Brian Engel

CS-370 Project 1

There are 2 main types of neural networks. There is a basic neural network, which consists of at least an input layer and an output layer, and often has hidden layers. The neural network takes the picture and pulls it apart and each level determines the probability of what the picture is. Each one of these stages is a perceptron, or basically a filter. It takes a series of inputs, associates it with a weight depending on a function, adds them all up and outputs a 1 or 0. In a multilayer perceptron or deep neural network, each of the neurons then passes the information along to every single neuron in the next perceptron, so each part gets analyze for many different patterns. A perceptron is either 0 or 1 and that is a big jump, and it will not help it to learn (Gulli 13), so it smooths out the number using an activation function, which is usually a sigmoid function or a rectified linear unit. This has the effect of saying there is a 90% chance that this picture is a car.

The other type of neural network is a convolutional neural network. These are usually used for processing grid type data, such as pictures and images. The layers in this type of neural network scan for patterns in the grid, such as horizontal or vertical lines. What’s interesting about this type of neural network is you can augment the data you already have by shifting, resizing, and rotating it to further train the model. These small differences make a convolutional neural network better suited at analyzing images and being able to pick out different objects from an image. For example, if you had a number on a white background, you would probably use the basic neural network, but if you had a number painted on a wall in an image with other objects around it, you would use the convolutional neural network to cut through all the noise. The reason you wouldn’t just use it for everything though is that it takes a lot longer to train the network in the first place.

Neural networks are used in almost every aspect of personalizing users experience. They are used in recommendation systems for every streaming service. They capture your browsing on e-commerce sites to recommend products. They are used in social media sites to display content and products you might like. The problem with these systems is that they can and most likely are biased. Facebook bases what comes into your News Feed off of what we have previously clicked and what our friends like (Granados). This is not an inherently bad thing because it should make it so it is populated with articles that you should find interesting. As long as you are aware of this you can also go to other places for information since you know that it is biased. I know there are plenty of times I have accidentally clicked on an article and started getting tons of similar articles popping up, and it is next to impossible to get out of the rabbit hole I accidentally fell into. There are obviously worse biases than this. When using a black box classification system, all you see is what goes in and what comes out, and nothing about how the model was trained. If the training material is biased, there is no doubt that the output will be biased. Filtering through training data and making it representative of what you are trying to achieve is extremely important to eliminate biases. A diverse labeling system and diversity in the people doing the labeling is important also. When it comes to training a neural network, “Garbage in means Garbage out” (Xiang).

General Data Protection Regulation is a set of rules to protect privacy and personal data in the European Union. This has implications for any company seeking to conduct business within Europe. There are seven principles behind the regulations: Lawfulness, fairness and transparency, Purpose limitation, Data minimization, Accuracy, Storage limitation, Integrity and confidentiality (security), and Accountability. They are set out right at the start of the legislation, and inform everything that follows. They don’t give hard and fast rules, but rather embody the spirit of the general data protection regime - and as such there are very limited exceptions (ICO). Transparency is affected because the user must be informed when their information is being used in order to create a personalized experience and given an opportunity to opt out of the personalization. For purpose limitation, the user must be informed of the purpose of the information being collected, such as personalization of content, and it can not be used for anything else. Data minimization in the context of personalization comes down to not collecting unnecessary data that has nothing to do with the purpose of personalizing the content. Accountability is necessary for data personalization to show that the organization has taken the other principles into consideration with the user’s data and is handling it securely and ethically. Basically, you need to prove you are following the other principles, not someone else needs to prove that you aren’t following them.

There is one line in particular that make me think that the company might be violating some or all of these principles: Your sales reps claim a click-through rate that is double that of your closest competitor because you know everything there is to know about your users. Depending on whether or not there is a Terms and Conditions Agreement that the user checks off on and specifically says that the company is authorized to collect all of the users data and use it for personalization purposes and is going to store it, there are a few potential breaches in the regulations that are pretty apparent. For transparency, the user would need to be informed of the information collected including mouse clicks, site navigation, links followed, time spent on a page, location data, and so on. Even with this though, it seems that this data goes beyond the scope of just personalization which is the stated purpose of the data collection. This would be a violation of data minimization. Also since there is storage of the data, it needs to be securely stored. The principle of accountability is obviously not being met since a regulator is asking about compliance and there is no answer. The fact that these things have not been researched yet is a violation in itself. Not collecting data from users would not be a good solution in my opinion. You would end up with very generalized advertising, which means the chances of the user actually clicking on the advertisement would be much lower. This in turn would lead to the loss of advertising income. It would also lead to a worse user experience, and could lead to a decrease in users, which would lead to less advertising dollars as well. Federated learning is an interesting compromise on this though, as it still collects data, but stores the parts of the algorithms that touch the data on the users’ computers (Ved). This would still need to be addressed in the transparency of the application though.

I touched on one trend in artificial intelligence and machine learning aimed at preserving privacy with federated learning, but there are several others as well. Generative Adversarial Networks and Matrix Capsules are forms of neural networks that require less data to train. Differential privacy, Homomorphic encryption, and Transfer Learning all help to protect privacy. Differential privacy adds noise to data purposefully (i.e. deliberate errors) so that even if it were possible to recover data about an individual, there would be no way to know whether that information was meaningful or nonsensical. Homomorphic encryption allows us to compute the data without decrypting it first. Transfer learning reuses a model on a new problem (Ved). For transparency there is also Explainable AI and Local Interpretable Model-Agnostic Explanations which explain the decisions that the AI came to. In order for the company to be compliant with GDPR, I would propose taking a close look at any existing Terms and Conditions Agreement and ensure that it accurately describes what information we are collecting, how it will be used and not deviate from that particular use, see if there is information that we are collecting that is not needed and eliminate it, checking to see if federated learning is an option for storage of the data we collect to limit our liability, and regularly review the way that we collect, use, and store data to hold ourselves accountable. The most effective solution is transparency and clear and efficient communication with the user.

Granados, Nelson. How Facebook Biases Your News Feed. June 2016. https://www.forbes.com/sites/nelsongranados/2016/06/30/how-facebook-biases-your-news-feed/?sh=26bda6321d51

Gulli, Antonio, and Sujit Pal. Deep Learning with Keras : Get to Grips with the Basics of Keras to Implement Fast and Efficient Deep-Learning Models, Packt Publishing, Limited, 2017. ProQuest Ebook Central, <http://ebookcentral.proquest.com/lib/snhu-ebooks/detail.action?docID=4850536>.

ICO. Information Commissioners Office. A Guide to Data Protection Principles. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/>

Ved, Anamike. How to develop Artificial Intelligence that is GDPR-friendly. February 28, 2019. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/

Xiang, Mark. Human Bias in Machine Learning. March 2019. <https://towardsdatascience.com/bias-what-it-means-in-the-big-data-world-6e64893e92a1>