The ACM case study “Drones and Privacy” demonstrates how drone programmers introduced surveillance functions which obtain location  information from users without first obtaining permission (ACM, 2018). The malfunction does not stem from  the technology but rather from a lack of professional ethics. According to the ACM Code of Ethics, this situation breaks both Principle 1.2 (Avoid harm)  and 1.6 (Respect privacy). The security measures failed during the development process to protect the  personal information of users who are tracked in real-time through these systems.

This issue spans beyond the technical domain  as it has legal implications. The General  Data Protection Regulation (GDPR) states that all location data collection must receive user consent to avoid violating  data protection laws. The BCS Code of Conduct specifies that computing professionals must follow legal and regulatory requirements while  promoting public welfare (BCS, 2023). The BCS code requires professionals to comply with  all legal standards but the ACM code puts emphasis on ethical behavior instead.

This specific case study amplifies  current social anxieties about surveillance practices within the modern world. According to Zuboff (2019),  continuing to hide data collection processes from the public will diminish social trust and individual freedom.From a professional standpoint, computing practitioners must understand that delivering functional technology is not enough. Ethical foresight, legal awareness, and the ability to anticipate misuse are essential parts of their role.

This case is a clear example of how ethical blind spots can emerge in the gap between capability and accountability. Developers must move beyond the mindset of “can we build it?” to “should we build it this way?”—and that shift begins with professional ethics.

**References**

Association for Computing Machinery. (n.d.). Case Study: Drones and Privacy. Available at: https://www.acm.org/code-of-ethics/case-studies/drones-and-privacy (Accessed: 19 May 2025).

BCS. (2022). BCS Code of Conduct. Available at: https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/ (Accessed: 19 May 2025).

Calo, R. (2016). Robotics and the Lessons of Cyberlaw. *California Law Review*, 103(3), 513–563. Available at: https://doi.org/10.2139/ssrn.2402972 (Accessed: 19 May 2025).

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*, 3(2), 1–21. Available at: https://doi.org/10.1177/2053951716679679 (Accessed: 19 May 2025).

Zuboff, S. (2019). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.