Law, Ethics, and Privacy issues in Data Science
(Talk by: Jonathan Manes)

Introduction

In an era marked by the unprecedented evolution of data science, the intertwining realms of ethics, law, and privacy have gained paramount importance, inviting profound exploration and discourse. This report ventures into these critical dimensions, meticulously examining the ethical quandaries, legal frameworks, and privacy considerations intrinsic to data science, and proposing robust safeguards and ethical practices to navigate the multifarious challenges therein.

Data science holds immense transformative potential, but its rapid integration across sectors has sparked pressing concerns regarding discrimination, fairness, transparency, and privacy. The ubiquity of algorithms has revealed their susceptibility to inherent biases and discriminatory outcomes, necessitating scrutiny and ethical reflection. This report analyzes how seemingly objective algorithms can perpetuate inequalities and explores the legal and ethical repercussions of such discriminatory practices.

Further, the report discusses the crucial role of legal norms and regulations in shaping responsible data practices and safeguarding individual rights. It investigates the requisites and implications of prominent legislations like the EU's GDPR and various U.S. privacy laws, underscoring the need for transparency, accountability, and compliance to ensure the ethical and lawful treatment of data and to foster trust and responsibility in the realm of data science.

Q1. Discuss with 2-3 examples some ethical, legal and privacy issues that you might need to consider in designing a data science application.

Example 1: Amazon's Hiring Algorithm
The Amazon hiring algorithm was biased against female applicants, underscoring the ethical concerns about fairness and equality. It is crucial that algorithms do not perpetuate or amplify existing biases and inequalities, as they can lead to unfair treatment and discrimination against certain groups.

Legal & Privacy Concerns: The biased algorithm potentially violates anti-discrimination laws, such as Title VII of the Civil Rights Act, which prohibits employment discrimination based on sex, race, color, national origin, or religion. Companies using biased algorithms could face legal sanctions, lawsuits, and reputational damage. In creating algorithms, sensitive data such as gender may be used, raising concerns over data privacy and protection. Mishandling or misuse of such sensitive data can lead to breaches of privacy laws and loss of individual privacy.

Example 2: Facebook Ad Targeting
Facebook enabling housing discrimination through its ad targeting tools raises ethical issues about enabling and perpetuating discriminatory practices. It's essential to ensure that technology is not used to harm or unfairly treat individuals or groups, especially those already marginalized or vulnerable.

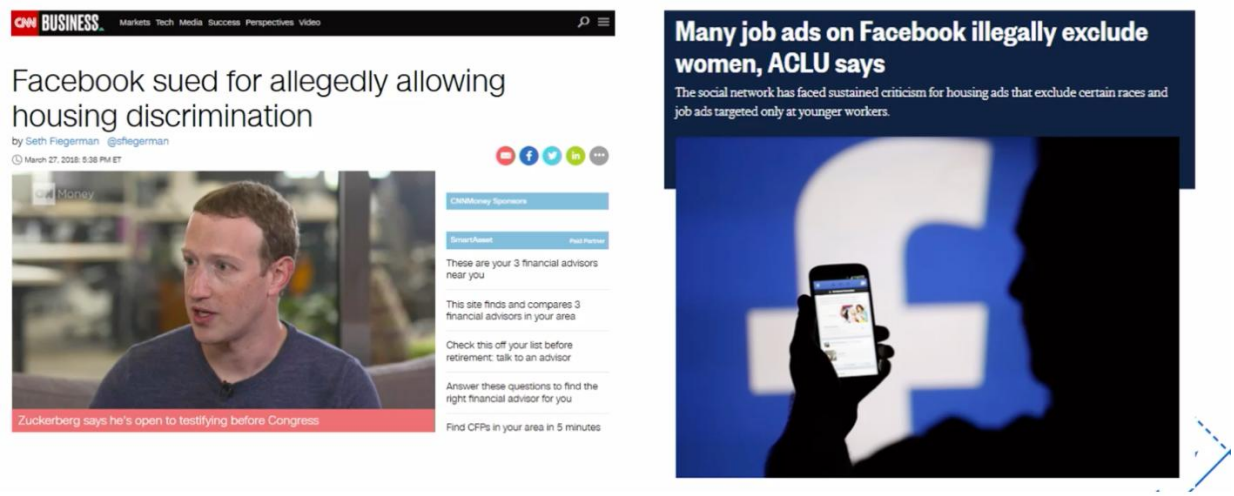

Fig.1 News Article on Facebook sued for allowing housing discrimination.

