**Collaborative Learning Discussion 1 - Peer Responses**

1. **Charlotte**

Further to Charlotte’s points, this case study suggests that some of Max’s abusive behaviour is directed specifically at female members of the team (ACM, N.D.). For example, by not allowing them to be named as authors on studies.

Discrimination on the basis of gender in the workplace is illegal under the Equality Act 2010 (Ayling & Miller, 2021). Furthermore, an amendment to hate crime laws in the UK to include misogyny is being considered and has garnered considerable support (Westendarp, 2022). If passed, this change would allow for more stringent sentencing of people who are hostile towards women based on their gender.

In addition to the criminal law applicable to Max, there are also legal concerns applicable to Jean and, by extension, the employing company itself (Health and Safety Executive, N.D.). Employers and those acting on behalf of employers, such as team managers, have a duty of care to staff. This includes protecting them from the kinds of harassment and abuse that are described in the case study. Failing to do so could result in litigation against the employer and individuals under civil law.

In conclusion, not only is Max in contravention of various professional codes of conduct for the IT industry, but what he is doing is also illegal and could carry heavier penalties if he continues to act in this way. In addition, management are also failing to appropriately protect Diane and could therefore face litigation themselves.

References

ACM (N.D.) Case: Abusive Workplace Behavior. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-abusive-workplace-behavior/> [Accessed 2 February 2022].

Ayling, L. & Miller, J. (2021) Sex discrimination and employment. Available from : <https://www.cipd.co.uk/knowledge/fundamentals/emp-law/sex-discrimination/factsheet#gref> [Accessed 2 February 2022].

Health and Safety Executive (N.D.) Preventing Workplace Harassment and Violence. Available from: <https://www.hse.gov.uk/violence/> [Accessed 2 February 2022].

Westendarp, L. (2022) UK upper house votes to make misogyny a hate crime. Available from: <https://www.politico.eu/article/house-of-lords-votes-to-make-misogyny-a-hate-crime-handing-johnson-series-of-defeats/> [Accessed 2 February 2022].

1. **Simon**

Safe routes for whistblowers to raise concerns are beneficial to the public interest as it can expose unethical or damaging behaviour that might otherwise go unaddressed (Unison, 2021). Whilst Q may have initiated civil litigation against the engineers (ACM, N.D.), the court could waive the breach of confidence if it was deemed to be in the public interest to disclose the information (Bott, 2014). However, court rulings are unlikely to protect the engineers from the victimisation that is common in whistleblowing cases, such as intentional reputational damage that could affect future employment. The Public Interest Disclosure Act (PIDA) 1998 was introduced in the UK with the intention of providing protection against victimisation in cases such as this one, however the application of this law is complex. To be afforded protections, a whistleblower must make sure that the type of disclosure qualifies under PIDA and that the way it is disclosed constitutes a protected disclosure. This complexity and uncertainty in the application of protections to whistleblowers means that many people still do not come forward.

In conclusion, whilst breaching a confidentiality agreement may be in the public interest, it could result in damage to the individual involved. In order to encourage responsible ethical decisions in businesses, individuals must have confidence that they will be protected if they raise concerns.

References

ACM (N.D.) Case: Automated Active Response Weaponry. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-automated-active-response-weaponry/> [Accessed 3 February 2022].

Bott, F. (2014) *Professional Issues in Information Technology*. 2nd ed. London: BCS.

Unison (2021) Whistleblowing. Available from: <https://www.unison.org.uk/get-help/knowledge/disputes-grievances/whistleblowing/> [Accessed 3 February 2022].

1. **Vaibhav**

Further to Vaibhav’s points, unethical implementations of artificial intelligence algorithms can stem from a lack of understanding as well as an innate bias to trust automated decisions (Fry, 2018). For example, after an investigation into an algorithm that was employed to determine disability benefits in the state of Idaho, it was shown that not only was the logic almost random in some cases but the historical data it used was erroneous (Stanley, 2017). Medicaid did not question the outputs of the algorithm and this led to serious impacts on claimants who had their benefits cut. This example shows the ethical importance of scrutinising both the logic and the data inputs used to inform automated decisions. To compound the issue of understanding algorithm logic, there may be certain situations where the logic cannot be followed by humans due to sheer complexity and this could lead to further ethical questions (Fry, 2018).

