ETHICS OF DATA SCIENCE

By Shesh Murali

INTRODUCTION

Data science is a field of science created in the 1960's that is under the umbrella fields of information technology and science. The study follows the branches of programming, machine learning and programming. By combining these realms of research and techniques, it uncovers relationships and patterns within the data to help inform decision making (Igual & Seguí, n.d.), build evidence-based decisions and solve real world problems. This essay will explore the ethics of data science and how this discipline concerned with what's right or wrong applies in the study of extracting insights from data. It will act as a case-study investigating examples or instances from different areas where data science is implemented and highlight the ethical dilemmas that were faced and the possible solutions that could have been implemented. Otherwise, it severely affects the reputation of these so-called businesses and industries that use data science (Edquist et al., 2022).

PRIVACY IN HEALTHCARE

The first case study will delve into the privacy concerns within the health industry when data science is utilised. Privacy and data collection involve usage of sensitive personal information, while safeguarding individuals' confidentiality. It's considered a fundamental right of individuals to have the ability to control their own personal information and how it is utilised, shared and collected (Bhattacharyya, n.d.). In the field of data science, there is considerable tension on the concepts whether the private data obtained is under protection or transparency (Online, n.d.). While transparency can provide positive benefits like the ability to access and work with the data no matter how where they are located or what application created them (*Why Data Transparency Matters | Toric*, n.d), there must be trust between the individuals who obtained the data and the ones who gave it. Often the thin line of trust between an institution with authority and people who don't hold that power. And no institute, whether private or government, have issues regarding trust with its patrons than the health-care industry (Voils et al., 2005). The healthcare industry has had a fervent usage of data science throughout time such as electronic health sectors, personalised medicine and now Health care AI (HIMSS, 2021). Yet, data science applications within this sector can breach privacy by mishandling data. The access to private data through transparency within the program, can allow cybersecurity breaches to steal health care data, which can lead to long-term identity theft and be utilised to give sensitive information to others for payments. Moreover, it allows the health care institutions to have control and manipulate the data. For instance, improper sharing of

medical records or unauthorised access can happen, violating individuals' rights to privacy. An example that occurred was the UCLA Health system data breach in 2015 where hackers gained access to patient information, like names, social security number, medical diagnoses and treatment information (*UCLA Health Victim of a Criminal Cyberattack*, n.d.). It resulted in millions of sensitive information being stolen leading to identity theft, the reputation of UCLA health care and the need to financially reprimand the health care sector as well. Therefore, this underscores the importance of cybersecurity measures and the need to establish ethical protocols when obtaining patient information (Lord, 2020). To resolve this, strict data anonymisation protocols, obtaining informed patient consent, and establishing robust data-sharing agreements can ensure privacy is maintained while allowing data-driven advancements in healthcare. Data science is a vital aspect in the healthcare system, without it, there would be a reduced efficiency on how data is obtained and utilised to benefit both the patient and health care institution, therefore preserving patient privacy is of the utmost importance to make advancements for all parties involved.

TARGETED ADVERTISING AND CONSUMER SERVEILLANCE

The second case study will follow the target advertising when brands implement data science techniques to further their product and to strengthen society surveillance and implement capitalist ideologies for continuous consumption over the public. Targeted advertising is a form of online advertising based on the interest, traits and especially data of the consumer in the online world where then the Algorithm pushes a product on them. From the insights of data science's scientific approach, targeted advertising leverages these insights to provide the correct advertisement to the correct individual and the correct time through the algorithm (Combining *Data Science and Targeted Advertising for Better Results*, n.d.). Consumers have become easier to analyse as life has become digitised, for instance people's entertainment and shopping are done online, thus what was once private data has become public (GCF Global, 2019). While these practices don't automatically persuade consumers for overconsumption, it raises the ethical dilemma of surveillance, data privacy and manipulation that perpetuates consumerism and capitalism when the gap between the one-percenters and common people grow further (*Targeted Online Ads Are the Success of "Surveillance Capitalism,"* n.d.). An example of this is when companies analyse browsing habits to create personalised ads. This is evident in the case of a political consulting firm, Cambridge Analytica, that used data from Facebook and other online forums to create targeted political advertising campaigns and advertisements in 2018 (Confessore, 2018). The company gained access to millions of personal data on Facebook without consent which breached their privacy, where they then pushed a political agenda and called vast amounts of user information. Facebook have often found themselves in Ad targeting controversies as due to their possession of sensitive information and to benefit from obtaining this information they promote advertisers who target consumers based on their interests, demographic can behaviour (Arwa Mahdawi, 2019). Therefore, to uphold the practice of ethical data science, solutions like user control, stricter regulations and algorithm transparency must be implemented to provide users a level of personalisation they are comfortable with, consent and ensure fairness and compliance from the companies to increase

