Summary Post

The ACM case discussion, "Inadvertent Disclosure of Sensitive Data," brings to the forefront profound ethical and legal implications for software engineering. In my prior post, I highlighted the breaches of Privacy Violations Principles 1.6 and 2.5, which stress privacy and risk assessment (Association for Computing Machinery, 2018). I also highlighted the requirements set by the UK Data Protection Act of 2018, as well as GDPR, about organizational safeguards and the consequences of failing to put such safeguards, highlighting the significant penalties that can be imposed and damage to reputation (Cumbley and Church, 2013).

This peer feedback has helped to broaden my understanding. Norris (2025) argued that software releases without sufficient testing damage public trust, which further emphasizes that ethical wrongdoing can lead to severe consequences beyond financial burden (Buttrick, Davidson and McGowan, 2016). Alzaabi (2025) provided a counterpoint by accepting the engineer's guilt but simultaneously urged an analysis of the broader systemic organisational culture and ethics surrounding it. Alharthi (2025) voiced the same concerns regarding erosion of trust towards information systems and emphasized that ethical considerations need to be integrated throughout the entire development process, not just towards the end.

There is a unified agreement and understanding that ethical responsibility is within a group. Developers, teams, and the leadership must construct an ecosystem that encourages ethical anticipation and thorough vetting during every phase of the Software Development Life Cycle (SDLC). Following ACM and BCS codes mean not only abiding legislation but casting strengthening faith to the society in technologies and its developers.

References

Association for Computing Machinery (2018) *ACM Code of Ethics and Professional Conduct*. [online] Available at: https://www.acm.org/code-of-ethics [Accessed 13 May 2025].

British Computer Society (2015) *BCS Code of Conduct*. [online] Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 13 May 2025].

Buttrick, H.G., Davidson, J. and McGowan, R.J. (2016) 'The skeleton of a data breach: The ethical and legal concerns', *Richmond Journal of Law and Technology*, 23(1), Article 2. Available at: https://scholarship.richmond.edu/jolt/vol23/iss1/2/ [Accessed 13 May 2025].

Cumbley, R. and Church, P. (2013) 'Is "Big Data" Creepy?', *Computer Law & Security Review*, 29(5), pp. 601–609. Available at: https://doi.org/10.1016/j.clsr.2013.07.007 [Accessed 13 May 2025].

Wright, D. and De Hert, P. (2012) *Privacy Impact Assessment*. Dordrecht: Springer.