Project One

Jeremia Faust

Doctor Obafemi Balogun

July 24, 2022

**Introduction**

As the lead engineer of a major social networking company that uses personal

algorithms to provide a personalized experience for our customers, I have been tasked to make sure that we are meeting the requirements of the pricy laws or GDPR law. This is due to the company being approached by regulators that claim that the company is not following the guidelines. The company has been collecting user date that is feed into multiple neural networks to create models that the company use to improve the customer experience on our site.

**Neural Networks**

A neural network for AI also known as machine learning is a bunch of algorithms that are designed to see patterns in the data that is fed into it. The idea of a neural network is loosely based on the human brain. It consists of neurons or nodes that is stacked in layers. These layers consist of an input layer, the hidden layer, and the output layer. The input layer is the layer that accepts that data and splits it apart, add weights and is sent to the hidden layer. The purpose of the hidden layer is to preform all the computations and sends it to the output layer. The output layers predict the output of the data. Neural networks take raw data and groups unlabeled data based on similarities then it classifies the data. The Classifications are based on how the data is labeled. A good example of machine learning at work is in your email. It takes all the incoming email and classifies it as junk mail or regular mail.

**Neural Net Applications to Personalization**

“Personalization is the process of delivering a customer experience that fits unique individual preferences.”(Marsh,2022) This is done by algorithms using neural networks and AI. They collect data in real time, the data is run through a neural network, then the AI will personalize the website or application for the user. This can be seen on sites such as Facebook, as the user navigates and clicks links, that data is used to offer suggestions. Personally, in my experience of Facebook’s personalization has extremely become forefront in the application. A good example of this is a couple of weeks ago I clicked on an advertisement for a cruise. If I were to open Facebook up, I will now see multiple advertisement for cruises and other vacation spots.

Personalization is a great tool for companies to use due to its ability to increase sales but there are some ethical concerns that need to be addressed. For personalization to properly work it requires a lot of user data to work properly. “When you collect and store personal information about customers it is your responsibility to ensure that this information remains private and is only used with customer permission.”(Bavati,2022)  If the data is gathered without the permission of the user or is sold to others, it leaves the company open to lawsuits.

When creating anything with machine learning it will learn whatever it is given. This leads to unintended consequences. Back in 2015 A

mazon realized that the algorithm that they used for hiring new employees was bias towards women. This was because the data that was fed to the program was using data that from resumes from the last ten years was from mostly from men. In personalization bias can cause a lot of issues for the company. Bias in algorithms in neural networks can cause “harmful discriminatory practices.”(Britt,2021) This could cause lawsuits or the loss of consumer faith. Rosaria Sillito from customerthink.com Could not have said it any better “Bias in, Bias out.”

**Analyzing GDPR on Personalization**

The General Data Protection Regulation or GDPR is an EU law on data protection and privacy. It was put in effect in May of 2018. There are seven key principles that make up the GDPR law transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability. Although all seven principles affect personalization, the four principles that directly affect personalization that we are going talk about are transparency, data minimization, storage limitation, confidentiality, and accountability.

According to Karl Wirth from Entrepreneur.com “Consumers are increasingly concerned about data privacy but willingly share their data with companies that have earned their trust.” Although on the surface this seems like a hardship for companies in reality it builds trust between users and the company. When collection data to use for personalization, it is important that we communicate to the users how the data is going to be processed. This includes how the algorithm helps personalizes the user experience. Also, it needs to be communicated if that data is later going to be sold. It is very tempting to to collect as much data that is available for later sale. With data minimization the company can only collect the data they need. Storage limitation is the most important and the most difficult to comply with. Data needs to have an expiration date attached to it, so the data is not kept long term. After the expiration date the data needs to be deleted or the data is stripped of all personal data to be used for statistical purposes. The users need to have the ability to remove all data related to them from the company servers. For confidentiality, any data that is collected it is the companies’ job to secure the data from theft.

