An artificial neural network (ANN) is a collection of layers comprised of nodes, or neurons, that serve to imitate the biological neural networks and neurons found in the brain. At the most basic level is the neuron, which is a mathematical computation with an associated weight. These neurons can utilize input from previous layers, if applicable, to be utilized in a computation and output the result. A weight is attached to the computation that can be modified to fine-tune each neuron's output over multiple test iterations to identify patterns more efficiently and accurately. A collection of neurons is structured in layers to form an ANN. It is important to note that information is passed between each layer sequentially (JavaTpoint, n.d.), meaning each neuron will incorporate, evaluate, and distribute the result one at a time. Furthermore, each neuron in a layer is connected to all the neurons in the previous and next layers. The first layer to receive data from the training data set is the input layer, which performs the initial processing of the information and disseminates the output to the next layer. From there, the information will be iteratively passed to one or more hidden layers, which further perform calculations to identify patterns present in the data and pass along the subsequent value. Finally, the data will be received by an output layer, which will provide information on the pattern identified by the ANN.

To determine how ANNs are utilized in aiding the personalization of the user experience, it is first critical to determine how ANNs identify and learn patterns. Once the ANN is implemented, a large volume of training data will need to be passed into the model. This training data should be segmented to ensure the model is continually learning patterns from fresh, unseen data. Furthermore, the training data should be previously documented with associated labels so the output of the ANN can be compared to verified data. As data is fed into the model, the previously mentioned weights will be continually adjusted through a process such as

backpropagation to continually tailor the model's output to the expected results. Subsequently, the model will be able to identify trends in the data and determine patterns with increasing precision.

With this information, ANNs can be utilized to enhance the user experience through personalization by extracting features from unstructured data (RecoSense, n.d.). This can be achieved by inputting the vast amount of information gathered through user interaction into an ANN. The model will then be able to identify notable data points, which are described as "using what's learned to segment users according to attributes like lifestyle or purchase habits. The business will then personalize its content and services based on the specific needs of each segment" (RecoSense, n.d.). By leveraging the computational power of computers, these user features can be identified quickly, and an organization can then recommend similar content based on relevancy. User interaction can further the accuracy of these recommendations by incorporating feedback from users, such as whether the recommendations were helpful or not. As the user continues to interact with the system, a more precise profile can be curated, and personalized content can be significantly improved.

However, utilizing ANNs to enhance the user experience through personalization does raise ethical concerns. As the ANN is utilized to enhance personalization, it will inevitably create a detailed profile of each user, which raises privacy concerns. Each profile is likely to contain sensitive user data that may be obtained in unauthorized ways and maliciously exploited through cyberattacks (Kumar, 2023). Next, hidden biases can be perpetuated in ANNs due to poorly defined training data. Should the ANN utilize a "black box" classification system, users will have no clear transparency on how decisions were made on their behalf. This lack of

transparency is described as “customers may be unaware that AI is used to target them with advertisements, and they may not comprehend how the algorithms operate or why they are being targeted. This lack of openness raises issues about consumer autonomy and the possibility of manipulating customers without their knowledge or agreement” (Kumar, 2023). Furthermore, the model may return data that is fictitious or discriminatory, which can have severe influences on individual user experiences.

The General Data Protection Regulation (GDPR) took effect in 2018 and serves to safeguard the interests and privacy of European Union (EU) citizens. As network traffic to the social networking company will likely include EU citizens, it is necessary to comply with the principles outlined in the GDPR. These principles are transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability. Initially, companies must clearly define how they will utilize user data. Then, data can only be gathered for these specific, clearly defined purposes and cannot be archived for future use. The company must also ensure to keep all data up-to-date, and all inaccuracies must be fixed immediately. All data must be kept secure to prevent unauthorized access and can only be stored for the duration of the time it is applicable. Any company found not to follow these principles is accountable and will subsequently face applicable repercussions.

By giving users full control over their own data, certain principles within the GDPR will affect personalization for companies that utilize such data. Transparency means that a company will clearly define how they are utilizing data. Therefore, the data to be used must be declared to the user in a consent request. Should the user decline consent to their data, content cannot be personalized based on their activities or interests. Furthermore, “black box” classification

systems cannot be utilized as they do not reveal how decisions were made. Purpose limitation and data minimization ensure data can only be collected based on these pre-determined purposes and cannot be archived. This solidifies the scope of data that can be collected, and additional data outside this scope cannot be collected to support content personalization. The company must also keep all data up to date without inaccuracies, as described in the accuracy principle. Subsequently, user data that is collected must be continually updated, and old profiles may not be used for personalization. Additionally, delivered content must be appropriate, as described as "the design, development, and use of AI should ensure that there are no unlawful biases or discrimination" (Ved, 2019). Therefore, a portion of personalized content will not be usable, and companies must closely monitor what information is being displayed to users. Finally, storage limitation declares that data can only be kept by a company for as long as it is applicable. This can severely impact the personalization of intermittent users, as if the profile cannot be maintained due to the time limitation, the data must be removed, preventing the possibility of immediate personalization (Spillane, 2022).

