies then ML will not be a good guide to decision making
- How would self-driving cars perform if rules on left or right turning were change*d*?

# *Man vs. Machine*

- Human beings will need to learn how to manage large data sets and interpret the output from machine learning algorithms

# *Industrial Revolutions (page 169-170)*

- Steam engine and water power (1760-1840)
- Electricity and mass production (1840-1920)
- Computers and digital technology (1950-2000)
- AI and automation (2000 onward)