**4-2 Project One**

Winnie Kwong

Southern New Hampshire University

CS-370 Current/Emerging Trends in CS

Professor Balogun

February 4th, 2024

**How Neural Networks Works**

Neural networks, also known as artificial neural networks (ANNs), can be defined as “… a subset of machine learning and are at the heart of deep learning algorithms. Their name and structure are inspired by the human brain, mimicking how biological neurons signal to one another.” (What Are Neural Networks? | IBM, n.d., para 1). The neural network comprises three layers: the inner, hidden, and output. However, ANNs will only have one inner and outer layer. The first layer of the nodes, the input layer, is when input data is received from the outside world to further process into the hidden layers. Many ANNs can have one or more hidden layers responsible for the learning patterns in the data that develop into a new representation, making it easier to understand and learn from. Lastly, the output layer is the final stage, where the data can be classified based on the weights and biases from the previous layers. Understanding neural networks helps to understand how data is learned, how to make accurate decisions, and how to handle complex patterns.

**Neural Networks Creating Personalization**

Neural networks are utilized to aid in the personalization of user experiences in various ways, such as analyzing user data and targeted advertising. When analyzing user data, neural networks can use data such as purchase and browsing history to determine a user’s interests and needs. In Kalinski’s article, a user frequently searches for cleaning products and pet food on a retail website. The website would be able to collect the data from the search history and determine any hidden connections to reveal more information about their customers. Using neural networks and collaborative filtering can identify patterns and similarities between two individuals. Suppose a person is looking to purchase property, and based on user data, the individual has similarities to a prior subject. As a result, neural networks could recommend other properties they have not seen with the same similarities as prior individuals. Kalinski (2021). While looking at user data, neural networks can also focus on demographic categories to target relevant ads or other interests. An example would be music preferences based on a person’s age and suggesting other music with similar temps to the user’s favorites.

A "black box" classification system occurs when there is a lack of transparency and explainability. It causes uncertainties for algorithms that are unknown to the user. However, one of the most significant ethical concerns that can be raised in the "black box" classification system is privacy and hidden biases. Since personalization requires heavy data collecting, privacy is always a concern due to security uncertainty. Security breaches are common, and companies can be prone to hacking, potentially leading to unauthorized users accessing sensitive user information that can be misused for their benefit. When looking at unintentional biases can cause issues within the applicant tracking systems as well. Amazon has problems with its natural language processing (NLP) algorithms after discovering it favored hiring men because certain words, such as "executed" or "captured," were on the resumes more than women. (IBM Data and AI Team, 2023). If the NLP continued, Amazon could have been involved in lawsuits involving gender discrimination. Another example is identifying areas with high crime rates. When used, historical data can lead to patterns of racial profiling, causing an enormous rift between communities. With the rise of ethical concerns growing in neural networks, it must be addressed through human observation to provide users with their rights and transparency.

**GDPR that Affects Personalization**

General Data Protection Regulation (GDPR) regulates data protection and privacy to give individuals control over personal data. Seven portions of GDPR are transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability. Transparency ensures a context is open and honest to ensure best practices are in place. Transparency is beneficial for data protection because it provides clear and concise communication for users to understand quickly what personal data is collected. Purpose limitation and data minimization ensure data collected is limited to strictly its intended purpose. Purpose limitation and data minimization are beneficial because they minimize the exposure of data breaches of users’ sensitive data. Accuracy is an essential factor when collecting data to ensure all information is up to date. Without accuracy, personal data could stir uproars in defamation. Storage limitation ensures data can only be stored only when it is necessary for why it was collected. Since data expires, it helps protect sensitive information and reduce the risk of data breaches. Confidentiality ensures all data is protected from any unauthorized users. By keeping sensitive information confidential, users are more likely to trust all data handling is secure. Lastly, accountability is placed to make sure organizations comply with GDPR. Accountability ensures responsibility is justified when handling personal data. Transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability are the framework of GDPR.

