Project 1

Jermaine Wiggins

Southern New Hampshire University

CS-370: Current and Emerging Trends in Computer Science

Professor Divya Vellanki

Sep 28, 2025

**Project 1**

**Neural networks**

Neural networks are computer systems designed to identify patterns, modeled after the structure and functioning of the human brain (Khan Academy). A helpful way to understand how they work is by looking at the structure of a single biological neuron. In the brain, neurons have dendrites that receive input, a soma that processes that information, and an axon that sends out a signal if certain conditions are met (Khan Academy). Artificial neural networks follow a very similar structure. The input layer takes in data, the hidden layers analyze and transform it using mathematical functions, and the output layer generates the results (Gulli & Pal).

Just like networks of biological neurons, artificial neural networks are made up of many connected units that pass information along. The input layer provides the raw data, the hidden layers transform it by identifying patterns and important features, and the output layer makes a classification or decision. For example, when recognizing a handwritten number, the hidden layers might first detect simple features like lines or curves, then combine them into shapes like loops or angles, and finally decide whether the number is a 3, 7, or 9. In this way, the similarities to biological neurons help make sense of how artificial networks receive input, process it, and produce output.

Evaluate how neural networks are used to create personalization

To provide a unique experience for each user, neural networks track and analyze a wide range of user interactions, including which pages are visited, links selected, time spent on content, mouse activity, and location, allowing the system to tailor recommendations and content to individual behavior.

After this data is received by the input layer it is then processed by hidden layers too identify patterns and other relevant information. Then the output layer then generates recommendations for friend request, discussions, games and ads the user may be interested in. Then As the user continues to use the application, neural networks learn from their feedback and improve their predictions, making the experience more personalized and keeping the user engaged with content and advertisements.

In this scenario where user data goes in as input and a recommendation is returned as output the internal process that determines the outcomes aren’t so easily explained and this is where the issues arise. Not knowing what causes certain outcomes makes it difficult to give users transparency on how each individual data collected is being used and the purpose of collecting each item (Kosinski, 2025). It also makes it difficult for the user to fully understand why certain things are being recommended to them. In addition to these hidden biases can also arise, if the training data reflects social stereotypes the system may output these outcomes, such as recommending products or groups based on demographic or location (Kosinski, 2025).

**GDPR affects personalization**

General data protection (GDPR) is set of rules outlining how a company can collect store and use personal data (Kosinski, 2025). The GDPR affects personalization through principles like transparency, purpose limitation, data minimization, and storage limitation. Transparency means users must know that their clicks, browsing, and location data are tracked to provide recommendations (Information Commissioner’s Office, n.d.). Purpose limitation ensures this data is only used to personalize content, not for unrelated purposes (Information Commissioner’s Office, n.d.). Data minimization requires collecting only the necessary information, such as page views needed for recommending posts (Information Commissioner’s Office, n.d.). Storage limitation mandates deleting or anonymizing data once it is no longer needed to improve recommendations (Information Commissioner’s Office, n.d.).

**GDPR affects** company practices

Using neural networks to personalize the user experience can raise several legal concerns under regulations like the GDPR. These systems often function as black boxes, meaning that while we can observe the data going in and the recommendations coming out, the internal decision-making process is not easily understood (Kosinski, 2025). This lack of transparency makes it difficult to explain to users how their data is processed and why certain recommendations or ads are shown. It also raises questions about whether the company is collecting more data than necessary or using it for purposes beyond personalization, which could violate data minimization and purpose limitation rules. Storing behavioral data indefinitely to improve personalization may breach storage limitation requirements. Additionally, biased training data can result in discriminatory outcomes, creating further legal risks.

Given these risks, it is crucial that they are taken seriously and properly managed, because this personalized experience is not possible without this data. If these specific inputs were removed the neural networks would be unable to make accurate recommendations, maintain engagement, or deliver relevant ads, which are essential for both user satisfaction and the company’s business model.

**Adaptions to company’s practices**

As of today, current best practices in artificial intelligence (AI) and machine learning (ML) focus on protecting user privacy and complying with regulations like the GDPR. Popular design strategies include Privacy by Design, which builds privacy protections into systems from the start, and differential privacy, which adds small changes to the collected data so users cannot be easily identified (Richter, 2025). Federated learning allows models to train on local data without sending it to a central server, while data minimization and purpose limitation ensure that only necessary data is collected and used for its intended purpose (Richter, 2025). Other practices like anonymization and pseudonymization, transparency and explainability, and regular audits or Data Protection Impact Assessments (DPIAs) help maintain privacy, reduce bias, and foster user trust (Richter, 2025).

To implement current trends and comply with GDPR, the company make some minor adjustment to its business model. Starting with transparency, the company can provide clear privacy notices or pop-ups in the app that explain how clicks, page visits, and time spent on content are used to suggest posts or ads. This is especially important because neural networks often function as black boxes. To improve data collection the company can follow data minimization and purpose limitation by collecting only the information needed for personalization and avoiding unrelated data collection. For example, if the social network collects exact location when general location gives the same recommendations then this can be omitted. In addition, storage limits can be maintained by regularly deleting or anonymizing old behavioral data, so it can still be used for trend analysis without identifying individual users. Finally, privacy-preserving techniques such as differential privacy, which adds small random changes to data, or federated learning, which trains models directly on users’ devices, can protect sensitive information while still allowing AI systems to learn patterns.

**References**

Khan Academy. (n.d.). *Overview of neuron structure and function.* https://www.khanacademy.org/science/biology/human-biology/neuron-nervous-system/a/overview-of-neuron-structure-and-function

Gulli, A., & Pal, S. (n.d.). Home -ProQuest Ebook Central - Libguides at ProQuest. <https://proquest.libguides.com/ebookcentral>

Kosinski, M. (2025, June 2). *What is black box AI and how does it work?*. IBM. https://www.ibm.com/think/topics/black-box-ai?utm\_source=chatgpt.com

Information Commissioner’s Office. (n.d.). *A guide to the data protection principles.* https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

Richter, A. (2025, June 25). *Privacy by design and AI.* TechGDPR. https://techgdpr.com/blog/how-to-build-trustworthy-ai-from-the-ground-up-with-privacy-by-design/