Privacy in the Age of AI:
Navigating the Ethical Dimensions of Machine Learning

By Kiara Ward

Privacy is a fundamental right as acknowledged by the UN Declaration of Human Rights which encompasses freedom from intrusion or disturbance into someone's personal life. Laws surrounding privacy are particularly concerned with the handling of sensitive information such as medical and criminal records, addresses, religious beliefs and ethnicity which can compromise security or interfere with autonomy.

Recently, concerns regarding privacy have emerged due to rapid advancements in the field of machine learning, a branch of artificial intelligence. Machine learning enables systems to learn and adapt without explicit programing in order to make accurate outcome predictions or classifications. However, this can only be achieved through the use of vast quantities of data which train an algorithm to make said predictions through the identification of patterns. The ethical issues that arise concern the unwilling collection of sensitive information from an individual in the form of data which is often stored insecurely.

Machine learning collects relevant data through scraping and capturing information from countless online sources and or using data fed to it manually. Often, this data contains information about people who have not consented to the use of the data to train an AI system, due to the process by which the data is collected. This encroaches on an individual's right to privacy as, by law dictated by the Australian Government, they have the right to know why personal data is being collected, how it will be used and who has access to it. (https://www.servicesaustralia.gov.au/your-right-to-privacy?context=1)

Additionally, the process of using personal data to train an algorithm results in a prediction which can in many ways be harmful to an individual. Certain sensitive information regarding a person's ethnicity, sexual orientation, health status and religious beliefs are protected by law and restrictions are put on the handling of such data. With access to sensitive information where no regulations have been implemented, AI is capable of making predictions that are discriminatory, perpetuate biases and enhance societal inequalities. This not only violates the right to privacy but impacts autonomy when predictions made by machine learning are implemented into the real world such as into the fields of employment or finance.
(https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/22-sensitive-information/regulation-of-other-aspects-of-handling-sensitive-information/)

Due to machine learning requiring large amounts of information in the form of data, the storage of that data is vital to the success of a machine learning system. However, securing the storage of data is regularly overlooked as a result of the extreme quantities that must be encrypted to ensure protection. Information is often consequently stored in plain text CSV files, which are vulnerable to attacks. These attacks can have extreme privacy ramifications as not only can sensitive data be accessed by malicious hackers, violating the right to data privacy, but can be released to the public in data breaches. Public access to sensitive information is incredibly dangerous as it can compromise an individual’s security and make them targets for further attacks such as personalised and convincing phishing attacks and identity theft.

Emerging AI technologies are increasingly encroaching on rights to privacy. Facial recognition technology is a recent development of machine learning and is progressively being implemented into electronic devices such as phones and security cameras. The technology is inherently intrusive as individuals are automatically identified and monitored without consent, violating privacy. In addition, the collection of faces in a database which is unable to be encrypted endangers security as it can be accessed and used for malicious intent such as identity theft and stalking.

In conclusion, machine learning often intrudes on the human right to privacy. Therefore, means by which data is collected, intended use for any sensitive data, security of data storage and consequences of new unexplored developments in the field of AI must be taken into confederation in order to ensure that an individual's private right of security and autonomy are preserved.