accountability (Mühlhoff & Willem, 2023). Data science has now become intertwined with the capitalist economic system where companies benefit from data extraction and thus to tailor to the needs of the public these ethics need to be preserved to balance the economic interests of businesses and individual's rights of consumers in a digital age.

ALGORITHMIC BIASES IN DECISION-MAKING

Finally, the last case study will explore algorithm biases regarding gender, education, socioeconomic and racial involved in different aspects of society like employment and criminal justice. Machine learning models are the procedures that are run on the datasets to recognise and highlight patterns, to then create an algorithm that acts on the patterns of the model through a program (El Naqa & Murphy, 2015). However, algorithm biases are the human prejudices that are reflected when machine learning models make decisions based on training data (Larkin, 2022). Biases can enter the algorithm due to the result of pre-existing cultural or institutional expectation that then does not consider the effect of these biases to the audience. This is deeply represented in the realm of the judicial system, employment, and banking. Hence, raising the ethical dilemma on how these industries perpetuate biases through algorithmic decision-making. For example, with data science the judicial system can make predictive policies through collecting racially biased training data and using machine learning algorithms to predict where crimes can occur where the majority are in low-income multicultural communities. This case occurred during the Chicago PD use of an algorithm Strategic Subject List (SSL) where on historical criminal data marginalised communities and promoted racial biases (Asher & Arthur, 2017). Moreover, in the regards of employment resume screening using machine learning algorithms are said to make the process more efficient but can inadvertently favour possible employees in certain demographics and education based on previous employees. For example, Amazon utilised a screening algorithm toll where there was a bias against women due to factors like biased training data, hence reinforcing negative gender biases (Sun et al., 2020). The risks of not following the ethical disciplines have a large negative effect, as it could warp their perception of groups. To address these issues, industries must establish unbiased data collection, different trained datasets, and transparency. Furthermore, monitoring is crucial for preventing perpetual algorithm biases (Rizinski et al., 2022). By doing so, allows for more diversity and reduces the negative stereotypes on marginalised demographics. These ethical dilemmas regarding algorithm biases only blunders society's advancements into becoming a more socially accepting society.

CONCLUSION

In conclusion, the ethics of data science are at the forefront of our rapidly evolving digital world. This essay acted as a case study, exploring cases underlining the ethical dilemmas in the applications of data science. Within the healthcare industry, there is tension between patient privacy and data transparency where private data is at risk, thus robust protocols and informed consent are needed to preserve confidentiality. Moreover, targeted advertising highlights the potentials of data science when surveillance and data manipulation are used in the pursuit of capitalist goals and overconsumption. Therefore, user control and regulation are needed to balance between business interest and consumer rights. Finally, algorithmic biases due to machine learning models in the realm of judicial system and employment, perpetuate discrimination. By addressing these issues requires unbiased trained datasets to reduce harmful stereotypes and increase fairness. The future of data science is dependent on vigilance and adaption, hence by striking a balance between innovation and ethical responsibility is needed. The lessons learned can shape the ethical landscape of data science and promote its usage in alternate fields.

