Data Privacy with Images

The growth of social media has heralded an era of online data sharing, wherein the majority of daily interactions are conducted between technological intermediaries. While this provides huge benefits in terms of productivity, communication, and accessibility, it also presents important privacy challenges.

A Brief History of Data Privacy

Since the human rights movement following the events of World War II, strict ethical requirements were developed which must be adhered to by social scientists and medical practitioners when performing experiments on humans. The prime example of these is the Belmont Report, created in 1978. This is true regardless of their impact, be it physical, psychological, or emotional. Although data science and machine learning practitioners do not directly experiment with human subjects, their impact can be commensurate with those of the social science community. Every time an e-commerce site changes the layout of their site using an A/B test, they are conducting a large-scale social experiment.

One of the key concerns of such requirements is the right to individual privacy. The breadth of data that can be obtained about human subjects can be highly valuable to businesses as well as the research community, but requires informed consent of the individual to be used. Today, companies like Google and Facebook have huge amounts of data based on the way users interact with their services. This information is often then marketed to companies and

subsequently used for targeted advertising campaigns. The right of the company to use this information is embedded within their terms of use for their respective services. Whilst these uses might seem unethical, especially to privacy advocates, they are entirely legal and abide by the ethical conventions of Belmont Report, as well as more modern ethical requirements developed during the age of big data, such as the Menlo Report.

However, the principle of informed consent has become increasingly difficult to ensure in the modern world. A good example is genetic information. By uploading genetic information to online platforms such as 23AndMe, an individual is voluntarily waiving their right to privacy. However, genetic information is largely similar between family members, and thus by uploading this information, the privacy of relatives is also violated. A famous example of this was the arrest of the “Golden State Killer”, who went uncaught for decades until DNA information from an online genetic database was linked to a relative of the murderer using DNA from the crime scene. Although this demonstrates a positive use of such data, its potential power is unsettling.

Data Privacy in Images

Image data is one of the most vulnerable mediums of online data. This is troubling as it is also one of the most commonly shared. Datasets may contain images of people curated from online resources wherein the user did not obtain informed consent from the individuals who own or are present in the images. Perhaps the most alarming feature is that of specific types of image which store geographical coordinates of the location a photo was taken, such as GeoTIFF or EXIF.

Most individuals would shrug this off as being harmless, since it has very minor ramifications to their personal life. However, with sufficient knowledge this information can be used to obtain a great deal of personal information. Images uploaded by individuals which are then voluntarily shared can present privacy violations to other individuals present in the image. This information can be used to find personal associations, and combined with image data to determine commonly visited locations or the homes of an individual or their relatives and friends.

This issue is well highlighted by a somewhat amusing and yet concerning study by two Harvard undergraduates looking at images on the Dark Web. By studying images of drugs scraped from websites on the Dark Web (websites only accessible using onion routing on a specialized web browser called Tor), the undergraduates were able to produce a map and isolate the approximate locations of drug dens. Most smartphones today attach this geographical information to pictures automatically, unbeknownst to the average user, and is easily extractable from a scraped image.

Relevance to TinyML

As data scientists and machine learning practitioners, it is important for us to find ways to uphold the ethical foundations set by our forebearers. One of the best ways for this to be done

is to understand the ethical ramifications of our actions, and to try and safeguard against situations where such transgressions may manifest. For example, when curating a publicly available dataset, ensuring that images are within the public domain or by entering into a third party agreement with the original data provider. If the dataset is to be used for computer vision, the geographical data provides no utility, and thus should be removed in order to minimize potential harm to the individuals that produced the original data. Similarly, if images contain personal or revealing information about an individual, they should not be used in a dataset. As a rule of thumb, the minimum amount of data should be utilized to obtain the desired result. If the provenance of a dataset is uncertain or the licensing ambiguous, it is important to err on the side of caution and either confirm the provenance or disregard the data.

This is true not just for during model training but also inference. In our TinyML visual wake words application, we use a camera which is able to take images in real-time. These images are transferred to a framebuffer which then performs inference on the newly obtained image. In the majority of TinyML applications, it is infeasible to obtain informed consent for each person that may potentially fall inside the image, presenting an ethical dilemma. For example, if an entity would like to save images from a smart doorbell for use at a later time, either for future training data or for diagnostics, it may violate the above-mentioned ethical principles. These images may also be saved with metadata, which may further compromise privacy. Thus, we must be mindful when developing these systems to ensure that the obtained images are only for real-time detection and are not archived, or are covered by additional provisions.