


# Collaborative Discussion 1

## Initial Post



**Initial Post**  
by Shashank Phatak - Friday, 8 August 2025, 7:52 PM

The Association for Computing Machinery (ACM) provides case studies to illustrate its Code of Ethics and Professional Conduct (ACM, 2018). The malware disruption "Rogue Services" case involves a web hosting company knowingly supporting clients distributing malware and spam to maintain "cheap and guaranteed uptime" (ACM, 2018). This analysis evaluates the application of the ACM Code, compares it with the British Computer Society (BCS) Code of Conduct (BCS, N.D), and highlights legal, social, and professional implications, supported by academic literature.

The ACM Code emphasises prioritising the public good as per Principle 1.1 and avoiding harm, Principle 1.2 (ACM, 2018). Rogue Services violates these by enabling malware and spam, which harm users through data breaches and privacy violations. This aligns with Gotterbarn *et al.*, (2017), who argue that ethical lapses in computing, such as ignoring harmful system impacts, undermine societal trust. Principle 2.5 requires comprehensive risk evaluations (ACM, 2018), which Rogue Services neglects by failing to address client activities. Legally, this could breach jurisdictional regulations like the General Data Protection Regulation (GDPR) in Europe (Voigt and Von Dem Bussche, 2017) or cybercrime laws, depending on the hosting location. Non-jurisdictional issues, such as international cybercrime treaties, may also apply (Clough, 2015). Socially, enabling malicious content erodes public trust in digital infrastructure, as Flick and Linders (2019) note, emphasising how unethical practices aggravate privacy concerns and societal harm.

The BCS Code of Conduct prioritises public interest, requiring members to safeguard health, safety, and third-party rights (BCS, N.D). Rogue Services' actions would violate this by enabling harm, like the ACM's stance. Both codes emphasise professional integrity, with BCS requiring due care and conflict avoidance (BCS, N.D), comparable to ACM's Principle 2.2 (ACM, 2018). However, the BCS provides a distinct mechanism for consulting the Secretary-General in ethical dilemmas (BCS, N.D), offering more structured guidance than the ACM. Mokander and Floridi, (2021) examine the role of ethical lapses in IT governance, particularly in AI systems, in contributing to systemic failures with organisational impacts, as illustrated by cases like One.Tel emphasised the need for adherence to ethical codes.

Professionally, Rogue Services' profit-driven approach undermines the computing profession's credibility. Gotterbarn *et al.*, (2017) stresses that ethical codes like ACM's and BCS's are critical for maintaining professional standards in computing. Flick and Linders (2019) further argue that the holistic application of ethical codes is essential for addressing modern challenges like AI and infrastructure risks. This case has deepened my understanding of moral responsibilities, reinforcing my commitment to uphold these standards in practice.

**References**

ACM (2018) ACM Code of Ethics and Professional Conduct. Available at: <https://www.acm.org/code-of-ethics> [Accessed 04 August 2025].

BCS (N.D) BCS Code of Conduct. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> [Accessed: 4 August 2025].

Clough, J. (2015) *Principles of Cybercrime*. 2nd edn. Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9781139540803>.


Flick, C. and Linders, B. (2019) Why should we care about technology ethics? The updated ACM Code of Ethics. Available at: [Why Should We Care about Technology Ethics? The Updated ACM Code of Ethics - InfoQ](#) [Accessed 04 August 2025].

Gotterbarn, D. *et al.* (2017) 'ACM code of ethics: a guide for positive action', *Communications of the ACM*, 61(1), pp. 121–128. Available at: <https://doi.org/10.1145/3173016>.

Mokander, J. and Floridi, L. (2021) 'Ethics-Based Auditing to Develop Trustworthy AI', *Minds and Machines*, 31(2), pp. 323–327. Available at: <https://doi.org/10.1007/s11023-021-09557-8>.

Voigt, P. and Von Dem Bussche, A. (2017) *The EU General Data Protection Regulation (GDPR)*. Cham: Springer International Publishing. Available at: <https://doi.org/10.1007/978-3-319-57959-7>.

