**Responsible Use of Neural Networks in a Social Networking Application**

Connie M. Knupp

Department of Computer Science, Southern New Hampshire University

CS370: Current / Emerging Trends in CS

Dr. Ashima Yadav

September 28, 2025

A major component of a company’s success as an industry leader in social networking is personalization. Efficient personalization relies on a well-developed neural network as a key part of the artificial intelligence (AI) system. It is expected that the software will anticipate consumers' needs in terms of recommended posts, recommendations for friend requests, groups to join based on shared interests, news articles, discussions they can join, games they can play, and other site features that they may find interesting. Additionally, revenue is derived largely from personalization, which enables higher click-through rates compared to those of competitors. However, users demonstrate a reluctance to accept unwarranted intrusions into their privacy in order to gain a personalized experience. To ensure the continued successful utilization of this technology, it is critically important to understand how neural networks are being used within social networking software. Furthermore, it is of equal importance to assess each system’s compliance with the legal standards set by the General Data Protection Regulation (GDPR).

Artificial neural networks (ANN) are computerized models for machine learning that were based on findings from studying natural neural networks found in the central nervous system of mammals. Each ANN consists of layers of interconnected neurons that fire messages when specific conditions are met (Gulli & Pal, 2017). Data is fed into an input layer, the layer responsible for receiving raw data. This layer does not process the data; it only receives it and passes the data to the next layer. The next layer is typically hidden. Hidden layers are “the intermediate layers between the input and output layers. They perform most of the computations required by the network.” (“Layers in Artificial,” 2025). These hidden layers each pass their output on to become the input to the next layer. Each neuron is connected to many other neurons and adjusts as it receives information from the connected neurons. The neural network adjusts computations based on feedback from training data, specifically whether its predictions were wrong or right. In this way, the hidden layers transform the data until it reaches the final layer, the output layer. This layer outputs the results or predictions, and the number of neurons in this layer is equal to the number of possible results (“Layers in Artificial,” 2025). “Neural networks that contain a large number of layers are often referred to as deep neural networks (DNNs).” (Fernandez, 2019).

The many fully connected layers utilized in deep neural networks used today are good at pattern recognition, able to identify patterns and predict the likely outcome. This pattern recognition is a key element in how neural networks are used to create personalization. IBM explains how neural networks and AI personalization work by “collecting customer data about user behavior, preferences and interactions—along with contextual data like location, time of day and device use.” (Hayes & Downing, 2025). Their explanation continues with the following:

This data is then analyzed by AI algorithms, which identify patterns and trends in user behavior. Typically, the AI will also group users into segments based on similar characteristics and behaviors in a process known as audience segmentation. By analyzing these segments and user behaviors, the AI then recommends products, services, or content that align with user preferences and demographics. It can also display specific content on a website or app to different users based on their unique profiles. (Hayes & Downing, 2025).

An article published on BytePlus expands on the benefits of AI personalization: “unlike traditional algorithms that follow rigid, predefined rules, neural networks can adapt and improve their performance through continuous learning.” (K.G., 2025)

Personalization has demonstrated a favorable impact on revenue by increasing consumer satisfaction, which leads to increased engagement. These data-driven AI systems yield a competitive advantage when utilized effectively. (Hayes & Downing, 2025). Nonetheless, the use of neural networks for personalization also presents a range of challenges and raises important ethical considerations. The challenges include the issues with data storage and secure handling associated with big data. It also creates unique privacy considerations, algorithmic bias concerns, transparency, and issues with consent and user autonomy. According to Matthew Kosinski, a great number of the most advanced machine learning models available today are “black box” AI systems, “whose internal workings are a mystery to their users.” (2024). Biases are a concern in machine learning as flawed training data can have an unintentional negative impact on results. The impact of the flawed results can unfairly disadvantage a particular group of people. Kosinski further explains that due to the enormous size of the training data sets and complex deep learning processes used in these models, “even the creators themselves do not understand exactly what happens inside them.” (Kosinski, 2024). The lack of transparency can obscure problems such as vulnerabilities, biases, and privacy violations.