BIBLIOGRAPHY

Arwa Mahdawi. (2019, November 5). *Targeted ads are one of the world's most destructive trends. Here's why | Arwa Mahdawi*. The Guardian; The Guardian. https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-news-clickbait-surveillance-capitalism-data-mining-democracy

Asher, J., & Arthur, R. (2017, June 13). Inside the Algorithm That Tries to Predict Gun Violence in Chicago. *The New York Times*. https://www.nytimes.com/2017/06/13/upshot/what-an-algorithm-reveals-about-life-on-chicagos-high-risk-list.html

Bhattacharyya, S. (n.d.). *What is Data Privacy in Data Science? | Analytics Steps*. Www.analyticssteps.com. https://analyticssteps.com/blogs/what-data-privacy-data-science#:~:text=Data%20privacy%20is%20a%20fundamental

Combining data science and targeted advertising for better results. (n.d.). Www.ibm.com. https://www.ibm.com/watson-advertising/thought-leadership/combining-data-science-and-targeted-advertising

Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Edquist, A., Grennan, L., Griffiths, S., & Rowshankish, K. (2022, September 23). *Data ethics: What it means and what it takes | McKinsey*. Www.mckinsey.com. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes

El Naqa, I., & Murphy, M. J. (2015). What Is Machine Learning? *Machine Learning in Radiation Oncology*, 3–11. https://doi.org/10.1007/978-3-319-18305-3_1

GCF Global. (2019). *The Now: What is Targeted Advertising?* GCFGlobal.org. https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/

HIMSS. (2021, July 13). *Top Trends for Big Data in Healthcare | HIMSS*. Www.himss.org. https://www.himss.org/resources/top-trends-big-data-healthcare

Igual, L., & Seguí, S. (2017). Introduction to Data Science. *Undergraduate Topics in Computer Science*, 1–4. https://doi.org/10.1007/978-3-319-50017-1_1

Larkin, Z. (2022, November 16). *AI Bias - What Is It and How to Avoid It?* Levity.ai. https://levity.ai/blog/ai-bias-how-to-avoid#:~:text=Machine%20Learning%20bias%2C%20also%20known

Lord, N. (2020). *Healthcare Cybersecurity: Tips for Securing Private Health Data*. Digital Guardian. https://www.digitalguardian.com/blog/healthcare-cybersecurity-tips-securing-private-health-data

Mühlhoff, R., & Willem, T. (2023). Social Media Advertising for Clinical studies: Ethical and Data Protection Implications of Online Targeting. *Big Data & Society*, *10*(1), 205395172311561. https://doi.org/10.1177/20539517231156127

Online, R. (n.d.). *Data Science and Privacy. How much is it okay to know?* RMIT Online. https://online.rmit.edu.au/blog/data-science-and-privacy-how-much-it-okay-know

Sun, W., Nasraoui, O., & Shafto, P. (2020). Evolution and impact of bias in human and machine learning algorithm interaction. *PLOS ONE*, *15*(8), e0235502. https://doi.org/10.1371/journal.pone.0235502

Rizinski, M., Peshov, H., Mishev, K., Chitkushev, L. T., Vodenska, I., & Trajanov, D. (2022). Ethically Responsible Machine Learning in Fintech. *IEEE Access*, *10*, 97531–97554. https://doi.org/10.1109/access.2022.3202889

Targeted online ads are the success of "surveillance capitalism." (n.d.). Magellan Financial Group. https://www.magellangroup.com.au/insights/targeted-online-ads-are-the-success-of-surveillance-capitalism/

UCLA Health Victim of a Criminal Cyber Attack. (n.d.). Www.uclahealth.org. Retrieved September 16, 2023, from https://www.uclahealth.org/news/ucla-health-victim-of-a-criminal-cyber-attack-2472#:~:text=As%20part%20of%20that%20ongoing

Voils, C. I., Oddone, E. Z., Weinfurt, K. P., Friedman, J. Y., Schulman, K. A., & Bosworth, H. B. (2005). Who Trusts Healthcare Institutions? Results from a Community-Based Sample. *Ethnicity & Disease*, *15*(1), 97–103. https://www.jstor.org/stable/48666528

Why Data Transparency Matters | Toric. (n.d.). Www.toric.com. https://www.toric.com/blog/data-transparency