## Peer responses



**Peer Response to Md Chowdhury**  
by Shashank Phatak - Thursday, 14 August 2025, 8:56 PM

Thank you for sharing a compelling analysis of the "Inadequate Security Measures" case study, which effectively highlights the ethical and professional failures of deploying vulnerable software under commercial pressure. Your application of ACM Code Principles 1.2 and 2.9 clearly illustrates how the developer's actions caused harm and neglected secure system design (ACM, 2018). Your reference to the BCS Code's emphasis on public interest and privacy protection (BCS, N.D) strengthens the comparison, showing how both frameworks demand accountability. The legal perspective, citing the Data Protection Act 2018, underscores the real-world consequences of such decisions, aligning with Clough's (2015) analysis of data breach liabilities.

Your point about undermining trust within teams and the broader industry, as supported by Gotterbarn *et al.* (1997), is particularly thought-provoking. Another thought crosses the mind, in understanding how the developers can foster a culture of ethical resilience when facing tight deadlines? Your suggestion of escalating risks and advocating for secure defaults is practical, but what mechanisms could ensure these actions are prioritised? Mittelstadt *et al.* (2020) propose ethical governance frameworks, like mandatory audits, to enforce accountability in high-stakes IT projects. It would be interesting to see if such measures prevent similar lapses, or would they risk holding back innovation under bureaucratic weight? The case also prompts reflection on whether professional training should emphasise ethical decision-making under pressure to equip developers better. In a practical world, it's always challenging to balance client expectations with moral obligations, particularly in agile development environments where iterative testing is standard. Your analysis encourages us to consider how transparency and proactive risk management can uphold public trust and professional integrity in computing.

**(Word count: 269)**

**References**

ACM (2018) ACM Code of Ethics and Professional Conduct. Available at: <https://www.acm.org/code-of-ethics> [Accessed 04 August 2025].

BCS (N.D) BCS Code of Conduct. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> [Accessed: 7<sup>th</sup> August 2025].

Clough, J. (2015) *Principles of Cybercrime*. 2nd edn. Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9781139540803>.

Gotterbarn, D., *et al.*, (1997) 'Software engineering code of ethics', *Communications of the ACM*, 40(11), pp. 110–118. Available at: <https://doi.org/10.1145/265684.265699>

Mittelstadt, B.D. *et al.* (2020) 'The ethics of algorithms: Mapping the debate', *Big Data & Society*, 3(2), p. 2053951716679679. Available at: <https://doi.org/10.1177/2053951716679679>



Peer Response to Dalbir Singh

by Shashank Phatak - Thursday, 14 August 2025, 8:54 PM

Thank you for your insightful analysis of the Accessibility in Software Development case study, which effectively highlights the tension between ethical responsibility and commercial pressures. Your application of ACM Code Principles 1.1 and 1.4 demonstrates how neglecting accessibility risks discriminates against users with disabilities, undermining inclusivity (ACM, 2018). Your reference to legal frameworks like the UK Equality Act 2010 (Government Equalities Office and Equality and Human Rights Commission, 2013) and WCAG standards (W3C, 2018) underscores the legal ramifications, reinforcing that ethical duties extend beyond compliance, as Friedman and Hendry (2019) advocate through value-sensitive design.

Your comparison with the BCS Code of Conduct, particularly Section 1(b) and Section 2, is compelling, as it emphasises enforceable duties to uphold equality and public interest (BCS, N.D). This alignment between ACM and BCS codes highlights a shared commitment to fairness. Yet, the BCS's explicit focus on third-party rights adds a layer of accountability that could guide developers in such dilemmas. Your point about reputational harm resonates with Mittelstadt et al. (2020), who argue that ethical lapses in technology governance can erode public trust, particularly in critical areas like accessibility.

This case raises a broader question, how can developers advocate for accessibility under tight deadlines without compromising project viability? Prioritising inclusivity may require innovative approaches, such as modular accessibility integration, to balance efficiency and ethics. Could embedding accessibility training in professional development, as suggested by Gotterbarn et al. (2017), help shift organisational priorities? Your analysis encourages reflection on how we, as future professionals and can champion inclusive design in high-pressure environments.

(Word count: 256)

References

ACM (2018) ACM Code of Ethics and Professional Conduct. Available at: <https://www.acm.org/code-of-ethics> [Accessed 7<sup>th</sup> August 2025].

