Privacy in the Age of AI: Navigating the ethical Dimensions of machine learning - Deakin Fisher

Machine learning creates a diverse range of opportunities once not thought possible, yet with this comes a range of complex ethical dilemmas, some of which uncover a greater threat to our given rights of privacy. Machine learning is based on the core principles of gathering, retaining, and utilising data, yet such principles can be harmful, especially regarding the gathering and utilisation of such data. This harm comes in the form of the exposure of sensitive information, which is common with big tech companies.

As cyberspace develops and machine learning becomes more complex, the extent to which data is needed to improve AI tools increases exponentially. Yet through this, the unethical way big data companies are obtaining this data comes to light through the complex privacy policies that stretch the limits of online consent. The gathering of such data spawns numerous unethical problems, the foremost of these being around the manipulation of consent through TOS (terms of service agreements). This is the primary way companies are able to legally obtain data, often with the user not knowing that their data is being collected. In most cases, this is harmless and a way for companies to improve both revenue and user compatibility, yet it also creates a level of distrust between the user and the company and can be used for malicious purposes.

An example of this in regard to machine learning is the implementation of voice data tracking in Amazon's Alexa devices. At face value, this presents as a way to enhance the user experience, and Amazon markets this as such, a free open database, yet the intentions behind the mass data collection are more monetary-based than user-based.

A study published at the ACM Internet Measurement Conference in 2023 revealed the harmful intent driven by monetary gain that Amazon had. The results showed that Amazon processes smart speaker interactions to further infer user interests, using them to further target personalised ads. Interactions with said smart speakers led to bids of over 30 times the average price per interaction (from third-party advertisers) compared to devices that were not smart speakers. The study also found that Amazon had not clearly disclosed the applications of their data, and these were not often disclosed in their policy documents.

The exploitation of data collection for monetary gain is an apparent problem within cyberspace and presents a difficult ethical question: sacrificing the efficiency of AI improvement to secure the privacy of the user. Recent years have seen attempts to tackle the gargantuan project of protecting users' privacy, such as the introduction of the GDPR (General Data Protection Regulation), a law which aims to tackle the difficult dilemmas data collection poses, especially around its utilisation in AI tools within Europe. The approach to the manipulation of users' privacy is largely punitive, imposing harsh fines and jail time for perpetrators, imposing a clear line between black and white, ridding data collection of its morally grey nature. Such measures are temporary, as machine learning is ever-evolving and rapidly outpaces any forms of punishment to stop it. Yet by setting up robust parameters, we can begin to formulate the way in which AI behaves in regard to data collection.

The advances in machine learning revolutionise the efficiency of many products and services, yet the nature of their improvement relies on a crucial aspect: the gathering of data. Due to the nature of how the data is gathered, machine learning is undermined, held down by the weight of a morally complex situation in which the true intent of data collection can be hidden. This presents itself famously in the example of the Amazon Alexa case, in which gathered data was used for monetary gain rather than improving the Amazon Alexa. While these issues might persist, robust punitive measures are being put in place as an attempt to unblur the line of morally grey. Yet such efforts are feasibly impossible when the line between black and white is constantly changing and evolving. The question lies now, if the true intent of machine learning is to automate how information processes, or instead to automate us.