The case study entitled *Automated Active Response Weaponry* published by the Association for Computing Machinery (ACM) outlines a hypothetical scenario where evolving interests of a company and its stakeholders begin to conflict with those employees responsible for designing and developing the product.

Q, a public safety and defence contractor designs and produces autonomous vehicles responsible for carrying out non-weaponized tasks such as ordinance diffusion and crowd surveillance (ACM Ethics, 2018). As the product's use case expands into higher risk conflict oriented applications, stakeholder interest in artificial intelligence (AI) guided weaponization is proposed and adopted leading to a number of engineers to publicly depart due to ethical concerns over the new product direction. This in turn leads to legal action being taken out against the whistleblowers for breaching their non-disclosure agreements (NDA), potentially violating government secrecy/clearance levels.

This case represents an interesting and complex application of ethics and the government regulation of classified material. The engineers are seen upholding some of the BCS codes of conduct, namely, the principle of public interest where individuals should have, "due regard for health, privacy, security and wellbeing of others and the environment (www.bcs.org, n.d.)." The departing employees are acting in the best interest of the public who may be directly impacted by the application of this technology. This is also in line with the ACM's code of ethics largely pertaining to sections 1.1 and 1.2 where IT professionals should contribute to a society of stakeholders (1.1), while taking into account the repercussions and avoidance of the potential for harm (1.2) (ACM Ethics, 2018).

It is rare for matters of ethics and law to be perfectly black and white and while the engineers may be justified in their response, they also violate other ethical principles observed by both BCS and ACM. ACM section 2.3 stipulates an adherence to the rules and policies enforced by an organization(ACM Ethics, 2018); likewise covered under the BCS policy to respect the organization or individual you work for (www.bcs.org, n.d.). This is exacerbated by the nature of the material made public, potentially violating United States code § 798 - Disclosure of classified information if Q was holding contracts with the US government (LII / Legal Information Institute, 2020).

Ultimately, this case study articulates the complexity of ethics in a professional environment, where ethically justifiable actions may not guarantee amnesty from legal action taken in response.

References:

ACM Ethics. (2018). *Case: Automated Active Response Weaponry*. Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-automated-active-response-weaponry/ [Accessed 24 Jan. 2022].

www.bcs.org. (n.d.). *BCS Code of Conduct | BCS*. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ [Accessed 24 Jan. 2022].

LII / Legal Information Institute. (2020). *18 U.S. Code § 798 - Disclosure of classified information*. Available at: https://www.law.cornell.edu/uscode/text/18/798 [Accessed 24 Jan. 2022].