The concept of neural networks has been around for decades, the thought of neural networks came about in the 1940’s and was used to model how the neurons in the brain functions. Fast forward 80 years and we have artificial neural networks. Neural networks are found in machine learning and more specifically, deep learning and AI (artificial intelligence) which is used for the improvement of machine learning. They can be used to solve real-world problems or for a specific purpose to assist humans with certain tasks. Neural networks are a set of algorithms modeled after the human brain (Fernandez, 2019). They are used to solve real-world and produce the best possible results based on the real-world data used to train the models.

One fascinating thing about the human brain is that it has over 80 billion neurons, now of course the neural networks created in no way come even close to that amount but nevertheless they do try to mimic the brains behavior. Neurons can be described as nodes interconnected together into layers which sends and receives messages when certain conditions are met. In a neural network a neuron is nothing more than a mathematical functions. Neural networks contain an input layer, an output layer and in between a hidden layer. Data is passed into the neural network through the input layer, the neurons in the input layer communicates with the hidden layers and passes the data. The hidden layers then process the data and assign the weights to the inputs. Input weights products are then summed up. This sum is then sent to the node’s activation function to determine how far a signal must go through the network to affect the final output (Insights, n.d.). It is at this time the hidden layer connects to the output layer so the outputs can be retrieved.

Just about everywhere you look you will see something computerized. A person would have to go out in the middle of nowhere before they would not see something related to computing. More than likely the car a person would drive to the middle of nowhere has some kind of computer in it. Our dependence on technology grows every day, most people could not get through the day if they did not have their cell phone or laptop. With all these computing devices running around in the world, would it not make your life so much easier if you were to see only the stuff you cared about whenever you are surfing the internet? This is where AI and machine learning come in and they are good at providing you with ads that a personal to you. They study your habits such as websites you visit, search terms, items purchased, and the list goes on forever.

Providing users with a personalized experience is done so with the use of machine learning and AI, models are trained endlessly so the experience provided to the consumer is the best possible outcome. So, the question is, does using AI and machine learning to generate ads that are targeted directly at the person browsing work? Well, numbers don’t lie, in 2020, paid advertising on social media reached the amount of $40 billion but in 2022 the sales from advertising on social media reached a staggering $56.85 billion, that is close to a 50% increase. While training the models weights are adjusted to make predictions and recommendations more accurate.

In black box AI classification systems decision making is usually trained by using large batches of data. The AI uses the data to build profiles of users based on their actions, such as websites visited, online purchases, web searches, choices made while visiting websites. The problem begins when the data used to train data contains bias, while data scientists do their very best to make sure the data used to train models does not contain bias, but data compiled by humans will almost always have bias. Data that contains bias can lead to AI that develops a bias which can lead to inappropriate materials being presented to a user. Unfortunately, this is where ethical concerns come into play. When an ethical violation is takes place, it can have huge legal ramifications. There are few laws or legislation in place to handle AI that creates ethical violations and privacy concerns.

In recent years, artificial intelligence has become a part of our normal everyday lives. The number of companies using AI has exponentially increased and the sophistication of AI has also grown. The more AI is interweaved into our lives, the more likelihood an ethical violation can occur, in the EU they have created the General Data Protection Regulation (GDPR) to regulate the use of personal data (Visier Team, n.d.). GDPR is broader and not just for AI but contains standards and guidelines for anyone developing AI or software. The two main areas of focus today are privacy and ethics, as AI learns and evolves based on modeling it can introduce ethical and privacy violations which is exactly what the GDPR was written to prevent.

