**Project One**

Kevin Liu  
Southern New Hampshire University  
CS-370: Current/Emerging Trends  
Professor Yaroslav Litvak  
March 30, 2025

**Project One**

Neural networks are defined as a subset of machine learning that mimic the human brain's ability to recognize patterns (Goodfellow et al., 2016). Neural networks are made up of three primary layers, the input layer, hidden layer, and the output layer. The input layer receives the data or information, while the hidden layer processes that data through weighted connections, and then the output layer produces the result. This process is also known as forward propagation as data moves through the layers of the neural network. These layers work together with a vast ocean of data to produce optimized and accurate results.

Neural networks can be used to create a personalized experience for its users. For example, TikTok has done this successfully through their algorithm and neural network. It uses vast amounts of data to analyze behavior, preferences, and interaction of its users to provide the best experience. However, ethical concerns arise when considering the “black box” nature of neural networks. Neural networks trained on a vast amount of data cannot explain how it arrives on certain conclusions or results. This is due to vast calculations happening at the same time and with billions of data points it is hard for humans to understand. Therefore, many creators will train systems until they get their desired result without being to explain it. The lack of transparency of these systems makes it difficult to trace how decisions are made, leading to potential biases and unintended discrimination. This lack of transparency also raises concerns of accountability, as users and regulators struggle to understand these outcomes.

Regulars created the General Data Protection Regulation (GDPR) to combat lack of transparency along with other issues. GDPR is a set of strict guidelines used for data protection and these include transparency, purpose limitation, data minimization, accuracy, storage limitation, Security, and Accuracy. Companies must be transparent and inform users about data collection and processing methods in an accessible and understandable manner (European Parliament, 2016). They must only use specified data stated in the agreement when users give their consent. They only need to collect and store the minimum amount of data necessary for personalization. They must be accurate with user data and ensure they are up to date and corrected if necessary. They cannot retain personal data indefinitely and must be deleted after a defined period. They also must ensure adequate protection such as encryption and access controls, which must be in place to safeguard user data. Finally, they must be accountable with regular audits that need to be completed in a timely manner.

Companies will need to change their practices in accordance with these guidelines to avoid legal consequences, however legal concerns remain. Reliance on extensive user data to power neural networks could lead to misinformed consent, where users can be misled to give consent and have their data used for another purpose. Data repurposing arises when behavioral data is reused for newer AI models without renewed consent, violating purpose limitations set by GDPR. Retention policies of user data can also be a cause for concern with storage limitations that prevent the indefinite storage of user data. Transparency may also be an issue when considering the lack of explanations in neural networks. These legal concerns are a headache, but they need to be considered as data collection is inevitable for the business model due to the utilization of neural networks in its personalization algorithms. The company collects user data in the form of mouse clicks, site navigation, links followed, time spent on a page, and location data. Everything a user does within the app is stored and fed into multiple neural networks that create models designed to personalize the user’s experience on the site, making it impossible for the company impossible to operate without collecting data.

To comply with GDPR, homomorphic encryption is one adaptation in artificial intelligence and machine learning aimed at preserving privacy. Homomorphic encryption allows data processing without exposing user data, ensuring user privacy while enabling neural networks to analyze encrypted data without decryption, maintaining GDPR compliance of transparency, and security. Another adaptation that complies with GDPR would be federated learning. This enables machine learning models to be trained across decentralized devices rather than centralizing user data in a single location. This is how federated learning enhances data minimization, storage limitation, and confidentiality. Homomorphic encryption and federated learning can be used together to achieve a balance between personalization and privacy while adhering to GDPR guidelines.

By addressing ethical and privacy concerns along with GDPR guidelines our company can maintain its leadership in personalized social networking. Implementing homomorphic encryption, federated learning, and following GDPR guidelines will enable us to provide highly personalized experiences while ensuring data protection. These implementations will mitigate data breaches, strengthen user trust, and create transparency. Therefore, allowing the prosperity of the company and the happiness of its users.

**References**

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

General Data Protection Regulation. (2016). *General Data Protection Regulation (GDPR) – Official legal text*. Retrieved from <https://gdpr-info.eu/>

Information Commissioner's Office. (n.d.). *UK GDPR guidance and resources*. Retrieved from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

*How to develop artificial intelligence that is GDPR-friendly*. (n.d.). [Reading].

*Rethinking data privacy: The impact of machine learning*. (n.d.). [Reading].