The company's use of ANN as a classifier to personalize the user experience may run into legal concerns as current operations do not adhere to GDPR guidelines. The company collects a vast amount of user data that users are likely not aware of. This involves tracking site navigation, links followed, time spent on each page, location data, and more. Furthermore, the ANNs utilized by the company are likely "black box" classification systems that do not provide insights on how determinations were reached. Subsequently, the collection of this data without informing the user and making unclear decisions are violations of the transparency principle of the GDPR. The company also does not clearly state what data will be collected from the users. In doing so, the purpose limitation and data minimization principles of the GDPR have been

breached, as current data collection methods have no pre-defined boundaries. Furthermore, the data collected is seemingly stored for an indeterminate amount of time for future personalization, which is not permitted under the storage limitation principle. Finally, the company does not possess any descriptions of how they maintain the accuracy or confidentiality of stored data. The content delivered to users in an ANN is highly personalized yet may contain hidden biases that may cause damage (Guidotti, Monreale, & Pedreschi, 2019), while user profiles may contain outdated information that is not permitted by the accuracy principle. Due to these infractions, the company may face further warnings, severe administrative fines, or varying levels of bans for data processing.

An alternative approach to complying with GDPR regulations is to not collect any data. However, this strategy would be significantly detrimental to company operations, user experience, and customer satisfaction. This is because this approach would effectively cease the personalization efforts the company currently offers, which would detract from preconceived user expectations. Subsequently, many users would likely no longer utilize the products made by the company, and revenue streams would rapidly decline. Therefore, a better approach would be to implement adaptations to current company operations to comply with GDPR guidelines.

To adhere to GDPR guidelines, the company should utilize best practices in artificial intelligence (AI) to better preserve privacy. One notable practice is to utilize a differential privacy technique to explicitly add noise and errors to the data to prevent damage from unauthorized access. This technique is described as “adding 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. One useful feature

of this approach is that even though errors are deliberately introduced into the data, the errors roughly cancel each other out when the data is aggregated" (Ved, 2019). Furthermore, all sensitive data should be anonymized in storage mediums and during ANN processing to effectively sanitize the data. Sokhach (2023) describes the benefits of data anonymization as minimizing the risk of prohibited access to personal data while still making the data available for research or analysis. This strategy also serves to protect the data minimization principle of the GDPR, as data outside the pre-determined collection boundary would not be introduced into the model.

Additionally, multiple changes should be made to the way the company collects, stores, and employs user data to comply with GDPR. First, the company should seek consent from users with detailed descriptions of the scope of data to be collected. Additionally, the company should utilize explainable AI (XAI) to enhance the transparency of the model's decision-making process. This is due to the nature of an XAI, which can "describe its purpose, rationale, and decision-making process in a way that can be understood by the average person" (Ved, 2019). These two modifications serve to uphold the transparency principle of the GDPR by explicitly defining how user data will be utilized and better explaining the decision-making process. By only gathering pre-specified and agreed-upon data, the company will also follow the purpose limitation and data minimization principles. Furthermore, biases in data can be minimized by utilizing an XAI to ensure the accuracy of output data through the transparency and responsiveness of the model. Next, any data that is stored by the company should also have an expiration date applied to ensure data is retained for only as long as applicable. This measure should be paired with the frequent updating of stored personalization metrics to ensure all data is kept up to date. Additionally, the data should be encrypted with adequate access controls applied

to prevent unauthorized access. In doing so, the company will be able to securely protect current data while only storing it for a predetermined length of time in accordance with the accuracy, storage limitation, and confidentiality principles of the GDPR.

Certain existing practices can be maintained throughout this transition to GDPR compliance. The company can continue to gather a similar range of information, outside of unnecessary sensitive personal information, from users if it has been transparently declared and with consent from the user. This is because the data minimization principle declares that data can only be gathered if it is specifically within the pre-defined scope. The company can also continue to provide highly personalized content for users based on the information contained within the pre-defined data collection boundary, so long as the content is validated to be accurate and free of potentially discriminatory information. Finally, data collected can be stored, albeit for a specified duration and in a secure fashion, to be considered in content personalization efforts as described in the storage limitation and confidentiality principles. With these modifications, the company can continue to provide highly personalized content to users while fully complying with GDPR regulations and incorporating best practices for privacy and data protection.

References

Guidotti, R., Monreale, A., & Pedreschi, D. (2019, January 22). The AI Black Box Explanation Problem. ERCIM News. https://ercim-news.ercim.eu/en116/special/the-ai-black-box-explanation-problem

JavaTpoint. (n.d.). Difference between Artificial Neural Network and Biological Neural Network. https://www.javatpoint.com/difference-between-artificial-neural-network-and-biological-neural-network

Kumar, D. (2023, March 31). Ethical and legal challenges of AI in Marketing: An Exploration of Solutions. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4396132

Sokhach, D. (2023, March 21). 4 Ways to Preserve Privacy in Artificial Intelligence. Landbot. https://landbot.io/blog/preserve-privacy-artificial-intelligence

Spillane, J. (2022, December 8). How GDPR Can Undermine Personalization and User Experience . Business2Community. https://www.business2community.com/customer-experience/how-gdpr-can-undermine-personalization-and-user-experience-02108269

RecoSense. (n.d.). Deep learning in Personalization. https://recosenselabs.com/blog/deep-learning-in-personalization

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