BCS (N.D) BCS Code of Conduct. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> [Accessed: 7<sup>th</sup> August 2025]

Friedman, B. and Hendry, D.G. (2019) Value Sensitive Design: Shaping Technology with Moral Imagination. The MIT Press. Available at: <https://doi.org/10.7551/mitpress/7585.001.0001> [Accessed on 13<sup>th</sup> August 2025]

Gotterbarn, D. et al. (2017) 'ACM code of ethics: a guide for positive action', *Communications of the ACM*, 61(1), pp. 121–128. Available at: <https://doi.org/10.1145/3173016>

Government Equalities Office and Equality and Human Rights Commission (2013) Equality Act 2010: guidance. Available from: <https://www.gov.uk/guidance/equality-act-2010-guidance#full-publication-update-history> [Accessed on 13<sup>th</sup> August 2025]

Mittelstadt, B.D. et al. (2020) 'The ethics of algorithms: Mapping the debate', *Big Data & Society*, 3(2), p. 2053951716679679. Available at: <https://doi.org/10.1177/2053951716679679>

W3C (2018) Web Content Accessibility Guidelines (WCAG) 2.1. Available at: <https://www.w3.org/TR/WCAG21/> [Accessed on 14 August 2025]

Summary Post



Summary Post

by Shashank Phatak - Tuesday, 19 August 2025, 7:30 PM

The case study analysis of Rogue Services applied ACM Principles 1.1, 1.2, and 2.5, demonstrating how the facilitation of malware undermines the public good and neglects harm avoidance (ACM, 2018). Comparisons with the BCS Code highlighted the importance of public interest and procedural mechanisms (BCS, N.D.). The analysis also considered legal implications such as GDPR and cybercrime laws, alongside the erosion of social trust, as supported by Clough (2015) and Flick and Linders (2019). Mokander and Floridi (2021) connected ethical failings to systemic issues, referencing the One.Tel case.

Feedback Integration

Peers praised the multilateral approach, suggesting practical solutions such as malware scanning (Hughes et al., 2025). In addition, the professor encouraged a more profound critique using ethical theories, including normative moral theories, to navigate dilemmas like the tension between commercial and societal responsibilities. More references per paragraph were also recommended.

Reflection and Learning Outcomes

This case study underscores the ethical complexities involved in balancing client expectations with public safety. A social perspective illustrates that Rogue's profit-driven strategy maximised short-term gains but ultimately led to greater harm, highlighting the need for proactive governance. Implementing ethical audits could enhance accountability (Mittelstadt et al., 2020). This aligns well with the learning outcomes regarding legal, social, and professional responsibilities.

Conclusion

Upon reflecting on this study, I realise that ethical codes serve not only as guidelines but as essential instruments for promoting accountability and trust in the field of computing. This analysis has supported the dedication to prioritising public welfare and advocating for systemic safeguards, such as ethical training and audits, to ensure responsible IT governance. I encourage my peers to consider how we can effectively integrate these practices into real-world systems.

References

ACM (2018) ACM Code of Ethics and Professional Conduct. Available at: <https://www.acm.org/code-of-ethics> [Accessed 04 August 2025].

BCS (N.D) BCS Code of Conduct. Available at: <https://www.bcs.org/membership/become-a-member/bcs-code-of-conduct/> [Accessed: 4 August 2025]

Clough, J. (2015) Principles of Cybercrime. 2nd edn. Cambridge University Press. Available at: <https://doi.org/10.1017/CBO9781139540803>

Flick, C. and Linders, B. (2019) Why should we care about technology ethics? The updated ACM Code of Ethics. Available at: [Why Should We Care about Technology Ethics? The Updated ACM Code of Ethics - InfoQ](#) [Accessed 04 August 2025].

Hughes, L. et al., (2025). AI agents and agentic systems: A multi-expert analysis. *Journal of Computer Information Systems*, 1-29. Available at: <https://doi.org/10.1080/08874417.2025.2483832> [Accessed on 15 August 2025].

Mittelstadt, B.D. et al. (2020) 'The ethics of algorithms: Mapping the debate', *Big Data & Society*, 3(2), p. 2053951716679679. Available at: <https://doi.org/10.1177/2053951716679679>

Mokander, J. and Floridi, L. (2021) 'Ethics-Based Auditing to Develop Trustworthy AI', *Minds and Machines*, 31(2), pp. 323–327. Available at: <https://doi.org/10.1007/s11023-021-09557-8>