Alfredo Romero

CS 370 Current/Emerging Trends

SNHU

09/24/2023

4-2 Project One Submission

1. **Explain the basics of neural networks and how they work** by addressing the following:

a. Provide a brief explanation of how neural networks work. How do the input layer, hidden layer, and output layer interact to classify objects? Consider the fact that your target audience may have limited technical knowledge.

During the second decade of the 21st century, there a many cool social networking companies that uses fancy neural networks to make the platform super personalized for us the consumer, like when you get awesome recommendations for friends, posts, articles, and ads, and it feels like the app really gets you. But here's the twist: some of these applications might be breaking the law, or violating some aspects of the GDPR(General Data Protection Regulation) law. This is why I will discuss the principles of transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability when obtaining using specific algorithm to capture user’s information. I will propose remedies and defend existing practices where applicable, keeping in mind the delicate balance between personalization and GDPR compliance.

Before delving into GDPR compliance, it is essential to understand the basics of how neural networks work. Neural networks are computational models inspired by the human brain. They

consist of layers of interconnected nodes or artificial neurons. In the context of our personalization algorithms:

1. **Input Layer**: This layer receives data from the user, such as mouse clicks, navigation, and other interactions within the app.
2. **Hidden Layers**: These intermediate layers process the input data through a series of weighted connections and activation functions. They extract patterns and features from the input.
3. **Output Layer**: The output layer generates predictions or recommendations based on the patterns learned in the hidden layers. In our case, it could be recommendations for posts, friends, articles, or other site features.

Having a clear idea of how a neural networks works, we can understand that the interactions between these layers enable the neural network to classify and predict objects or outcomes, such as personalized content recommendations. In conclusion, the company's personalization algorithms, driven by neural networks, can align with GDPR principles while delivering valuable user experiences and targeted advertising. Recommendations include improving transparency, data minimization, data accuracy, data retention policies, and data security.

2. Evaluate how neural networks are used to create personalization by addressing the following:

a. How are neural networks utilized to aid in the personalization of the user experience?

b. What ethical concerns can this raise? Consider hidden biases that may arise in using a “black box” classification system, where the algorithms are unknown to the user.

Okay, imagine you're using a social media app, and it seems to magically know what you want to see – your friends' posts, articles, and even ads that are just right for you. That's the power of neural networks! The first step is that the app collects data about what you do on the platform, like what you click on, what pages you visit, and how long you stay on them. This data is like puzzle pieces. Then, neural networks come into play. They're like super smart detectives that learn patterns from all those puzzle pieces. They figure out your interests and habits, like what topics you're into or who you might want to connect with. Once these neural networks understand you, they start making recommendations. For example, they suggest friends, posts, articles, and ads that match your interests based on your past actions and what people similar to you have liked. this process never stops! Neural networks keep learning from your actions, making recommendations even better over time. It's like having a personal assistant for your online experience.

But, using these neural networks isn't all sunshine and rainbows. There are some **Ethical Concerns and Hidden Biases** we need to be aware of. First, neural networks learn from historical data, which can sometimes have unfair biases. These biases might be related to gender, race, or other factors. If the network learns from biased data, it can make biased recommendations, like showing you content that only matches certain demographics. Second, neural networks can be like black boxes, they work, but we don't always know how. This can be a problem because users might not understand why they're seeing certain things, which can lead to frustration and mistrust. Sometimes, these networks create filter bubbles. That means you see only stuff that matches your existing beliefs and interests. While it keeps you engaged, it can also limit your exposure to different perspectives. Third, Collecting lots of data for personalization

can make people worry about their privacy. Users might not know exactly what data is being collected or how it's being used, which can be a problem. And last, there can also be legal problems, like violating data protection laws if data isn't handled properly or if users' rights aren't respected.

Therefore, to ensure ethical use of neural networks for personalization, we can take several actions. Firstly, transparency is crucial, requiring clear communication about data collection and usage, with the help of explainable AI techniques. Secondly, we should actively address biases in algorithms to ensure fair recommendations for everyone. Providing users with control over their personalization settings is essential. Third-party audits can offer an independent check on ethical practices. Lastly, strict adherence to data and privacy laws is necessary. In essence, balancing personalization with ethical considerations is vital for fostering a fair and inclusive online environment.

3. **Analyze how portions of the GDPR affect personalization** by addressing the following:

a. Summarize the portions of the GDPR that affect personalization. Be sure to consider *at least four* of the following in your answer: transparency, purpose limitation, data minimization, accuracy, storage limitation, confidentiality, and accountability.

GDPR's emphasis on transparency, purpose limitation, data minimization, and accountability significantly affect how personalization is conducted. These regulations promote responsible data handling and protection while maintaining the goal of providing tailored user experiences within legal and ethical boundaries. Let’s get into details:

Transparency: GDPR emphasizes transparency, which means companies must be clear about how they collect and use user data. For personalization, this means we need to be open with users about what data we're gathering, why we're collecting it, and how it will be used. This is important to build trust and ensure users understand the personalization process.

Purpose Limitation: GDPR restricts the use of data to specific, predefined purposes. In the context of personalization, this means that the data we collect should only be used for enhancing the user experience, such as recommending relevant content or connections. We cannot use the data for unrelated purposes, ensuring that personalization remains user-centric.

