Peer response 2 – Marie

Marie's analysis effectively demonstrates how Q Industries' progression from passive to lethal autonomous systems violates both ACM and BCS ethical principles, particularly regarding public good and human rights protection (Association for Computing Machinery, 2018; British Computing Society, 2022). Abdulhakim builds on this foundation by identifying the hierarchical tension between competing principles—specifically the conflict between respecting intellectual property and serving public welfare—while questioning whether clearer guidelines are needed for mandatory whistleblowing obligations. Opeyemi strengthens the technical argument by providing concrete evidence of facial recognition bias and connecting professional ethics to international humanitarian law frameworks, particularly the UN Convention on Certain Conventional Weapons (United Nations Office for Disarmament Affairs, 2001).

The most pressing issue raised across these contributions is Abdulhakim's question about when professionals have not just the right, but the obligation to break confidentiality agreements. Both ACM Section 1.7 and BCS Section 2.4 address confidentiality exceptions for legal violations or public harm, but the threshold remains ambiguous. Historical precedents like the Pugwash Conferences demonstrate how scientific communities established collective ethical boundaries that transcended individual employer obligations (Rotblat, 1999), with computing professionals needing similar mechanisms. Regarding Opeyemi's question about operationalizing international frameworks, the IEEE's autonomous systems standards (IEEE 2857-2021) provide technical implementation guidance that bridges professional codes with legal requirements (*IEEE Standard for Transparency of Autonomous Systems*, 2021). The dual-use dilemma Abdulhakim identifies reflects broader challenges documented in science and technology studies: defensive technologies inevitably evolve into offensive capabilities (MacKenzie, 1993), requiring proactive ethical frameworks rather than reactive responses. The Campaign to Stop Killer Robots demonstrates how professional communities can influence policy development in autonomous weapons governance (Wareham, 2020).

The Q Industries case ultimately demonstrates that professional ethics in computing must evolve beyond individual decision-making to encompass collective responsibility for technologies that can fundamentally alter power balances between states and citizens. The convergence of technical bias, legal frameworks, and ethical obligations reinforces that computing professionals bear heightened stewardship responsibilities when their work intersects with fundamental human rights and international security.

References:

Association for Computing Machinery (2018) ‘Code of Ethics’. Available at: https://www.acm.org/code-of-ethics (Accessed: 31 August 2025).

British Computing Society (2022) *BCS Code of Conduct for members - Ethics for IT professionals*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct (Accessed: 31 August 2025).

IEEE Standard for Transparency of Autonomous Systems (2021) *IEEE Standards Association*. Available at: https://standards.ieee.org/ieee/7001/6929/ (Accessed: 31 August 2025).

MacKenzie, D. (1993) *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. Cambridge, MA, USA: MIT Press (Inside Technology).

Rotblat, J. (1999) ‘A Hippocratic Oath for Scientists’, *Science*, 286(5444), pp. 1475–1475. Available at: https://doi.org/10.1126/science.286.5444.1475.

United Nations Office for Disarmament Affairs (2001) ‘The Convention on Certain Conventional Weapons’. Available at: https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/ (Accessed: 31 August 2025).

Wareham, M. (2020) ‘Stopping Killer Robots’, *Human Rights Watch* [Preprint]. Available at: https://www.hrw.org/report/2020/08/10/stopping-killer-robots/country-positions-banning-fully-autonomous-weapons-and (Accessed: 31 August 2025).