Legal & Privacy Concerns: Allowing housing discrimination through ad targeting is illegal under the Fair Housing Act, and companies enabling such discrimination can face legal action. Ensuring compliance with anti-discrimination laws is crucial to avoid legal repercussions and uphold individual rights and equal treatment. Ad targeting involves the use of user data, often without explicit consent, raising significant privacy concerns. The misuse or unauthorized access to user data can lead to violations of data protection laws and infringe on individuals' rights to control their personal information.

Example 3: COMPAS Criminal Risk Scoring Tool

The incorrect analysis of crime risk by the COMPAS tool can lead to unjust treatment and impacts on individuals' lives. Ethical principles of justice and fairness are at stake when individuals may be wrongly categorized and treated based on inaccurate or biased assessments.

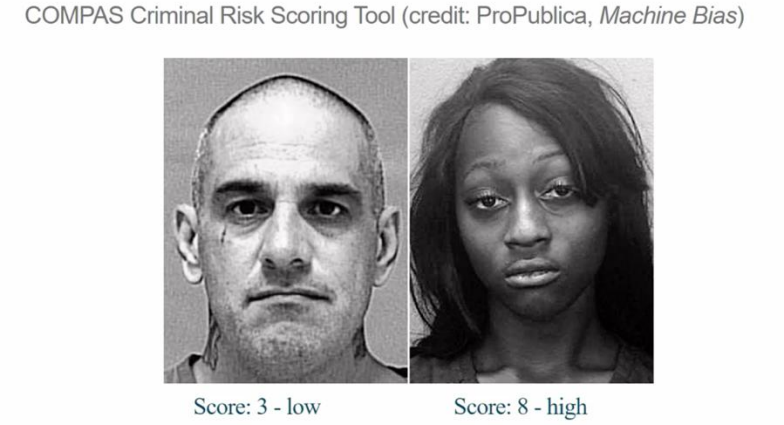

Fig.2 Incorrect analysis of crime risk by the COMPAS tool.

Legal & Privacy Concerns: Using such tools in judicial decisions can lead to violations of due process and equal protection under the law, as guaranteed by the Constitution. It's crucial to ensure transparency, accuracy, and fairness in algorithmic decision-making to uphold legal rights and avoid discriminatory outcomes. The use of sensitive personal data in risk assessment tools without proper safeguards can lead to privacy violations. Ensuring the confidentiality and security of such

data is paramount to protect individual privacy and comply with data protection laws. In designing data science applications, addressing these ethical, legal, and privacy concerns is crucial to create fair, lawful, and respectful solutions that uphold individual rights and values.

Q2. How can algorithms be potentially discriminatory - illustrate using some of the examples referenced in the talk.

Algorithms can potentially be discriminatory due to biases in training data, mislabelling, selection biases in data collection, and the use of proxies for protected characteristics. Here's a more in-depth look at how algorithms can discriminate, illustrated with examples referenced in the talk:

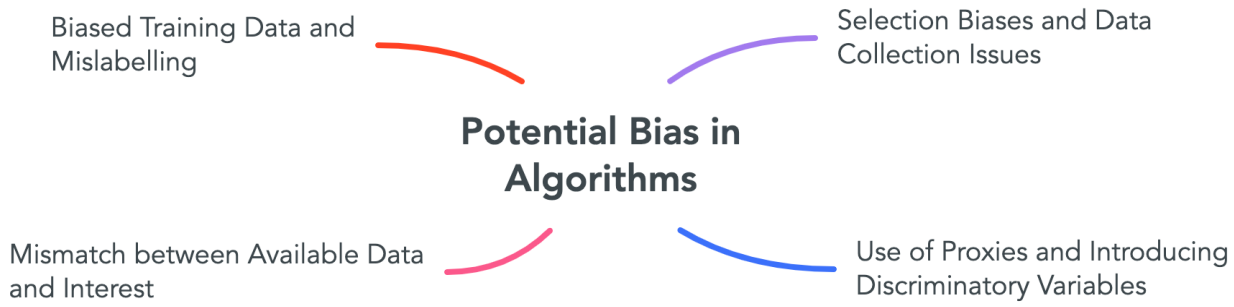

Fig.3 Potential Bias in Algorithms

1. Biased Training Data and Mislabelling
Example : Amazon's Hiring Algorithm : This algorithm was trained on ten years of the company's hiring data, which reflected a preference for male candidates, causing the algorithm to rank female applicants lower. This is a classic example of how the biases present in the training data can lead to discriminatory outcomes, creating a disparate impact on female candidates. The algorithm even penalized resumes that included the word "women's," further exemplifying how biases in the training data can lead to unfair treatment.

