Collaborative Discussion 1 – Codes of Ethics and Professional Conduct

In this discussion, I engaged with various peers on ethical dilemmas in computing, particularly focusing on how professional codes like the ACM Code of Ethics and BCS Code of Conduct guide ethical decision-making in complex digital environments.

Jaafar El Komati's Case: Malware Disruption and Rogue Services

Jaafar introduced a compelling case involving Rogue Services, an ISP that supported malware distribution under the guise of guaranteed uptime. He highlighted breaches of ACM Principles 1.1, 1.2, and 2.8, and linked them to the BCS sections on public interest and avoidance of harm. His argument emphasized how ignoring repeated warnings and hosting unauthorized content raises both ethical and legal concerns.

What stood out to me in Jaafar's analysis was his nuanced view of the ethical counteraction—the deployment of a worm aimed at stopping Rogue. Even though this action was well-intended and designed to minimize harm, it still resulted in damage to innocent third parties, raising tensions between intent and impact.

Peer responses further deepened this discussion. Dhia pointed out the unintended harm caused despite self-limiting safeguards, showing how even ethically motivated interventions require extreme caution. Martyna expanded the conversation by introducing the concept of accountability in distributed systems, where legal jurisdiction gaps make it difficult to assign responsibility. Craig reinforced the argument by stressing the legal and ethical failures of Rogue, noting that the company's actions endangered users and violated cybersecurity norms.

From this, I realized that ethical decisions in computing must account not only for direct consequences but also for broader systemic and global dimensions. The debate reminded me that good intentions are not enough—we must also anticipate ripple effects and potential harms.

Koulthoum Flamerzi's Case: Inadvertent Disclosure of Sensitive Data

Koulthoum's case focused on a software engineer who released an app without thorough testing, leading to a data leak. She highlighted violations of ACM Principles 1.6 and 2.5, and referenced GDPR and the UK Data Protection Act. She also connected these breaches to the BCS Code, emphasizing the importance of public interest and professional competence.

The peer responses were insightful. Craig emphasized the erosion of public trust that results from ethical negligence. Mohamed added another layer by questioning whether the blame should lie solely on the engineer, or whether organizational culture and lack of testing protocols also played a role. Shaikah stressed that ethical considerations must be embedded across the entire development lifecycle, not only at the end stages.

These reflections made me think deeply about shared ethical responsibility—it's not just about individual developers, but also the leadership, project managers, and company policies. A strong ethical culture must be cultivated across all levels of a development team.

My Own Case: Ethical Risks in Generative AI for Education

In my initial post, I discussed a case involving a startup that used generative AI trained on internal academic data without consent. I identified violations of ACM Principle 1.6 (respect privacy) and 1.2 (avoid harm), and related the case to GDPR transparency standards. I contrasted the ACM and BCS codes—while the ACM focuses on

individual responsibility, BCS adds a systemic view by urging proactive management of emerging tech risks.

Although I didn't receive direct peer responses, writing this post helped me recognize how ethical computing today involves much more than data privacy. We must also consider explainability, accountability, and fairness, especially as AI becomes embedded in sensitive domains like education.

This case made me reflect on the need for ethical foresight in AI development—professionals are no longer just builders of tools; we are shaping how future generations learn and interact with technology.

Final Takeaways

Across all cases, one shared theme stood out to me: ethical responsibility in computing is both individual and collective. Whether it's combating malware, protecting user data, or deploying AI in education, decisions must be guided by structured ethical frameworks and grounded in social awareness. Both the ACM and BCS codes offer valuable guidance—but they must be actively practiced, not just referenced.

This discussion reinforced for me that ethical computing is about anticipating harm, ensuring transparency, and fostering trust—in users, in systems, and in the broader digital ecosystem we all contribute to.