CS 370 Project One

GDPR Compliance White Paper

By Alex Frankel

Social networks are an integral part of the human experience in the digital world today. It is important to understand that most of the information about you on the web has been collected voluntarily. For example, your Facebook profile only knows your name, birthday, and interests because you personally provided them. This is useful for the platform in several ways, allowing yourself and others to interact with your digital self. That should not be done without discretion, however! The user should ideally be in control of the depth of which they want to interact with these systems. Collecting one’s information involuntarily or unknowingly is unethical. I will address the possibilities of a transparent and accountable future for your online presence.

Let us begin to understand the technology behind all of this- Machine Learning in its many forms is being used to custom tailor one’s online experience. Neural Networks are great at learning how to classify objects such as images of people, vehicles, symbols, or pretty much anything else. They mimic the structure of the human brain in an effort to learn similarly to the way we do. Raw training data enters a neural network through an input layer at first. This data could be images that are going to be classified. Neural Networks can be configured at practically any size with a number of intermediary ‘hidden layers’. Each hidden layer may “recognize more specific features layer by layer” (Coursera, 2024). Say we are trying to learn how to perceive a human face. The first hidden layer may detect the eyes, and the next one the ears, and so on. The more hidden layers there are, the ‘deeper’ the system becomes. “Each hidden layer can look at a different aspect of the input”. The more complex the task, the more important these multiple layers become.

All this aside, let’s talk about how these systems affect you. There exist content algorithms that create a feed with posts that you are more likely to appreciate. This algorithm is fine-tuned with your data. This data may be the links you click, posts you interact with, pages you like, and other preferences that you have at some time defined. Neural Networks can be trained on your preferences in this way, to fetch content that you are more likely to interact with on some level. This may be great when it comes to personal enrichment or enjoyment, but in many ways the consequence is a monetary incentive and turning you into a product for advertisers. On top of all of this, it is impossible to understand a neural network in its entirety. Much of its operation is a ‘black box’ which means that when data goes in… all we get is what comes out. We don’t know just how much of our data is being used or how it is being used at all at this point.

Luckily for us, the GDPR provides several principles that can guide the process as to how data is obtained and used. The current method our company employs is to track and store all user data as well as all user interactions on the platform and feeding it into one or many different AI models. This practice will be affected by a number of aspects of the GDPR.

The first and arguably most important rule is Transparency.

“It should be transparent to individuals that personal data concerning them are collected, used, consulted, or otherwise processed and to what extent the personal data are or will be processed,” (Data Protection Commission, 2024).

Users need to give consent for any usage of their information under the act. If the company can outline every single data collection technique as well as their rationality for using them then they can be considered transparent. The use of AI models, especially ‘black-box’ models that are difficult to explain to users in detail, “fail to comply with the GDPR requirements of transparency, accountability, and putting the data subject in control,” (Ved, 2024).

Purpose Limitation is the idea that data may be gathered for “pre-specified purposes”.

“Specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data,” (Data Protection Commission, 2024).

This is in line with transparency- the service provided is a custom-tailored social media profile. However, the network needs to save user preferences and data to continue providing relevant posts and targeted advertising. This tenet specifies that data cannot be used for any other purpose than that which has been specified. This may be difficult to achieve if the network, and thus their advertisers, is constantly changing. If their data is being fed into new AI networks, is that a deviation from this rule? I believe that as long as the consumer agrees to and understands its terms of use, this may be possible to uphold even if the platform is updated. An example of this would be that a company cannot sell user data that was collected at a previous time where they did not give consent. This is a serious matter and should be discussed with legal counsel in order to further understand this rule.

Data Minimization builds upon purpose limitation in the respect that erroneous data cannot be collected for any reason that hasn’t been specified by the platform.

“Processing of personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed,” (Data Protection Commission, 2024).

This is important when being transparent to users of our network. A good example of this is that the company may record clicks and interactions with content within reason… perhaps they shouldn’t use a keylogger, however.

Accountability is the last tenet I will be exploring.

“The controller is responsible for, and must be able to demonstrate, their compliance with all of the above-named Principles of Data Protection,” (Data Protection Commission, 2024).

The idea is that we are being held accountable for all of the previously mentioned reasons. If we can adapt to protect the use of our users’ data, we will not be in violation of their rights.

The GDPR drastically affects the way that our company currently operates. The methods in which we collect data are not transparent. The reason we are collecting data is unclear to the user. Finally, there is no limitation on the data we are collecting. Despair not, because we can change our practices to better our ethics and the services we provide! It is possible that we can halt data collection if so desired. For example, a user may opt out of algorithmically driven content. They can specify preferences independent of their personal data or limit their feed’s personalization. Advertisements will not be personalized, but they can still be shown. This does not break the social media experience! I believe that the company’s business model is still viable under the act.

There are a number of things our company can do to keep up with the times. The most important idea here is to give our users a choice. If we allow them to consciously decide which data we can collect from them, we are upholding transparency. If they don’t want us to, we will not do it. It’s that simple! Some people like the idea of their compiled interests serving them content, and others don’t. This is ok! There is a middle ground within this issue, and that is allowing a user to decide exactly how much of their data *they* want to be collected. If they decide they want their data tracked, we can use it responsibly. Rather than selling their data to advertisers, we can serve ads internally and without violating purpose limitation if we act as an intermediary in the process. If the information is self-contained, this upholds our confidentiality and purpose limitation. Basically, don’t sell a user’s info without their consent! Machine learning models can become biased and profile people. A good way to uphold transparency has been theorized: “investing in scientific research on explainable artificial intelligence,” (Ved, 2024) is a great idea! This involves “ensuring individuals are informed appropriately when they are interacting with AI and provide adequate information on the purpose and effects of AI systems,” (Ved, 2024). We can demonstrate that we are contributing to a well-informed public by shedding light on our systems and how they work. Power to the people!

As we move forward, complying with international confidentiality standards can be revitalizing for our company image. At its worst, it is an expensive mistake: a mistake that can and should be avoided, but one that we learn from, nonetheless.

Works cited:

What is a hidden layer in a neural network?. Coursera. (2024, April 10). <https://www.coursera.org/articles/hidden-layer-neural-network>

Principles of Data Protection: Data Protection Commission. Principles of Data Protection | Data Protection Commission. (n.d.). <https://www.dataprotection.ie/en/organisations/data-protection-basics/principles-data-protection>

Ved, A. (2024, February 22). How to develop artificial intelligence that is GDPR-friendly. TechGDPR. https://techgdpr.com/blog/develop-artificial-intelligence-ai-gdpr-friendly/