**Overview**

This assignment will help you get hands-on experience training convolutional neural networks in Keras and using them to make predictions. This will deepen your understanding of neural networks. You will then gain practice considering the ethical and legal implications of this type of technology. This will support your work in Project One, which is due in the next module.

**Prompt**

Access the Virtual Lab (Apporto) by using the link in the Virtual Lab Access module. It is recommended that you use the Chrome browser to access the Virtual Lab. If prompted to allow the Virtual Lab access to your clipboard, click “Yes”, as this will allow you to copy text from your desktop into applications in the Virtual Lab environment.

1. Once in the Apporto environment, create a new Jupyter Notebook and configure it using the following naming convention:

<YourLastName>\_<YourFirstName>\_Assignment3.ipynb

Thus, if your name is Jane Doe, please name the submission file “Doe\_Jane\_Assignment3.ipynb”.

For information on how to navigate the Jupyter environment, review the Jupyter Notebook in Apporto (Virtual Lab) Tutorial.

1. Read through the “Recognizing CIFAR-10 images with deep learning” example on pages 84–94 of Deep Learning with Keras. Copy the code into your Jupyter Notebook, including the code for a deeper network and data augmentation in your model. Run the code to build a convolutional neural network model that includes a deeper network and data augmentation.

Note: More information about the training and test data sets can be found in the CIFAR-10 and CIFAR-100 Datasets repository.

1. The algorithm you worked to train can be used to distinguish more realistic images than the hand-written digits example from the previous module. While distinguishing between animals or vehicles may not pose a serious ethical dilemma, it’s important to consider what other types of images an algorithm such as this could be trained on. For example, could such an algorithm eventually be used to distinguish people’s faces? If so, what are the ethical and privacy implications? Create a Markdown cell in your Jupyter Notebook after your code and its outputs. In this cell, analyze the ethical and privacy implications of the algorithm you just created. You are expected to include resources to support your answers, and must include citations for those resources.

Specifically, you must address the following rubric criteria:

* Configure the Jupyter Notebook correctly and use the proper naming convention.
* Build a convolutional neural network model using a deeper network and data augmentation for CIFAR-10 image data.
* Explain how this algorithm could result in ethical and privacy concerns if it were trained on different sets of images.

**What to Submit**

Please submit your completed IPYNB file. Make sure that your file is named as specified above, and that you have addressed all rubric criteria in your response.

The algorithm would make it possible to distinguish people’s faces. However, there are various ethical and privacy complications regarding cell phones, law enforcement, and deepfakes. According to OLOID, “If unchecked, face-based recognition technology can lead to surveillance states where individual freedoms are compromised.” (Oloid Desk, 2023, para 5). With the advancement of technology today, unauthorized users can unlock a victim’s smartphone to obtain sensitive information and extort personal and financial data. Another issue faced with ethical and privacy concerns would be law enforcement and identifying suspects. Hill argues, “Clearview’s app carries extra risks because law enforcement agencies are uploading sensitive photos to the servers of a company whose ability to protect its data is untested.” (Hill, 2021, para 12). When using Clearview, a recently discovered facial recognition company, law enforcement uploads sensitive data of potential interests that unknowingly encourage discriminatory profiling or targeting specific groups. Furthermore, with the rise of AI technology, deepfakes have become a rising concern due to their fabrication when digitally altering an appearance to be someone else. Thousands of deepfakes have surfaced on social media platforms, and deepfakes create fake photos and videos of an individual that may harm one’s reputation and personal life. If not addressed, ethical and privacy concerns with facial recognition and cell phones, law enforcement, and deepfakes can lead to a world without that will know everything and everyone within minutes.

**References**

Hill, K. (2021, November 2). The secretive company that might end privacy as we know it. *The New York Times*. <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>

Oloid Desk. (2023, October 2). *The ethics of face-based recognition: Privacy, bias and regulation*. OLOID. <https://www.oloid.ai/blog/ethics-of-facial-recognition/#:~:text=One%20of%20the%20primary%20ethical,without%20explicit%20consent%20from%20individuals>.