Name: Sahithi Dodda
Person Number: 50441731
UB Email: sahithid@buffalo.edu

Assignment 4

EAS 504: Applications of Data Science - Industrial Overview - Spring 2023

Lecture by Jonathan Manes - Law, Ethics and Privacy issues in 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.

Ans: When working with large quantities of data and analyzing it to extract valuable insights, it is crucial to design and implement data science applications while considering ethical, legal, and privacy issues. To ensure that the application is responsible and ethical, applications need to consider various issues related to privacy, legality, and transparency. Here are a few examples of where ethical, legal and privacy issues need to be addressed while designing a data science application.

Public Discourse and Social Life: When designing a data science application, the designer must consider several ethical, legal, and privacy issues. These include protecting users' right to free speech, preventing the spread of biased and false content, safeguarding personal data from misuse and abuse, ensuring fair and unbiased algorithms, and complying with legal regulations. For instance, let's consider Facebook, Instagram, or twitter, the content we see on our news feed is not what someone has recently posted, an algorithm designed by these companies decides what we see, how long we see based on our browsing patterns and interests. It is crucial to ensure that the application does not infringe upon users' rights and that their data is collected and used only for its intended purpose, with full transparency and compliance with the relevant regulations.

Medical & Health Care: The protection of medical and healthcare data is crucial, and strong security measures must be in place to prevent unauthorized access, hacking, or theft. Patients' privacy must be respected, and their personal and health information should not be shared without their consent. Obtaining informed consent from patients before collecting, analyzing, or sharing their data is a critical ethical consideration. The application's algorithms must be fair and unbiased to ensure equitable outcomes for all patients. There have been cases where data issues have occurred in healthcare, such as when IBM Watson recommended a fatal cancer treatment to a patient or when a computer program predicted recidivism with a bias against African Americans. These examples highlight the potential errors that can arise with machine learning algorithms and the importance of fairness and non-discrimination in algorithmic decision-making.

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

Ans: Algorithms can be discriminatory if they are trained on biased data or are designed with biased criteria. If the criteria used to design the algorithm are themselves biased, the algorithm will be biased as well. Discrimination can be in many ways based on Race, Gender, Marital status, Pregnancy, Age, Religion, Disability status, National Origin, Citizenship, Veteran status etc. Charging more for males than females by insurance companies is an example of algorithmic discrimination. Federal Laws as well as state laws prohibit discrimination that sometimes vary in coverage. Lots of domains like Employment, Housing, Public Accommodation, Banking, Education, Government Contractors, Government Entitles etc., in which data science is predominant is covered by anti - discriminatory laws. As an example, we can look at Facebook's housing advertisements, which have been the subject of a lawsuit under the Fair Housing Act. An example of algorithmic discrimination can be seen in the case of job resume screening tools, such as the promotion test designed for firefighters in New Haven, Connecticut. The test was designed to be fair to all candidates, without any advantage to white or black individuals, due to a history of black people being excluded from the fire department. However, the test results showed that only two black people passed, while all the other successful candidates were white. This was not the expected outcome and was considered discriminatory. As a result, the city planned to discard the test and conduct a new one. However, white firefighters who had passed the test sued the city, alleging that the test was not flawed, and that they could not be deprived of their promotions on the basis of race. The case reached the Supreme Court, which ruled that even if a test has a clear disparate impact, it cannot be thrown out unless there is strong evidence that something about the test was leading to that problem. In this case, the court did not allow the test to be discarded, despite its clear discriminatory impact on black firefighters, as there was no strong evidence that the test was flawed. This case shows how algorithmic discrimination can occur even when a test is designed to be fair to all candidates.

In the data science process, human decision-making plays a crucial role, but it can also result in unconscious biases. It is important to design target variables that are necessary for the business and closely related to it. However, the definition of target variables should be carefully constructed, as loose definitions may intentionally or unintentionally result in discriminatory outcomes. The selection of target variables and class labels, data collection, sampling bias, labeling data, and the use of proxy features or masking discrimination are stages in the data science project lifecycle where human biases can be encoded. Organizations must be cautious during this stage to avoid encoding any bias, as different types of target variables can have varying effects on protected groups. Another instance is the Enron Mail dataset is not appropriate for building machine learning algorithms aimed at interpreting natural language as it can be biased, deceptive, and unreliable. After an examination of an algorithm built with this data, it was found that two factors, Jared's name and playing high school lacrosse, were the most significant indicators of job performance, demonstrating that the algorithm was biased. So as discussed above, algorithms can be potentially discriminatory, and all the factors must be considered carefully.

