Code Quality, Security & Ethical Implications in ML Development

AI Masters Capstone Project - Presentation 5

Jonathan Agustin

November 2024

Agenda

- Code Quality Assurance
- Security Scanning & Attestation
- Automating Documentation & Reporting
- Ethical Software Development: Accountability & Justice

We finalize our ML toolset by anchoring it in ethical responsibility and legal accountability.

Code Quality Assurance

- Consistent style guidelines & linting for maintainable code
- Code reviews as ethical checkpoints—raise questions on suspicious logic
- Clear documentation prevents “plausible deniability” in unethical designs

High-quality code is a foundation for both technical excellence and ethical accountability.

Security Scanning & Attestation

- Automated vulnerability detection to preempt misuse
- Attestation ensures the integrity & authenticity of code components
- A secure pipeline guards against ethically disastrous exploits

Security is not neutral—failing to secure your code can facilitate immense harm.

Automating Documentation & Reporting

- Model cards & data sheets reveal assumptions, limitations, and potential biases
- Transparent audit trails: who changed what, when, and why
- Supports meaningful recourse and contestability for impacted communities

Information empowers oversight, shifting power back towards those impacted.

Ethical Software Development

- Go beyond accuracy: consider societal impact, justice, and accountability
- Encourage internal dialogues: raise flags if your code could be misused
- Remember VW: developers can face prison, not just moral regret

Ethical coding is about preventing harm and ensuring that "just following orders" never becomes your legacy.

A Complete Ethical ML Ecosystem

- Ethical data handling + responsible training + safe deployments = trust
- Code quality, security, and transparency build on that trust
- Aligning technology with human rights, justice, and societal well-being

Your ML pipeline is now both a technical marvel and a moral statement.

Final Thoughts

- ML developers shape global narratives and human destinies
- Ethical safeguards aren't optional; they are our shared duty
- Innovate responsibly—balance power, challenge injustice, and uphold human values

Go forth and build ML systems that reflect our best selves, not our worst impulses.

Temporary page!

LATEX was unable to guess the total number of pages correctly. As there was some unprocessed data that should have been added to the final page this extra page has been added to receive it.

If you rerun the document (without altering it) this surplus page will go away, becau LATEX now knows how many pages to expect for this document.