One of the four pillars of the BCS code of conduct centres around professional competence (BCS, 2021). In this case study, the lack of competence of the engineers and decision-makers involved with Blocker Plus has been exposed in their approach to not only the implementation of machine learning without scrutinising the data inputs, but also the decision to continue to use the same logic and data approach even after exposing the underlying issue (ACM, N.D.). The hope that the algorithm will use new data inputs to in effect correct itself is fundamentally flawed and does not acknowledge the bias that may already have been created.

In conclusion, these case studies expose the importance of ensuring competence in the use of advanced technologies before employing them. This competence should include an understanding of both the limitations and potential ethical impacts of the technology being used.

References

ACM (N.D.) Case: Malicious Inputs to Content Filters. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-malicious-inputs-to-content-filters/> [Accessed 7 February 2022].

BCS (2021) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 7 February 2022].

Fry, H. (2018) *Hello World: How to be Human in the Age of the Machine*. 1st ed. Transworld Digital.

Stanley, J. (2017) Pitfalls of Artificial Intelligence Decisionmaking Highlighted In Idaho ACLU Case. Available from: <https://www.aclu.org/blog/privacy-technology/pitfalls-artificial-intelligence-decisionmaking-highlighted-idaho-aclu-case> [Accessed 7 February 2022].

1. **Jan**

There is a theme throughout this discussion of considering whether an unethical act, such as using a worm to disrupt a service provider, can be considered ethical under certain circumstances (ACM, N.D.). In order to answer this question, the collateral damage would need to be considered beforehand and possibly remedied following the event (Bryant & Kennedy, 2014). Beforehand, did the coalition of vendors and governments risk assess the collateral damage to the genuine online retailers hosted by Rogue Services in line with code 2.5 of the ACM Code of Ethics (ACM, 2018)? And what if the mechanism to prevent spread to other service providers had not worked? Following the event, the coalition could be subject to legal recourse from the genuine retailers that have lost data, service and possibly suffered other, less tangible impacts, such as reputational damage. Had the coalition set aside resources to identify, assess and remedy the damage to these genuine businesses?

Whilst this approach was taken in pursuit of the overall public good, this was not the only course of action available to disrupt this malicious service provider. As such, due consideration for the collateral damage should have been included in the decision making process as well as in the wake of the event. The coalition could only claim this to be an ethical act if they use assessments and professional judgement to determine that the public good genuinely outweighs the collateral damage linked to the event.

References

ACM (2018) ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics> [Accessed 11 February 2022].

ACM (N.D.) Case: Malware Disruption. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption> [Accessed 11 February 2022].

Bryant, R. & Kennedy, I. (2014) ‘Investigating Digital Crime’, in: Bryan, R. & Bryan, S. (eds) *Policing Digital Crime*. Farnham, Surrey: Ashgate. 123-145.

1. **Umar**

To further Umar’s point on data management, data ethics is an emerging field that is gaining attention due to data collection and processing becoming an inherent part of daily life, from optimising physical exercise to managing personal finances (Lou & Yang, 2020). This has even led to professional codes of conduct being established specifically for data scientists (Grindrod & Moreno, 2018). This code introduces the concept of a logbook to record data issues that could impact processing results, for example issues with data accuracy and potential biases. Making this logbook available to decision makers would ensure they could make informed decisions that consider the ethical risks associated with any data processing, such as in the case of the Blocker Plus content filter (ACM, N.D.). This code also draws attention to the need for continued professional development to ensure professional capabilities keep pace with developments in the field. I would argue that this is applicable to all IT professionals given the pace of technological change and its potential to cause harm if used incorrectly.

References

ACM (N.D.) Case: Malicious Inputs to Content Filters. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-malicious-inputs-to-content-filters/> [Accessed 14 February 2022].

Grindrod, P. & Moreno, J. (2018) Code of Conduct. Available from: <http://www.code-of-ethics.org/code-of-conduct/> [Accessed 14 February 2022].

Lou, S. & Yang, M. (2020) A Beginner’s Guide to Data Ethics. Available from: <https://medium.com/big-data-at-berkeley/things-you-need-to-know-before-you-become-a-data-scientist-a-beginners-guide-to-data-ethics-8f9aa21af742> [Accessed 14 February 2022].