2. Selection Biases and Data Collection Issues
Example : Training Data Labelling Issues : The process of labeling data involves human judgment and can reflect existing biases. For instance, when labeling data to determine job performance, the algorithm erroneously concluded that having the name "Jared" and playing high school lacrosse were indicative of job performance, overlooking the real qualifications needed for the job. This reflects how biases in labeling and defining target variables can lead to unfair and discriminatory algorithmic outcomes.

3. Use of Proxies and Introducing Discriminatory Variables
Example : Proxies in Algorithms : Even when protected characteristics like race or gender are not directly included in the dataset, the algorithm may still use other features that act as proxies for these characteristics. For example, using zip codes could inadvertently introduce racial biases, as zip codes can correlate highly with race due to historical segregation. When proxies are used, machine learning models can inadvertently reintroduce the influence of discriminatory variables, leading to disparate impacts on protected groups.

4. Mismatch between Available Data and Interest

Example : Facebook Ad Targeting : Algorithms may discriminate when there is a mismatch between available data and the actual phenomenon of interest. For instance, Facebook's ad targeting tools enabled advertisers to target or exclude users based on seemingly neutral criteria that acted as proxies for race or gender, leading to discriminatory ads. This highlighted how algorithms, without proper safeguards, can facilitate discrimination even when the used criteria seem neutral.

Algorithms, while often perceived as objective, can indeed be discriminatory due to biases inherent in their development processes, including biased training data, mislabelling, use of proxies, and selection biases in data collection. The referenced examples underscore the need for careful consideration and mitigation of biases during the development and deployment of algorithms to prevent discriminatory outcomes and ensure fairness and equity.

Q3. Discuss data privacy issues in the context of the Facebook-Cambridge Analytica example.

The Facebook-Cambridge Analytica scandal is a significant illustration of data privacy issues and underscores the ethical and legal ramifications of mishandling user data. Here's an in-depth discussion on the data privacy issues that emerged from this scandal. Cambridge Analytica, a political consulting firm, acquired the data of approximately 87 million Facebook users without their knowledge or explicit consent. The data was harvested via a quiz app that not only collected data from the users who engaged with it but also from their friends, exploiting Facebook's API.

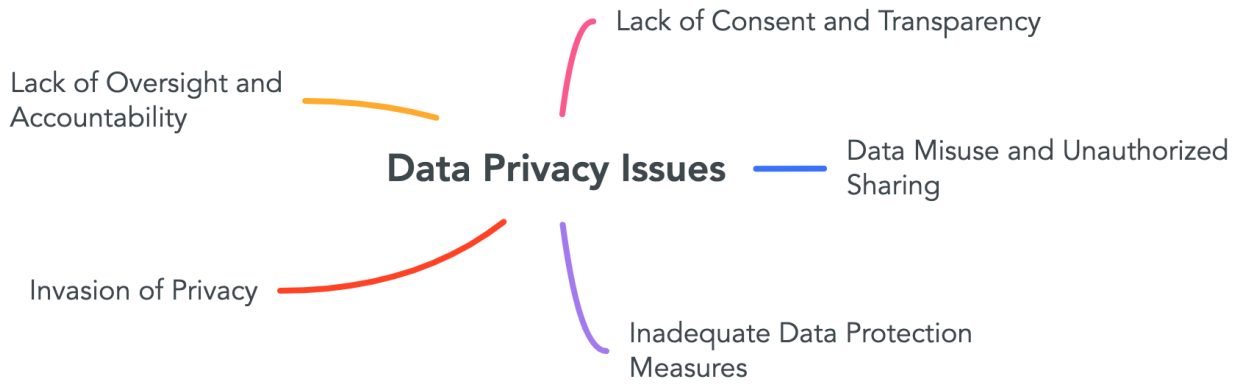

Fig.4 Data Privacy Issues in the context of Facebook-Cambridge Analytica

Data Privacy Issues:

1. Lack of Consent and Transparency: Users were not adequately informed about the extent of data collection, and consent was not explicitly obtained. The data harvested was far more extensive than users were led to believe, and the purposes for which the data was used were not transparently conveyed to the users.