Data Minimization: GDPR encourages the principle of data minimization, which means we should only collect the data necessary for the specified purposes. In personalization, this ensures that we don't gather excessive or irrelevant user data, respecting user privacy.

Accountability: GDPR holds companies accountable for following its principles. This means that we need to establish clear internal processes, designate a Data Protection Officer, and regularly audit and assess our GDPR compliance. For personalization, accountability ensures that we are responsible for protecting user data and adhering to GDPR guidelines.

4. **Assess how the GDPR is affecting the company's practices** by addressing the following:

a. What specific legal concerns may arise from your company's use of neural networks as a classifier to personalize the user experience?

b. Is not collecting data a possibility for the company's business model? Defend your answer.

The use of neural networks for personalization in our company's practices raises several legal concerns in the context of GDPR compliance, One of them been **Data Processing and**

Consent which requires explicit user consent for data processing. The complexity of neural networks as classifiers may make it challenging to clearly explain how user data is used to achieve personalization. This can raise concerns about obtaining valid consent. Another concern is that GDPR mandates data minimization, collecting only what is necessary for the specified purposes. Neural networks often process large volumes of data, potentially exceeding what is strictly required for personalization. This could pose issues related to data minimization. Another concern is the Transparency is a key GDPR principle. If the functioning of neural networks is perceived as a "black box" to users, it may be difficult to provide the required level of transparency about data processing, potentially violating this principle. And last, If neural networks inadvertently learn and perpetuate biases present in training data, it can lead to discriminatory recommendations, which may not comply with GDPR's non-discrimination principles.

While not collecting any data is not a practical option for our company's business model, some degree of data minimization and privacy-enhancing practices can be implemented. This approach aligns with GDPR requirements and ethical consideration. the company can focus on collecting only necessary data, obtaining clear user consent, implementing robust data protection measures, and regularly auditing data handling processes to strike a balance between personalization and GDPR compliance. This approach ensures that user experiences remain personalized while respecting legal and ethical boundaries regarding data privacy and protection.

5. **Propose adaptations to the company’s practices to act in compliance with the GDPR** by addressing the following:

a. What are the current trends (best practices) in artificial intelligence and machine learning aimed at preserving privacy?

b. What changes to the way the company collects, stores, and employs user data do you propose to comply with GDPR? Defend existing practices where applicable.

Current trends in artificial intelligence (AI) and machine learning (ML) focus on preserving privacy while maintaining effective personalization. Differential privacy techniques add noise to data to protect individual privacy while still allowing useful insights to be extracted. Implementing this can help the company ensure user data remains confidential. Federated learning enables model training on decentralized data sources without exchanging raw data. This approach can enhance privacy by keeping user data on their devices while still benefiting from personalization. Homomorphic encryption allows computations on encrypted data without decrypting it. This can be utilized to protect sensitive user data during processing. Researchers are developing models that can provide personalized recommendations without the need to access individual user data directly. Techniques like collaborative filtering and secure multi-party computation are gaining traction.

Proposed changes to the way the company collects, stores, and employs user data to comply with GDPR include enhancing transparency by making privacy policies more accessible and understandable. Clearly explain what data is collected, how it's used, and offer users granular choices on data processing. Evaluate data collection practices and implement strict data minimization policies. Only collect data necessary for personalization, avoiding excess information. Enhance the consent mechanism to ensure explicit, informed user consent for data

processing. Users should have the ability to opt in or out of data collection and personalization. Strengthen data security measures, including encryption and access controls, to safeguard user data from breaches. Explore techniques for data anonymization to reduce the risk of personally identifiable information being exposed. Establish a regular audit process to monitor compliance with GDPR principles and promptly rectify any identified issues. Integrate privacy considerations into the development process of personalization algorithms and ensure they adhere to GDPR principles from the outset. Educate employees on GDPR compliance and privacy best practices to create a culture of data protection. In cases where existing practices align with GDPR principles, these practices should be defended and maintained while continuously striving to improve privacy measures and user consent processes.

In conclusion, neural networks are like virtual brains that help computers make decisions. They have input, hidden, and output layers that work together to figure out what something is. Think of it as learning from examples, like recognizing cats in photos. Neural networks personalize our experience, but they can hide unfair biases. We need to be careful and open about how they work to make things fair for everyone. GDPR rules affect personalization by requiring clear rules about data, like being clear about what we collect and not using data for unrelated stuff. We need to be accountable for this. GDPR might worry about how we use neural networks, but not collecting data isn't an option because personalization needs some data. We need to do it right and be transparent. To follow GDPR, we should use privacy-friendly AI trends like adding noise to data or keeping data on devices. We should also improve consent, data security, and minimize what we collect. Some existing practices are good and can be kept, but we need to keep improving.

Source

- Spillane, J. (2022, December 8). How GDPR Can Undermine Personalization and User Experience. Crypto Expert.
- Ved, A. (2019, February 28). How to Develop Artificial Intelligence that is GDPR-friendly. Privacy by Design.
- Dorschel, A. (2019, April 24). Rethinking Data Privacy: The Impact of Machine Learning. Luminovo.