These ethical concerns underscore the importance of regulatory mechanisms like the General Data Protection Regulation (GDPR), which sets explicit boundaries for data collection, data sharing, data use, and limitations. It also sets expectations for protecting privacy and safeguarding data online. The GDPR governs many aspects of the use of personal data, which is utilized in massive amounts in neural network training for personalization. These aspects include transparency, accuracy, confidentiality, accountability, data minimization, storage limitation, and purpose limitation. Following is a table that summarizes how the GDPR regulates these areas specific to AI-generated personalization.

|  |  |  |
| --- | --- | --- |
|  | GDPR Mandates | Applied to AI Personalization |
| Transparency | Article 5 (Principles relating to processing of personal data): Paragraph 1(a) -“Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.” (Art 5 GDPR, n.d.). | Personal data obtained for training the algorithm specific to the user for personalization must be used in a transparent manner. This can be a challenge as deep neural networks often operate in a “black box.” This regulation necessitates that system engineers fully understand how their network is functioning in order to explain it to the users. |
| Accuracy | Article 5 (Principles relating to processing of personal data): Paragraph 1(d) -“Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.” (Art 5 GDPR, n.d.). | Personal data obtained for AI personalization needs to be accurate, and if identified as inaccurate, it needs to be erased without delay. This is an area that requires massive improvement with respect to AI. As stated by Higa, Bedikian, and Costa, “AI often creates outputs based on statistical patterns and relationships learned from training data – if an AI has been trained on an individual’s personal details before a deletion request, it may still infer, predict, or reconstruct similar details when prompted.” (2025). To completely erase bad data, the AI system needs to be completely retrained, which is often time and resource-prohibitive. |
| Confidentiality | Article 5 (Principles relating to processing of personal data): Paragraph 1(f) -“Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.” (Art 5 GDPR, n.d.). | Personal data used for personalization must be processed and stored securely to ensure it remains confidential. Simply removing common identifiers like name, gender, and ID numbers is not enough. AI systems can reconstruct identity from other identifiers, like predicting age range and gender from shopping and content browsing patterns. Data stored for neural network training needs to follow all industry standards to ensure confidentiality. |
| Accountability | Article 5 (Principles relating to processing of personal data): Paragraph 2 - “The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1.” (Art 5 GDPR, n.d.). | Applications using personal data for AI personalization are held to the standards established in the GDPR. The challenges inherent in using big data to train neural networks do not excuse breaches in the law, and companies can be held responsible. |
| Data minimization | Article 5 (Principles relating to processing of personal data): Paragraph 1(c) - “Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.” (Art 5 GDPR, n.d.). | Training the neural network for personalization on each specific user currently entails the use of massive amounts of data, so following this regulation is difficult in AI. According to TechGDPR, techniques for reducing the need for training data include: generative adversarial networks, federated learning, and matrix capsules. (Ved, 2019). |
| Purpose Limitation | Paragraph 1(b) - “Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with [Article 89](https://gdpr-info.eu/art-89-gdpr/)(1), not be considered to be incompatible with the initial purposes.” (Art 5 GDPR, n.d.). | Data obtained for use in personalization by the AI system can not be used for other purposes or processes in a way that is not congruent with the initial purpose. |
| Storage Limitation | Article 5 (Principles relating to processing of personal data): Paragraph 1(e) - “Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with [Article 89(](https://gdpr-info.eu/art-89-gdpr/)1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject.” (Art 5 GDPR, n.d.). | Personal data, such as the data obtained for AI personalization, can only be retained as long as it is needed for processing unless archived for specific purposes. This poses a challenge for AI since it is difficult to eliminate data from trained neural networks, as previously explained. |

The GDPR is affecting our company’s practices by regulating how and when personal data can be collected and stored. Specific legal concerns for our use of neural networks to personalize the user experience are fair and transparent AI, maintaining privacy for users, and data security and storage. “This standard of accountability that companies must achieve will increase the standard of AI neural networks and force all of us to use an AI we can understand and control.” (Hanania, 2018). Following the principles laid out in the GDPR will ensure high integrity training data, as well as build consumer trust, while providing consumers with the personalized experience they expect. These expectations are documented in an article by Hayes and Downie, “according to the consultancy McKinsey, 71% of consumers expect companies to deliver personalized content. 67% of those customers say they are frustrated when their interactions with businesses aren’t tailored to their needs.” (2025). These expectations, combined with the nature of social networking applications and our chosen method of monetization, require that we continue to utilize AI-powered personalization. However, meeting both consumer expectations for personalized experiences and the strict data handling requirements of the GDPR requires a proactive and deliberate strategy.