**Impacts of GDPR on Company Practices**

Currently the company collects data on everything the user does within the website this includes mouse click to location data which is then fed though the company’s neural networks. The models created is then used to create a personalize experience. Currently there are no indications of our compliance to the GDPR law which leaves us liable for compliance. This can result in heavy fines being levied against the company. In 2018 the Marriott was fined $100 million dollars for a data breach. After a deeper investigation, the fine was later reduced to $23.8 million (2020). We need to update our policies, data collection methods, and security measures to bring us into compliance with the GDPR law. It is tempting just not to collect any data or just erase our database but that is not necessary. This can be mitigated by being transparent with what data is being taken and how the algorithms are using that data. There may be some data that we do not really need to collect such as monitoring user clicks within the website.

**Adaptations for Compliance with GDPR**

The company needs to make some changes to how we are collecting, storing, and using data to comply with GDPR. The first step will be looking for ways to preserve privacy in out Neural network. According to [www.boozallen.com](http://www.boozallen.com) there are four ways to preserve privacy in AI

1. Use good data hygiene
2. Use good data sets
3. Give users control
4. Reduce algorithmic bias

Using good data hygiene changes how we look at data and reduce the amount we need to but produce the same personalization that our customers expect. Do we need to keep track of everything the user does? What can we stop tracking? Use good data sets is the quality of data use to create our models. We need create data that that we train our neural networks that is “accurate, and fair”(n.d.) and check the results with other algorithms to check the quality. We need to give users control. This is including how their data is being used and if it is being used to improve the AI. They also should have the ability to deny the use of their data. When teaching the AI every effort must be taken to remove bias from the data. Now we need to make sure our databases are a secure as possible by using current industry cryptology methods.

References

*4 ways to preserve privacy in Artificial Intelligence*. Booz Allen Hamilton. (n.d.). Retrieved July 23, 2022, from https://www.boozallen.com/s/solution/four-ways-to-preserve-privacy-in-ai.html

Bavati, I. (2022, May 24). *Ethical personalization: Weighing benefits and risks*. KeenEthics. Retrieved July 23, 2022, from https://keenethics.com/blog/ethical-user-personalization

Britt, P. (2021, December 13). *4 tips for taming the bias in Artificial Intelligence*. CMSWire.com. Retrieved July 23, 2022, from https://www.cmswire.com/customer-experience/4-tips-for-taming-the-bias-in-artificial-intelligence/

Dorschel, A. (2020, May 8). *Data Privacy in Machine Learning: A technical deep-dive*. Medium. Retrieved July 23, 2022, from https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

*GDPR fines & data breach penalties*. GDPR EU. (2020, December 14). Retrieved July 23, 2022, from https://www.gdpreu.org/compliance/fines-and-penalties/

*Introduction to neural networks*. Section. (n.d.). Retrieved July 23, 2022, from https://www.section.io/engineering-education/introduction-to-neural-networks/

Janet. (2021, May 14). *Overcome and prevent bias in AI*. Figure Eight Federal. Retrieved July 23, 2022, from https://f8federal.com/overcome-and-prevent-ai-bias/

Marsh, J., Lucas, A., & Wilson, T. (2022, July 19). *3 ways AI is helping personalize customer experiences*. Datafloq. Retrieved July 23, 2022, from https://datafloq.com/read/3-ways-ai-helping-personalize-customer-experiences/

Spilka, D. (2018, August 15). *How GDPR can undermine personalization and user experience*. Business 2 Community. Retrieved July 23, 2022, from https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

*Tips for battling bias in AI-based personalization*. CRM Magazine. (2021, June 1). Retrieved July 23, 2022, from https://www.destinationcrm.com/Articles/Editorial/Magazine-Features/Tips-for-Battling-Bias-in-AI-Based-Personalization-147143.aspx

Wirth, K. (2018, June 19). *Personalization and privacy in a GDPR world*. Entrepreneur. Retrieved July 23, 2022, from https://www.entrepreneur.com/article/314611