reply by Craig Norris

A good read, thank you for the post. The ACM case about accidental data leaks does indeed show a serious failure to protect user privacy including regulations such as GDPR. The app was released without enough testing, breaking ACM rules that say developers must respect privacy and carefully check for risks (ACM, 2018). This mistake is part of a bigger problem in software development, where speed is often valued more than ethics. Buttrick et al. (2016) point out that data breaches don’t just cost money—they also damage public trust and put people’s personal information at risk.

References:

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

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/**

reply by Mohamed Alzaabi

Your analysis of the "Inadvertent Disclosure of Sensitive Data" case is both insightful and grounded in key ethical frameworks. You clearly connect the engineer’s oversight to violations of ACM Code Principles 1.6 and 2.5, highlighting the responsibility to respect privacy and evaluate risks thoroughly (ACM, 2018). I also appreciate how you tied this to the legal consequences under GDPR and the UK’s Data Protection Act—demonstrating how ethical lapses often lead to legal repercussions.

What stands out in your post is the link to the BCS Code of Conduct, particularly around public interest and professional competence. This dual-code comparison strengthens your argument that ethical awareness must be embedded at all stages of software development.

That said, I wonder if the responsibility lies solely with the individual engineer. Could this failure also reflect systemic issues, like organizational culture or lack of proper testing protocols? In such cases, shouldn't ethical responsibility be shared across teams and management, not just placed on the developer?

Your post makes a strong case for embedding ethical foresight into software practices, and I’d be interested to hear your thoughts on how companies can create more ethically resilient development environments.

reply by Shaikah Alharthi

The ACM case titled “Inadvertent Disclosure of Sensitive Data” highlights an ethical and legal issue of concern in software engineering that stems from a lack of thorough data custodianship and poor testing. This incident violates the ACM Code of Ethics, particularly the Principle 1.6 regard privacy. The software engineer released an application with incomplete testing which, in turn, resulted in the exposure of customer sensitive information. Additionally, he did not evaluate the complete system and attempted mitigations, which is a violation of Principle 2.5. A lapse of due care in the protection of user data is a basic expectation in professional computing, and in this case, User Data was neglected.

Legally, the breach appears to conflict with the UK Data Protection Act 2018, and the GDPR. These policies require businesses to implement appropriate organizational and technical measures safeguards that ensure the protection of private data. Not abiding these policies puts companies at high risk of being fined and suffering monetary losses as well as damage to their reputation down the road. This should be treated equally as important: the erosion of trust in digital platforms comes when users surrender control over their data, thus lower the public’s confidence in technology, and the governance of them.

The BCS Code of Conduct upholds this ethical position. Clause 1 focuses on protection of the public interest, while Clause 2 compels professionals to maintain competence and integrity. In this instance, both clauses were ignored. There is a lack of adequate testing and oversight by the engineer which indicates a lapse in professional responsibilities and suggests an overarching organizational problem with regard to quality control within the assurance processes.

This particular case illustrates the need to anticipate ethical boundaries and implement rigorous testing measures in software engineering. Following the ethical principles set by the ACM and BCS goes beyond legal and professional obligations. It also upholds the eroding faith in the technology and the technologists who claim to serve the users. Ethical adherence ought to be built into each phase within the development lifecycle so as to minimize the occurrence, as well as the consequences, of such breaches.