Matthew Trembley

9/25/2022

Southern New Hampshire University

CS-370

Project One

An issue has been brought to the company’s attention that the way user data is collected and utilized may violate certain aspects of the General Data Protection Regulation (GDPR). The following text is a basic outline of some artificial intelligence ideas such has neural networks, and how they interact with a user and the user’s data to address concerns of the EU regulators of the GDPR.

Starting with neural networks, which bares some resemblance to the human brain’s own nervous system, is a data algorithm that in it’s basic definition filters data from an input to produce an output. In an academic textbook, *Deep Learning with Keras*, the authors define a neural network as a “class of machine learning models… Each net is made up of several interconnected *neurons*, organized in *layers*, which exchange messages when certain conditions happen” (Deep Learning with Keras, 2017). A node in a neural network is loosely modeled after a neuron in a human’s nervous system where single computations happen. Many nodes make up a layer, in which there could be many layers inside any given network. A deep-learning network is composed of **3 or mores** layers; input, “hidden”, and output. Each layer of nodes will train on a distinct set of features based on the output of the layer before it. The further you advance into the neural net, the more complex the features your nodes can recognize, since they aggregate and recombine features from the previous layer (A Beginner's Guide to Neural Networks and Deep learning, n.d.). Simply put, the first layer is input from the user. Each subsequent hidden layer will filter and output a result to the next layer until finally it reaches the output layer, which is more akin to a classification or label than a tangible “output”. If a network was to train on a set of 100,000 photos of people, and then a user inputs a picture of a person, it start with the input layer. It will then move to the hidden layers, where it will continually piece together small features through each hidden layer. Once it is through all the hidden layers, the network essentially will output something to the effect of being 95% sure this photo is of a person, and label it an arbitrary term like male, female, person – whatever the program is designed to do.

Neural networks are utilized in the creation of personalized experiences through the collection of data and filtering of said data. Data from third-party sources and cookies can be used to personalize a user’s experience. This can curate a wide variety of experiences – for example; if a user was using a search engine to find facts about New Hampshire, posts on social media may start to include information or users from New Hampshire through use of a network. The input data is the user’s search engine queries, which may be data sold or tracked to a third party, and on a social media platform the network will narrow down all posts to New Hampshire and surrounding areas to personalize the user’s experience. A main ethical issue with this is violation of users’ privacy. At what point is too much information being sold and/or tracked between companies that a user’s privacy has become exploited? What happens if the data being store in a neural network is compromised? These are big questions that are still being debated. Meanwhile, other ethical concerns such as bias may occur. If a neural network is trying to personalize a user’s experience, it is entirely possible for it to go too far and become bias. Biases will tend to arise in a “black box” classification system, where the user does not know about the algorithms. In an academic journal for Tongji University in Shanghai, China, the authors write, “Unlike traditional [machine learning] methods, the training process of [deep learning] lacks transparency” (Explaining the black-box model, 2021). Neural networks, which is considered deep learning, has the high potential of lacking transparency. The end-user can not possibly know how exactly the network and algorithms work, therefore reducing confidence in the usage of applications where these networks exist. Transparency in and of itself may have an effect on personalization.

There are few portions of the General Data Protection Regulation that can affect personalization. First and foremost, transparency is one of the most important concepts to users. Users feel much more comfortable using software if the company providing it is clear and concise in how they gather and use data. If the user may reject this acquisition of their data, the software may not be able to deliver a personalized experience. This transparency goes hand in hand with data minimization. Data minimization is a principle that only data gathered for pre-determined purposes may be gathered, nothing more. As the GDPR law states, “Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed” (General Data Protection Regulation, 2018). This boxes in companies to set a purpose for data before they retrieve it and using the data only for that purpose. As data is collected it will also need to be stored. The GDPR specifies that data can only be kept for so long, and that it must be disposed. The time span can be quite vague, as the law references “public interest, scientific or historical research purposes or statistical purposes” (GDPR, 2018). This broad wording does give some companies room to store data for a longer amount of time, enabling them to continually give a user a personalized experience. But the longer the company stores personal data, the longer it is potentially exposed to bad actors trying to access private user data. Also, not only does the data need to be collected purposefully and only for a finite amount of time, the data needs to be accurate. If a company collects data on someone living in Ireland, they can not utilize it in a way that portrays the person living halfway around the world like the state of Hawaii.

The General Data Protection Regulation is affecting the company’s practices in a positive manner. The company applies neural networks to promote a personable and engaging user experience to maximize the user’s time on the site. The regulation is not a roadblock hindering the sites ability to give the user a positive experience but acts more as a guideline to be ethical and trustworthy site. The use of neural networks does give way to legal concerns – mostly dealing with data storage, data manipulation and handling, and confidentiality. Using neural networks as a classifier to personalize the user experience could possibly backfire if a fault arises in the any of the steps of the network, whether it be training, testing, or application. If a network becomes faulty, the potential to expose private data of user A to user B can happen. Not collecting data is not a possibility for the company’s business model. This is because personal data being collected helps generate revenue by creating personalized ads. If the user has spent time searching online for shoes, ads for shoes will then appear on the site to keep the user interested in their search. It would be infeasible to suddenly stop curating a personalized experience to the user, as that is also a selling point of using the site – not just the ads.

One trend that helps avoid black-box issues and other privacy concerns is Explainable AI (XAI). This idea surrounds that all decisions made by AI should be explainable to the user. In XAI, the software is programmed to describe its purpose, rationale, and decision-making process in a way that can be understood by the average person (How to develop Artificial Intelligence that is GDPR-friendly, 2019). This immediately improves transparency to the user and improves accountability for the company. If the company needs to make the honest effort to explain exactly what the AI is doing to the user, it will in effect push the company into compliance of transparency and hold them accountable for their use of data. Another technique that helps with privacy concerns is a matrix capsule. Matrix capsules are a new type of neural network that require much less data for learning compared to traditional deep learning networks. For the company to stay within compliance, the technique of differential privacy. Differential privacy “represents a stringent privacy notion guaranteeing that no individual’s data has a significant influence on the information released about the dataset” (Rethinking Data Privacy, 2019). In practice, the goal of differential privacy is to ensure that anything learned about a user from released information can be learned without that user’s data being included. This means an algorithm is differentially private if an observer examining the output is not able to determine whether a specific individuals information was used in the computation (Rethinking Data Privacy, 2019). If the company can adopt and maintain algorithms based around differential privacy, user data may not need to be stored for longer neural networks or than need be. Paired with explainable artificial intelligence, the company can be transparent, accountable, and conscious of user data and how it is handled.

# References

European Union. (2019, September 2). *General Data Protection Regulation (GDPR)*. Intersoft Consulting. Retrieved September 23, 2022, from https://gdpr-info.eu/

Dorschel, A. (2019, April 24). Retrieved from Medium: https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60

Gulli, A., & Pal, S. (2017). *Deep Learning with Keras : Get to Grips with the Basics of Keras to Implement Fast and Efficient Deep-Learning Models.* Packet Publishing Limited.

Liang, Y., Li, S., Yan, C., Li, M., & Jiang, C. (2021). Explaining the black-box model: A survey of local interpretation methods for deep neural networks. *Neurocomputing*, 168-182.

Nicholson, C. (n.d.). *A Beginner's Guide to Neural Networks and Deep Learning*. Retrieved from Pathmind: https://wiki.pathmind.com/neural-network

Ved, A. (2019, February 29). *How to develop Artifical Intelligence that is GDPR-friendly*. Retrieved from Tech GDPR: https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/