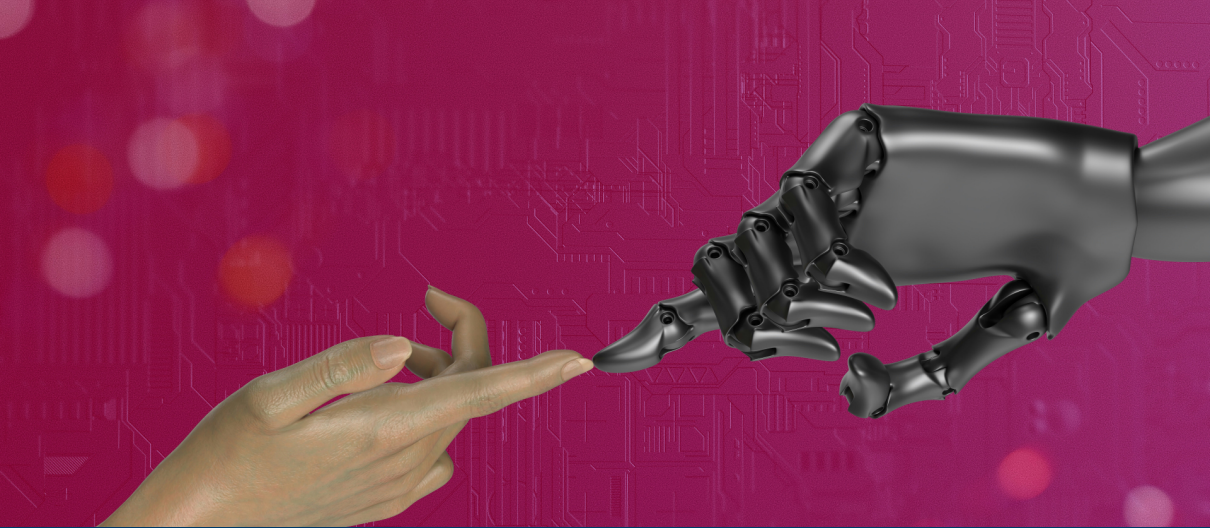




Hands-On Machine Learning

Dr. Derek Bridge | 2026/2027

22. Data Ethics

In this lecture, we look at data ethics. This is a huge topic — and an active area of research, policy formation and legislation. We only skim the surface in this lecture.

Where Do Datasets Come From?

In industry datasets won't generally come from your lecturer (CS1109, alcohol), from Kaggle (loans and diamonds), from the UCI ML Repository (concrete and glass) or from open government web sites (stop-and-search).

Internal Datasets

- You may have historical datasets, e.g. about customers or patients.
 - E.g. on paper — which you can digitize.
 - E.g. in files and databases — which you can re-structure (merge, join, flatten).
- You may create new datasets.
 - E.g. conduct surveys of customers or the public.
 - E.g. record transactions (such as web purchases or clicks) or log incidents (such as equipment failures) on an on-going basis.
 - E.g. install sensors to take measurements.

External Datasets

- You might pay for access to data from a data broker such as an Internet analytics service.
- You might use another organization's API to obtain their data, e.g. reviews from Amazon. You may have to pay if you want unthrottled access.
- You might scrape data from the web. Sites are likely to block unauthorized scrapers.

Where Do Labels Come From?

Internal labelling

- Your own employees might do the labelling.
- It may be a by-product of their normal work.
 - E.g. grading a student exam.
 - E.g. moving an email to the junk folder.
- Or it might be a separate activity.
 - E.g. asking medics to label X-rays.

Crowdsourcing

- Where specialist knowledge is not needed, you can recruit labeling labour on the web.
- E.g. you could use Amazon's *Mechanical Turk* to pay the public to label photos.
- E.g. when you complete a *CAPTCHA*, you are, in fact, labelling the images.
- Each example should be presented to multiple crowd-workers to obtain a consensus about the label.



Outsourcing

- There are companies that provide labelling as a service. Often, they operate in the Global South.
- E.g. <https://www.sama.com/> employs Kenyans and others to label objects in photos and to do text/image/video content moderation.

Who Owns The Data?