For the application in our mock company, all (Medairy, n.d.)the GDPR principles will need to be addressed. Here I will outline each and show why it is important that the principles and guidelines must be followed. Starting with transparency, it is paramount that our company lets users know exactly what is being done with there information, what information is being captured and that information captured will not be shared or sold. This is important because if our company does not disclose this information, they could be setting themselves up for litigation implying the misuse of user data. If this information would have been made it could prevent legal fees and possible harm to the reputation of the software. Purpose limitation goes hand in hand with what I mentioned in transparency. The purpose of gathering information it must be documented the purpose for the gathered data, the data collected can only be stored until it is no longer applicable which is usually whenever a user updates data or cancels their account. As stated above, only the data we specify can be collected and nothing more. Data collected must be accurate and must not be manipulated. If for some reason incorrect data is collected or if the data is referenced to the wrong user this could be a huge issue. First and foremost, this raises privacy concerns as the information from one user may be shown to another user. It is possible if data is not accurate it could violate data minimization, purpose limitation and transparency. Mainly if the information collected isn’t information the company reported to the user as collecting. Storage limitation is directly related to purpose limitation, it can only be stored for the time it is applicable and no longer. All data stored must be confidential, securing data will prevent data breaches and if data breaches did occur it may prevent difficult to decrypt if it were to be encrypted. This is very important for multiple reasons, if data is not secure and records are leaked, the confidence of the company will be lost and should that happen, it could last for years affecting the companies’ finances. Not only that if the GDPR was violated there could be fines and/or civil penalties. Accountability feeds right into what was being discussed in confidentiality if a regulation of the GDPR is violated there must be accountability if the first 6 are not followed and violations take place. In my opinion there does not need to be penalties for violations that arise from AI learning and transforming itself. Not every scenario can be accounted for and there may be situations in which AI may raise ethical concerns. For situations with what happened to the Google Photos in 2015, I believe there should be very harsh penalties, because the next time a company will think twice before they deploy software where there is a probability ethical or privacy concerns.

As I learned in a previous course, current trends to preserve privacy starts with the development. It is improbable that AI will ever think like humans do, this means that our information must be used to train AI. Our personal data can sometimes be used against us and without our control. Developers can reduce privacy concerns during development (Medairy, n.d.). Creating data policies and strategies along with monitoring of AI will further minimize the chances of privacy breaches. Other ways to protect privacy are:

Use good data hygiene - Means you only collect the necessary data types, it should only be

kept if it is applicable and while keeping it make sure it is secure.

Use good data sets – AI should be built to be accurate, fair and representative of the data

used to train it. Algorithms should be written to check other algorithms for quality.

Give users control - Users should know when their data is being used to make decisions

regarding them. Users should also be able to control what of their information is

used, when it is used and how it is used.

Reduce AI Bias – Ensure data used for training is as free from bias as possible. While it is

not entirely possible to remove all bias randomizing data is a good way to reduce bias.

One change that can be made to the way the company collects data is a system that a lot of large companies today (such as Apple) is differential privacy. Differential privacy is a system for publicly sharing information about a data set by describing patterns of data within the dataset without revealing information about individuals in the dataset. (Rachel Cummings, 2018). The theory behind differential privacy is it is a way to prevent individual records from being identified by adding noise to data in a controlled manner. This guarantees privacy no matter what a hacker knows or what they do during an attack on the data. It does not matter how much computing power and knowledge of algorithms and systems used to collect data. A popular mechanism used in differential privacy systems is the Laplace mechanism. In this type of mechanism noise is added to output of a function, the amount of noise created by the function depends on the sensitivity of that function and is obtained from a distribution. The sensitivity of a function corresponds to how much of an impact a individual records can affect the output of the function in a worse case scenario. The key to differential privacy is adding noise to data used to train AI. It is claimed that individual privacy is safe when it is used, only the future will tell.

In conclusion, AI is only going to get smarter and more sophisticated. As it does the potential for privacy breaches and ethical concerns grow. There must be legislation or guidelines and standards put in place to ensure software written does not raise ethical concerns. The U.S. government has not introduced any legislation to regulate development of AI. Neural networks are amazing and how they work are astonishing. If they can be approved or changed them to mimic human brain activity is left to be seen. In my opinion, I don’t think they will ever get neural networks to function just like human brains because they still aren’t sure how the brain learns and saves information. The technology industry is at an impasse, something must be done before the proverbial snow starts going down the hill. Because once it starts rolling it will be very hard to stop.