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

Ans: In 2016, Cambridge Analytica, a UK-based company, utilized data from millions of Facebook users to create psychographic profiles that were used for targeted political advertising during the

U.S. presidential election campaign. The data was obtained through a personality quiz app developed by Aleksandr Kogan, which required users to log in to their Facebook profiles, giving Kogan access to their personal information. Kogan combined the quiz results with Facebook data to develop psychometric models, which were then sent to Cambridge Analytica. In addition, Kogan's app collected the personal data of users' Facebook friends, allowing for the compilation of similar profiles within a few months. Approximately 270,000 people took the survey, and the data of up to 87 million friends was also harvested, a significant portion of all U.S. Facebook users. Cambridge Analytica used this data to target people with political messaging promoting Trump, which they claimed helped the campaign's strategy, although the campaign disputes this. Kogan claimed that his work was for academic research, but he also shared the information with Cambridge Analytica, which violated Facebook's policies. Facebook was fined $5 billion by the US Federal Trade Commission for violating data privacy policies, as the settlement with the FTC in 2011 stipulated that information would not be shared with third parties without user consent.

This incident raised several data privacy issues. First, Facebook's policies at the time allowed third-party apps to collect data not only from users who installed the app but also from their friends, without explicit consent. This allowed for a vast amount of data to be collected without users' knowledge or consent. Second, the incident revealed that Facebook did not adequately monitor or enforce its policies on data sharing, which allowed Cambridge Analytica to obtain and use the data without Facebook's knowledge or consent. Third, the incident highlighted the potential misuse of personal data for political purposes, which raised concerns about the impact of targeted advertising and manipulation on democratic processes. Following the scandal, Facebook faced widespread criticism and regulatory investigations, which resulted in changes to its data handling practices. Facebook restricted third-party access to user data and implemented additional measures to monitor and enforce its policies. However, the incident demonstrated the need for greater transparency and accountability in the collection, use, and sharing of personal data, particularly by large tech companies that hold vast amounts of user data.

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

Ans: US privacy laws require organizations to establish safeguards for proper data collection, storage, and usage. This includes compliance with industry-specific regulations such as FERPA, HIPAA, FCRA, and RFPA. These measures include transparency, where organizations must openly and clearly state the types of data collected, how it is used, and who it is shared with. Consent is also essential, requiring explicit and informed agreement from individuals before collecting and using their data. Additionally, organizations must limit data collection to specific purposes and minimize the amount of data collected and stored to only what is necessary. Security measures, such as encryption and access controls, must be in place to protect against unauthorized access, use, disclosure, or destruction of data. Data retention policies should be implemented to destroy unnecessary data and individuals have the right to access, correct, and delete their personal data. Organizations must report any data breaches that could result in harm to individuals to both authorities and affected individuals. In the event of a data breach, organizations should have a plan in place to promptly investigate and contain the breach, notify affected individuals and

authorities, and take appropriate measures to prevent similar incidents in the future. Another important safeguard is the requirement for organizations to conduct regular risk assessments to identify and mitigate potential privacy risks associated with data collection, storage, and use. This can include conducting privacy impact assessments, vulnerability scans, and penetration testing to identify potential security weaknesses. Organizations must also ensure that their third-party service providers and vendors comply with the same privacy and security standards as the organization itself. This can be achieved through contractual provisions that require third-party providers to adhere to specific privacy and security protocols.

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

Ans: The GDPR is a privacy protection regulation established by the European Union, which differs from the US approach in that it adopts a uniform approach. The regulation covers both data processors and data controllers, where data processors are entities holding and using the data, and data controllers are companies directing how the data is used. For instance, if Amazon Web Services is used to run a system, it is the data processor, and the company utilizing the services is the data controller. The GDPR requires that personal data can only be used when explicitly permitted, and general consent is not enough; users must provide affirmative opt-in. Organizations cannot bundle broad consent as a condition of access. Data subjects have the right to access their information and correct it, as well as the right to know who their data was shared with. The GDPR also mandates that withdrawing consent must be as easy as giving it. Additionally, data subjects have the right to data portability and data erasure. Any processing information involving a person irrespective of which domain, are governed by GDPR. The EU sees data privacy regulations as human rights, giving users control over their data. As a result, consent is not automatically provided; rather, it must be given by the user. Under GDPR, users are granted several rights, including the right to access and control their data, know who it is shared with, revoke permission for its usage, request its deletion, and control every use of their data.

Also, 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)

Ans:

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