2. Data Misuse and Unauthorized Sharing: The acquired data were used for unauthorized purposes, specifically for creating psychological profiles of voters to target them with personalized

political advertisements. Facebook's policies were violated when user data collected for academic purposes were sold to Cambridge Analytica for commercial and political ends.

3. Inadequate Data Protection Measures: Facebook failed to implement stringent data protection measures and did not adequately secure its API, allowing third-party apps to access vast amounts of user data without proper safeguards, leading to unauthorized data access and sharing.

4. Invasion of Privacy: The unauthorized collection and use of user data for psychological profiling and targeted advertising represent a severe invasion of privacy. Users were unknowingly subjected to manipulation and influence, infringing on their right to privacy and autonomy.

5. Lack of Oversight and Accountability: Facebook did not have adequate oversight mechanisms to monitor and control the access and use of user data by third-party apps. There was a failure to ensure accountability and compliance with data protection norms, leading to the unchecked misuse of user data.

The Facebook-Cambridge Analytica scandal highlighted the urgent need for robust data protection measures, stringent oversight, and enhanced transparency in data collection and usage practices. It emphasized the importance of obtaining informed consent and respecting user privacy and led to increased scrutiny of data practices of tech companies, ultimately contributing to the development and enforcement of stricter data protection regulations globally, such as the GDPR. The scandal underscored the profound implications of data privacy breaches and reinforced the critical importance of ethical and legal compliance in data handling and processing practices.

Q4. Describe in the context of data collection, storage and use, some safeguards that are necessary to be in compliance with US privacy laws.

To ensure compliance with U.S. privacy laws, organizations must implement several safeguards throughout the lifecycle of data – from collection to storage and use. Below is a detailed explanation of each of the mentioned safeguards.

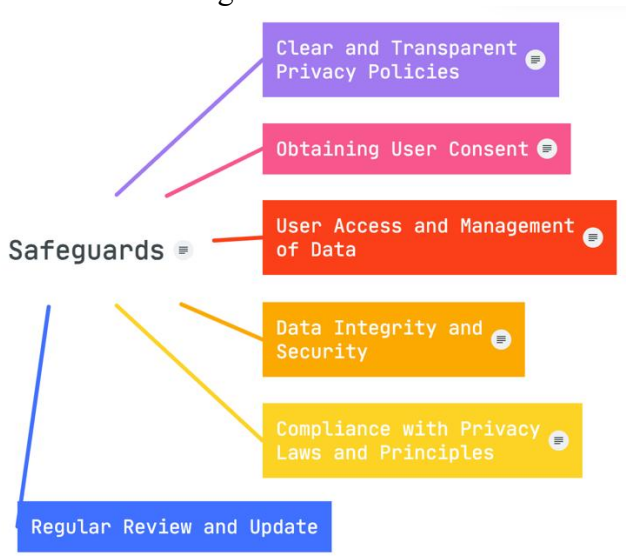

Fig.5 Safeguards necessary to be in compliance with US privacy laws.

1. Clear and Transparent Privacy Policies: Organizations must develop comprehensive privacy policies that are easily accessible and understandable to the users. These policies must clearly articulate the types of data being collected, the purposes for which the data will be used, and the entities with whom the data might be shared. Clear and transparent policies are crucial for building trust with users and ensuring informed consent.

2. Obtaining User Consent: Before collecting and processing user data, explicit and informed consent must be obtained from the users. Organizations should provide users with clear options to grant or withhold consent and must respect the users' choices. The process should be user-friendly, and any changes to data practices should be communicated promptly, with renewed consent sought as necessary.

3. User Access and Management of Data: Organizations must empower users by allowing them to access their own data. Users should be able to review, correct inaccuracies, and manage their data preferences. They should also have the option to delete their data, ensuring user control over personal information. Providing such access and management options is vital for maintaining data accuracy and respecting user autonomy.