The strategy recommended for our company to successfully adapt to regulations set by the GDPR while still exceeding customer expectations is to shift our model to a combination of federated learning and differential privacy. “Federated learning is a machine learning paradigm that allows a model to be trained across decentralized devices or servers holding local data samples without exchanging them.” (Vaj, 2023). By not collecting personal data and leaving it on the user’s device, when possible, we greatly reduce the risk of noncompliance for the company. Differential privacy adds noise to individual data sets to mask the real data. This can be used to obscure any data obtained by the company. Shifting to a federated learning model and using differential privacy must be combined with utilizing industry best standards for data security, like firewalls and homomorphic encryption, which allows for data to be processed while encrypted. With the personal data collection reduced as much as possible and these measures in place, we can be confident in our adherence to the GDPR.

Fair, unbiased algorithms are necessitated by the GDPR, to ensure our application is providing appropriate results and not trained with flawed data, bias audits should be completed frequently. There are several tools for bias audits, many of which are open-sourced. The development team should research which tool is best to meet our needs, then implement routine auditing with adjustments made when needed. Explanations of how our algorithm functions, bias audit results, and remediation efforts should be made publicly available. Different perspectives can provide new ideas for improvement, enhancing our system as feedback dictates. This strategy will build trust with our consumers and will comply with GDPR.

References

*Art. 5 GDPR – principles relating to processing of personal data*. General Data Protection Regulation (GDPR). (n.d.). <https://gdpr-info.eu/art-5-gdpr/>

Fernandez, E. (2019, November 30). *AI is not similar to human intelligence. thinking so could be dangerous*. Forbes. <https://www.forbes.com/sites/fernandezelizabeth/2019/11/30/ai-is-not-similar-to-human-intelligence-thinking-so-could-be-dangerous/#3fbd0b846c22>

GeeksforGeeks. (2025, July 23). *Layers in artificial neural networks (ANN)*. GeeksforGeeks. <https://www.geeksforgeeks.org/deep-learning/layers-in-artificial-neural-networks-ann/>

Gulli, A., & Pal, S. (2017). *Deep learning with keras: Implementing deep learning models and neural networks with the power of python*. Packt Publishing, Limited.

Hanania, P.-A. (2018, November 30). *AI and the Janus face of the GDPR – chance or challenge?*. Capgemini. https://www.capgemini.com/pt-en/2020/01/ai-and-the-janus-face-of-the-gdpr-chance-or-challenge/

Hayes, M., & Downie, A. (2025, May 29). *AI personalization*. IBM. <https://www.ibm.com/think/topics/ai-personalization>

Higa, H., Bedikian, S., & Costa, L. (2025, May 20). *The right to be forgotten is dead: Data lives forever in AI*. Tech Policy Press. <https://www.techpolicy.press/the-right-to-be-forgotten-is-dead-data-lives-forever-in-ai/>

Intersoft Consulting. (n.d.). *Artificial Intelligence Act: AI Act*. AI Act. https://ai-act-law.eu/

K, G. (2025, April 24). *Neural networks for personalization in e-commerce*. BytePlus. <https://www.byteplus.com/en/topic/392903?title=neural-networks-for-personalization-in-e-commerce>

Kosinski, M. (2024, October 29). *What is black box AI and how does it work?*. IBM. <https://www.ibm.com/think/topics/black-box-ai>

Vaj, T. (2023, December 14). *The difference between differential privacy and Federated Learning*. Medium. <https://vtiya.medium.com/the-difference-between-differential-privacy-and-federated-learning-6cbe19333c09>

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/>