- Arguably, no-one!
- But different rights may apply.
- E.g. was the data collected with consent?
- E.g. does the consent extend to the data being sold on/re-purposed?
- E.g. when using APIs or scraping, are you observing terms and conditions?
- E.g. when data comes from the web, copyright may apply.

The Risks of Unauthorized Data Collection

- Litigation.
- Reputational harm.

Data Ethics

- **Data ethics** refers to the moral principles that govern the collection, processing and use of data.
- It refers to the guidelines for balancing the benefits of using data with the protection of individual rights and societal values.

Five Principles

- Protection of individual rights.
- Mitigation of bias.
- Enhancement of trust and accountability through transparency.
- Safeguarding against harm.
- Promotion of social responsibility.

Protection of individual rights

Without protections, there are risks of infringing upon individuals' rights to privacy, autonomy and dignity. Key to this are informed consent, given freely and revocable. Only the minimum data necessary for the stated purpose should be collected, and collection of sensitive data should be avoided unless there is a clear justification.

Mitigation of bias

Without mitigation, there are risks of perpetuating or amplifying existing inequalities — or introducing new ones.

Enhancement of trust and accountability through transparency

Transparency in data collection and clear communication of data use policies fosters trust between data providers, the data user and the broader community. Transparency when there are failings fosters accountability.

Safeguarding against harm

Safeguards should ensure the correctness of the data and protect against its unauthorized use or disclosure. Without safeguards, there are risks of privacy breaches, identity theft, incorrect decision-making, . . .

Promotion of social responsibility

To promote social responsibility, the broader implications of data collection and use on diverse stakeholders, communities and society must be considered. These might include social outcomes and sustainability.

Facebook/Cambridge Analytica Case Study

Based on material from Sheera Frenkel & Cecilia Kang: *An Ugly Truth: Inside Facebook's Battle for Domination*, 2021 and [Wikipedia](#).

- In 2007, Facebook (FB) launched *Facebook Platform* — a framework which lets third-party developers create apps that access data about FB users.
- It exposes user names, email addresses, cities of residence, birth dates, relationship details, political affiliations and employment history — but also the data of a user's friends.
- For every 10 FB employees tasked with recruiting new app partners, there was just one overseeing the partnerships to check the data was being used responsibly.
- In 2013, Aleksandr Kogan — at the time, an academic in the University of Cambridge — created one of these apps. *thisisyourdigitallife* was a personality quiz.
- Kogan's company, Global Science Research, in collaboration with political consultancy *Cambridge Analytica* (CA) paid FB users to complete the quiz.
- Each participant gave their consent to having their data collected for academic use.
- Nearly 300,000 users participated.
- But the app also harvested data about the participants' FB friends, without their knowledge or permission.
- This resulted in data on somewhere between 30 million and 87 million users, including a huge swathe of the American electorate.
- For Kogan to share the app data with CA was a breach of FB's terms and conditions.
- CA used some of the data for political ad micro-targeting in the 2016 US presidential election in support of Donald J. Trump and in opposition to Hilary Clinton, an election that Trump won — his first term of office. The effectiveness of the micro-targeting is disputed.

Facebook/Cambridge Analytica Case Study

- The story broke in 2018.
- FB CEO, Mark Zuckerberg, was summoned in front of the US Congress for two days. Ultimately, the US Federal Trade Commission fined FB \$5 billion, for repeated privacy breaches dating back to 2011.
- British authorities siezed CA's servers and investigated CA's role in support of the 2016 Brexit referendum. The company filed for bankruptcy in 2018.
- Kogan left the University of Cambridge, settled with the US Federal Trade Commission over allegations that he misled the app users, and is now a tech entrepreneur.

Exercise

What did Facebook do wrong? What did Kogan do wrong? What did Cambridge Analytica do wrong?

Data Ethics

- Data ethics is about organizational culture.
- It is about responsibility and accountability.
- It is everyone's responsibility: from developers to managers to directors.
- It is about communication of values and embedding them in organizational practice.
- Ongoing education and training are required.
- It goes beyond the question of what is legal/illegal.

Image credits



Taken from

<https://www.grovestreett.com/blog/why-do-online-captcha-boxes-show-traffic-pictures>
