Initial Post

Case Study: ACM Case on "Inadvertent Disclosure of Sensitive Data"

In this ACM case, an application that had not been thoroughly tested was pushed and, along with it, sensitive customer information was exposed by a software engineer blunder. This raises issues under ACM Code of Ethics (Association for Computing Machinery, 2018) as it concerns “Privacy” and in principle 1.6 states: “Respect privacy” and” Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks” which is Principle 2.5. In this case, the primary ethical failure is the lack of proper personal data custodianship.

Legally, such an incident may breach the UK’s Data Protection Act 2018 and the General Data Protection Regulation (GDPR), both of which require organisations to implement appropriate technical and organisational measures to protect personal data (Cumbley and Church, 2013). Imposing these regulations exposes the organization to significant financial penalties and reputational damage. From a socio-ethical perspective, customer trust and public confidence in digital systems may become detrimental.

The BCS Code of Conduct (British Computer Society, 2015) offers a parallel framework. It draws attention to the public interest protection (Clause 1) as well as the maintenance of competence and integrity (Clause 2). In this instance, both were neglected. Deficient care as shown by the engineer's actions which breach professional standards.

This case highlights sharp focus violation of ethical foresight along with testing robust processes within software development. Following and respecting both ACM and BCS codes guarantees computing professionals meet their societal and professional obligations.

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].

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.