Steven Foltz

1/27/2026

CS 370 Project One

In response to an EU regulator's worries about our neural network-driven personalization systems' compliance with the General Data Protection Regulation (GDPR), this white paper was written. As the main engineer, I am aware that our advanced AI models—which are essential to our user experience and business strategy—operate in a setting that requires both strict ethical and legal stewardship and technical brilliance. Our objective is to set a new benchmark for ethical innovation rather than just avoiding fines. In order to do this, this article will offer a clear description of our technology, an honest assessment of its ethical ramifications, a thorough examination of the pertinent GDPR principles, and a series of practical, forward-looking suggestions intended to fully comply with our practices.

It's critical to comprehend the underlying technologies in order to contextualize our compliance journey. A neural network is a type of artificial intelligence that is loosely based on the neural network of the human brain. Its main purpose is to identify intricate patterns in large datasets. The system is organized in layers at a high level. Every click, view, timestamp, and interaction from a user's session are sent to the input layer as raw data points. The actual "learning" takes place after these signals are processed through one or more hidden levels.

Each layer eventually builds from basic associations to more abstract representations of user desire and behavior by assigning weights of importance to various data combinations. Ultimately, the output layer presents a choice: a suggested buddy, a recommended post, or a tailored advertisement. In order to forecast what will optimize user involvement, this system continuously improves its internal model by iterative training on large datasets rather than explicit programming (Goodfellow, Bengio, & Courville, 2016). It is most useful to consider it as a dynamic, self-optimizing filter that shapes each user's own digital environment for our colleagues in legal and other non-technical departments.

The personalization of our platform is powered by these neural networks. They develop predictive models that anticipate personal wants and interests by examining the entire fabric of user activity. Relevant content boosts engagement, which in turn generates more data to improve the model, creating a potent positive feedback loop. This cycle is essential to both our monetization through greater ad targeting and user delight. But this very capability raises serious ethical issues, mostly related to the "black box" issue.

Even its engineers are frequently unable to understand the complex, multi-layered decision-making process of an advanced neural network. This lack of explainability can significantly affect user autonomy and conceal and reinforce hidden biases in the training data, such as unintentionally directing particular demographics toward alternative opportunities or information. According to Mittelstadt, Allo, Taddeo, Wachter, and Floridi (2016), fundamental concepts of openness and fairness are challenged when users are directed into customized "filter bubbles" by a technology they are unable to understand. The first step toward moral and law-abiding AI is acknowledging this.

Our present data practices are directly challenged by the principles established by the GDPR. Four stand out in particular. First, in order to be transparent, we must explain data processing in a way that is understandable, clear, and accessible. Users are unable to understand how their data affects their experience, therefore our present dependence on legalese-filled privacy regulations fails this test. Second, Goals Limitation requires that data be gathered only for clear, precise, and acceptable objectives. Our general defense of "service improvement and personalization" is perhaps too nebulous to meet regulatory requirements.

Third, Data Minimization forces us to gather just information that is sufficient, pertinent, and absolutely required for our declared goals. This fundamental principle is seriously violated by our default stance of gathering all potential interaction, from mouse hovers to scroll velocity. Lastly, personal information must not be retained in an identifiable form for longer than is necessary due to storage limitations. This approach is directly at odds with our indefinite preservation of raw behavioral data for model training.

These possible infractions result in actual legal and financial dangers, such as the possibility of hefty fines and required operational adjustments. Because it is challenging to prove compliance when the decision-making process is not completely interpretable, the opacity of our neural networks makes it more difficult for us to uphold the Accountability principle. Furthermore, we do not currently offer the increased level of precision and clarity needed to gain valid user consent for such complicated processing. Whether we can just cease gathering data is a crucial topic.

The answer is no; our value offer is inherently personalized. The best course of action is not to stop, but to change our policies such that they are legal, equitable, and transparent while still utilizing AI's capabilities.

AI is already moving in the direction of Privacy-By-Design. Federated Learning, which enables model training across devices without centralizing raw user data; Differential Privacy, which protects individual identities in datasets by adding mathematical noise; and Explainable AI (XAI), which seeks to improve the interpretability of algorithmic decisions, are examples of promising trends (Yang et al., 2019). These perspectives need to be integrated.

We suggest three modifications. First, we need to change the way we acquire and minimize data. We need to stop collecting non-essential meta-behaviors and instead use a granular, purpose-specific consent model. Second, we must create an interactive "Privacy Center" in order to transform transparency and user control. This dashboard would enable users to monitor and modify their inferred preference profiles, give clear toggles for various processing tasks, and explain personalization in simple terms. Third, we need to impose stringent storage restrictions, anonymize raw activity logs after a brief retention period, and base long-term models on generated preference vectors rather than permanent behavioral data.

We can also firmly defend several current practices in this reshaping. In order to execute our service contract, we have a legitimate interest in using data for security, fraud prevention, and platform integrity. In a similar vein, the use of fully anonymized and aggregated data for research and system-wide optimization is not covered by GDPR and is still an essential and justifiable part of our engineering practice.

In line with ethical innovation, achieving GDPR compliance is a strategic necessity. We can reduce substantial legal risk and foster stronger, more reliable connections with our users by proactively resolving the "black box" conundrum, adopting data minimization, and giving users true transparency and control. It will take a coordinated, cross-functional effort to complete this quest. To put these suggestions into practice and establish our business as a pioneer in ethical AI-driven personalization, I urge the prompt creation of a special task force that brings together engineering, legal, product, and ethics.

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT press.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2).

Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology (TIST), 10(2), 1-19.