4. Data Integrity and Security: Organizations are responsible for maintaining the integrity and security of the collected data. Implementing robust security measures such as encryption is crucial for protecting data during storage and transmission. Secure data handling practices, including regular security audits, vulnerability assessments, and timely patching of security flaws, are essential to safeguard data against unauthorized access, breaches, and leaks.

5. Compliance with Specific Privacy Laws and Principles: Depending on the sector and the type of data handled, organizations must comply with applicable sector-specific privacy laws, such as HIPAA for healthcare data and COPPA for children's data. Adherence to the Fair Information Practice Principles, which emphasize notice, choice, access, and security, is also crucial to ensure fair and lawful data practices.

6. Regular Review and Update of Data Protection Measures: The dynamic nature of the digital landscape necessitates regular reviews and updates of data protection measures. Organizations should stay abreast of emerging threats and vulnerabilities and update their security protocols, data handling practices, and privacy policies accordingly. Continuous improvement and adaptation of data protection measures are critical for mitigating new risks and ensuring ongoing compliance with evolving legal requirements.

Implementing these detailed safeguards is not just a legal necessity but also an ethical obligation for organizations. By adhering to these practices, organizations can ensure the respectful and lawful treatment of user data, build and maintain trust with users, and mitigate the risks of legal sanctions and reputational damage.

Q5. Discuss what additional safeguards might be necessary to be in compliance with the EU GDPR requirements.

The General Data Protection Regulation (GDPR) in the European Union uses the following additional measures so that organizations can ensure compliance, particularly focusing on algorithmic processing and decision-making:

Fig.6 Personal Privacy / Data Protection for GDPR

1. **Transparency**: Organizations are required to be transparent about the use of algorithms in decision-making processes. Users must be informed that an algorithm is being used and provided with meaningful information about the logic involved, helping them understand how their data is being processed and how decisions that affect them are being made.

2. **Human in the Loop**: GDPR mandates the inclusion of a "human in the loop" for decisions with serious effects on individuals. This means that there should be human oversight to review and intervene in decisions made by algorithms, ensuring that outcomes are fair, accurate, and justifiable. This provision helps in mitigating the risks of erroneous or biased algorithmic decisions.

3. **Restrictions on Purely Algorithmic Decision-Making**: Organizations cannot rely solely on algorithms for making decisions unless the individual has explicitly consented, it is necessary to implement a contract, or it is permitted by law. This safeguard ensures that individuals are not subjected to unfair or discriminatory decisions made without human judgment and scrutiny.

4. **Right to Challenge and Obtain Explanations**: Individuals have the right to challenge algorithmic decisions and seek explanations for the decisions made. They must be provided with clear and understandable reasons for the decision, allowing them to contest and seek redress for potentially unfair or harmful outcomes. This right reinforces individual autonomy and empowerment in algorithmic decision-making.

5. **Auditing the Algorithm**: Both internal and external audits of algorithms are required to ensure that data processing is accurate, fair, and non-discriminatory. Regular algorithmic auditing helps

in identifying and addressing biases, errors, and discrepancies in algorithmic models and promotes accountability and compliance with data protection principles.

By adhering to these GDPR requirements, organizations can ensure ethical and lawful use of algorithms, protect individual rights, and foster trust and transparency in algorithmic decision-making processes. These provisions are crucial for mitigating the risks of algorithmic bias, discrimination, and error, and for upholding the principles of fairness, accountability, and respect for individual autonomy in the age of AI and advanced data analytics.

Answer the following multiple-choice questions: You can list the question number and the letter corresponding to the correct choice as Answer in your report, (2x5 = 10 pts of the 80 C+R points in the rubric)

Q1. A
Q2. D
Q3. C
Q4. B
Q5. A

Reference :
[1] Lecture video Lecture 4: Jonathan Manes.
[2] Figure 1,2 and 6 from Lecture slide (Lecture 4: Jonathan Manes).
[3] Figure 3,4 and 5 Edited in the mindmeister.
[4] Facebook housing discrimination https://www.youtube.com/watch?v=JwGGHtNpB0Q&t=8s
[5] How Cambridge Analytica Exploited the Facebook Data of Millions
https://www.youtube.com/watch?v=mrnXv-g4yKU&t=1s