Autonomy Without Accountability

The case study Automated Active Response Weaponry (ACM, 2018) raises serious concerns about Q Industries' compliance with professional ethics. Q has moved from passive defence technologies to non-lethal and now potentially lethal autonomous responses. Evaluated against the BCS Code of Conduct, this progression exposes ethical, legal and professional failures.

Public Interest (Clause 1): Facial recognition at protests and autonomous weapons risk breaching privacy rights, human rights law and public safety. Public trust erodes quickly when rights are threatened. Google Glass, for example, faced strong backlash due to privacy concerns (Denning et al., 2014). Unlike current military drones, which require human oversight for lethal action, Q's proposed systems would remove accountability and increase the likelihood of unlawful harm (Horowitz and Scharre, 2015).

Professional Competence (Clause 2): Q ignored ethical warnings and failed to safeguard against misuse. This breaches competence and integrity obligations and exposes the company to negligence and liability. A similar pattern has appeared in self-driving car development, where overstated readiness and unclear responsibility damaged public confidence (Bonnefon, Shariff & Rahwan, 2016; Stilgoe, 2018).

Relevant Authority (Clause 3): Engineers who resigned and spoke out mirrored Edward Snowden, who prioritised public interest over contractual loyalty (Greenwald, 2014). Both cases show the conflict between legal obligations and professional judgement.

The Profession (Clause 4): Q's retaliation against whistleblowers risks discrediting the wider profession. The Facebook, Cambridge Analytica scandal showed how misuse of personal data by one organisation damaged trust in technology across society and raised questions about the integrity of computing professionals (Isaak & Hanna, 2018; Susser, Roessler & Nissenbaum, 2019).

Q's pursuit of lethal autonomy prioritises operational goals over public good, violating the BCS Code. Unlike the fictional "Q Branch" of James Bond, real computing professionals must work within ethical and legal limits to prevent cinematic fantasy from becoming real world harm.

References

Association for Computing Machinery (ACM) (2018). *Automated Active Response Weaponry*. ACM Code of Ethics: Case Studies. Available at: https://www.acm.org/code-of-ethics/case-studies/automated-active-response-weaponry (Accessed: 28 August 2025).

Bonnefon, J-F., Shariff, A. and Rahwan, I. (2016). 'The social dilemma of autonomous vehicles', *Science*, 352(6293), pp. 1573–1576. Available at: https://www.researchgate.net/publication/301293464_The_Social_Dilemma_of_Autonomous_Vehicles (Accessed: 28 August 2025).

Denning, T., Dehlawi, Z. and Kohno, T. (2014). 'In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI 2014)*, pp. 2377–2386. ACM. Available at: https://ar-sec.cs.washington.edu/files/ar-chi2014.pdf (Accessed: 28 August 2025).

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the US surveillance state*. New York: Metropolitan Books. Available at: https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1552&context=jss (Accessed: 28 August 2025).

Horowitz, M.C. and Scharre, P. (2015). 'Meaningful human control in weapon systems: A primer', *Parameters*, 45(1), pp. 7–17. Available at: https://www.files.ethz.ch/isn/189786/Ethical_Autonomy_Working_Paper_031315.pdf (Accessed: 28 August 2025).

Isaak, J. and Hanna, M.J. (2018). 'User data privacy: Facebook, Cambridge Analytica, and privacy protection', *Computer*, 51(8), pp. 56–59. Available at: https://doi.org/10.1109/MC.2018.3191268 (Accessed: 28 August 2025).

Stilgoe, J. (2018). 'Machine learning, social learning and the governance of self-driving cars', *Social Studies of Science*, 48(1), pp. 25–56. Available at: https://www.jstor.org/stable/pdf/48569070.pdf (Accessed: 28 August 2025).

Susser, D., Roessler, B. and Nissenbaum, H. (2019). 'Technology, autonomy, and manipulation', *Internet Policy Review*, 8(2). Available at: https://policyreview.info/pdf/policyreview-2019-2-1410.pdf (Accessed: 28 August 2025).