**GDPR Affecting Company’s Practices**

Legal concerns that arise from GDPR affecting company practices while using neural networks as a classifier to personalize user experience by transparency, data minimization, accuracy, and accountability. Ved argues, “Organizations should improve AI systems transparency by investing in scientific research on explainable artificial intelligence.” (Ved, 2019, para 4). If organizations improve their AI systems, they can build trust, confidence, and overall public acceptance, enabling AI systems to be integrated into our lives. Data minimization is used to collect only sufficient and relevant data for the purpose for which it is being collected. Companies can follow these standards by identifying the purpose and limiting the collected data. Practicing accuracy on personalization ensures all collected data helps to avoid any misleading information that may negatively impact a user’s experience and trust. Due to GDPR’s principles, organizations must ensure data is accurate and up-to-date, or the inaccurate data must be erased from storage. Lastly, accountability affects personalization by increasing responsibility and reducing the risk of ethical concerns. All collected data must be fair and transparent to empower individuals with user rights. With an understanding of transparency, data minimization, accuracy, and accountability, companies can follow the standards of GDPR for best practices.

Not collecting data is a possibility, depending on the company type. Suppose a company is a small craft business that sells products directly to buyers for cash. These types of companies practice direct transactions that do not require collecting data as long as there is no online presence or digital payments. However, companies like Amazon and Walmart would find it more difficult not to collect data because they require personal data to stay with current trends and attract customers continuously. Although a company can refrain from collecting data, it would be difficult for it to increase scalability.

**Proposition for Company Practices in Compliance with GDPR**

Current artificial intelligence (AI) and machine learning trends aimed at preserving privacy are differential privacy (DP), consent requests, and establishing frameworks and regulations. Dorschel states, “DP represents a stringent privacy notion guaranteeing that no individual patient’s data has a significant influence on the information released about the dataset.” (Dorschel, 2019, para 12). By using DP, individuals can remain confidential while the system can accurately analyze data. With the rise in concern about data privacy, many websites request users agree to data collection terms before allowing users to access the website. Having the opportunity to decide whether to consent to data collection also enables users to feel empowered regarding how their data can be collected and used. Lastly, many websites are currently establishing standard guidelines for how data is collected. Since companies are establishing frameworks and regulations for AIs and their development and data protection, users are exposed to transparency. There are plenty of other current trends for AI and machine learning that are aimed at preserving privacy. However, DP, consent requests, and establishing frameworks and regulations will mitigate ethical concerns.

How a company collects, stores, and employs user data to comply with GDPR is viable by using data sharing, designing products that protect privacy, and researching provisions. Data sharing requires cautious considerations, such as implementing security measures to protect unauthorized users. When companies use security measures such as encryption to mitigate the risk of data breaches or access controls to ensure users only have permission based on their specified tasks. Children’s privacy is always a concern for parents, and GDPR has a proposition to enable high privacy settings on shared devices. According to ICO, “If you allow multiple users to access a service from one device, where possible, allow them to set up their own profiles with individual privacy settings.” (Protect children’s privacy by default, n.d.-d). An example of children creating their profile is on Netflix, which will ensure high restrictions on children’s profiles. Lastly, when using research provisions to comply with GDPR, using principles such as storage limitation can provide data protection with appropriate safeguards. According to ICO, when using storage limitation, personal data collected cannot be kept longer than needed, ensuring data breaches or unauthorized access is mitigated— (Principles and grounds for processing, n.d.-e). Using data sharing, designing products that protect privacy, and research provisions can ensure companies can collect, store, and employ user data to comply with GDPR.

**References**

Dorschel, A. (2021, December 9). Rethinking Data Privacy: The impact of Machine learning. *Medium*. <https://medium.com/luminovo/data-privacy-in-machine-learning-a-technical-deep-dive-f7f0365b1d60>

IBM Data and AI Team. (2023, October 16). *Shedding light on AI bias with real world examples*. IBM Blog. <https://www.ibm.com/blog/shedding-light-on-ai-bias-with-real-world-examples/>

ICO. (n.d.-e). *Protect children’s privacy by default*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/designing-products-that-protect-privacy/childrens-code-design-guidance/protect-children-s-privacy-by-default/>

ICO. (n.d.-d). *Principles and grounds for processing*. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/the-research-provisions/principles-and-grounds-for-processing/>

Kalinski, A. (2021, December 13). Personalization using machine learning — from data science to user experience. *Medium*. <https://medium.com/booking-product/personalization-using-machine-learning-from-data-science-to-user-experience-3b1ef5d23ced>

Ved, A. (2023, April 19). *How to develop Artificial Intelligence that is GDPR-friendly*. TechGDPR. <https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/>

*What are Neural Networks?  | IBM*. (n.d.). <https://www.ibm.com/topics/neural-networks>