Research Methods and Professional Practice April 2024

Discussion topic: 1 Codes of Ethics and Professional Conduct

My initial post:

I chose a case study from the ACM Code of Ethics to illustrate how a social media corporation violated user privacy by sharing private user information for targeted advertising without permission. The notion of privacy preservation and user transparency is emphasized in the ACM Code, which specifically mandates that professionals "avoid harm" and "respect privacy" (ACM Code, 2018). In this case, the transgression violated fundamental ethical duties, affecting the legal and social domains.

Jurisdictions differ in how they handle data privacy legally. For example, the GDPR of the European Union enforces stringent rules around data processing and user consent; failure to comply can result in hefty fines (Voigt & Bussche, 2017). But data privacy regulations in places like the U.S. are more disjointed, which leads to disparities in accountability and enforcement (Solove & Schwartz, 2019). The significance of ethical self-regulation is highlighted by this contradiction, particularly in non-jurisdictional circumstances where social expectations for data protection are nonetheless high despite potentially laxer legal requirements.

This and the British Computer Society's (BCS) Code of Conduct are similar in that they both stress professionalism and integrity, but BCS also emphasizes "public interest." According to BCS standards, members must "avoid causing risk or harm to society," which is consistent with ACM's position but specifically expands it to encompass public welfare (BCS Code of Conduct, 2021). This difference emphasizes how crucial it is for computing professionals to put ethical behavior above and beyond simple compliance, demonstrating a dedication to both professional integrity and societal trust.

Computing professionals that follow these codes of ethics not only stay out of trouble with the law but also keep their reputations intact, which promotes an ethically responsible culture in the sector (Moor, 1985). One's ethical development and commitment to professional integrity might be demonstrated by recording such reflections in an e-portfolio.

References:

- ACM Code of Ethics (2018)
- BCS Code of Conduct (2021)
- Moor, J. H. (1985). What is Computer Ethics? *Metaphilosophy*
- Solove, D., & Schwartz, P. (2019). *Information Privacy Law*
- Voigt, P., & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*

Post by Maria Ingold:

The Association for Computing Machinery (ACM) (N.D.) "Abusive Workplace Behaviour" case study discusses the breach of six codes from the ACM (2018) Code of Ethics and Professional Conduct.

Table 1 lists the key points violated in the case study, their respective ACM Code, and how they map to the British Computing Society (BCS) Code of Conduct.

TABLE 1 | Relevant ACM and BCS Codes

Case Study	ACM Code	BCS Code
Verbal abuse *(social, professionalism)*	**General Ethical Principles** Principle 1.1 Societal and human well-being	**You make IT for everyone** PUBLIC INTEREST 1) Due regard for well-being of others
Unprofessional communication *(professionalism)*	**Professional Responsibilities** Principle 2.2 Professional competence, conduct and ethical practice	**Show what you know, learn what you don't** PROFESSIONAL COMPETENCE AND INTEGRITY 5) Offer honest criticisms of work
Removal and blocking *(legal)*	**General Ethical Principles** Principle 1.5 Respect work and innovation	**Show what you know, learn what you don't** PROFESSIONAL COMPETENCE AND INTEGRITY 6) Avoid reputation damage by malicious action

Targeting women *(legal)*	**General Ethical Principles** Principle 1.4 Be fair and avoid discrimination	**You make IT for everyone** PUBLIC INTEREST 3) Without discrimination
Failed psychological safety *(social, professional)*	**Professional Leadership Principles** Principle 3.3 Manage to enhance working life	**Respect the organisation or individual you work for** DUTY TO RELEVANT AUTHORITY 3) Professional responsibility for those under your supervision
Failure to support ethical principles *(social, professional, legal)*	**Professional Leadership Principles** Principle 3.4 Apply and support Code policies and processes	**Keep IT real. Keep IT professional. Pass IT on.** DUTY TO THE PROFESSION 2) Develop, use, and enforce professional standards

Comparing the two codes, the ACM uses the word “ethic”, while the BCS does not. Furthermore, ACM seems more concerned with psychological safety, professional leadership, and respect for the individual, while BCS appears to focus more on legal compliance. For instance, the BCS discrimination wording appears mostly designed to comply with the UK’s 2010 Equality Act (Wadham, 2021). However, as the ACM is a global organisation, it makes sense that its wording is more general.

Psychological safety at work is key to facilitating performance, goal achievement, successful teamwork, knowledge sharing, and innovation (Edmondson & Bransby, 2023). While the abusive behaviour of the team lead violates ethical and professional principles, the enabling behaviour of the team manager perpetuates it. Bancroft (2003) describes abuse as coming from entitlement, control, and ownership, and notes that changing abusive behaviour requires calling it out by peers and superiors, as well as being held accountable with consequences. As raised by the ACM, having and enforcing ethical policies would help the team manager to enable psychological safety.

References

ACM (2018) *ACM Code of Ethics and Professional Conduct*. Available from: https://ethics.acm.org/ [Accessed 3 May 2024].

ACM (N.D.) *Case: Abusive Workplace Behavior - ACM Ethics*. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-abusive-workplace-behavior/ [Accessed 3 May 2024].

Bancroft, L. (2003) *Why Does He Do That?: Inside the Minds of Angry and Controlling Men*. Penguin Publishing Group.

Edmondson, A.C. & Bransby, D.P. (2023) Psychological Safety Comes of Age: Observed Themes in an Established Literature, *Annual Review of Organizational Psychology and Organizational Behavior* 10(10): 55–78. DOI: https://doi.org/10.1146/ANNUREV-ORGPSYCH-120920-055217/CITE/REFWORKS.

Wadham, J. (2021) *Blackstone's guide to the Equality Act 2010*. 4th ed. Oxford University Press. DOI: https://doi.org/10.1093/oso/9780198870876.001.0001 [Accessed 3 May 2024].

My response:

Hello Maria,

I really enjoyed your post,as I think the subtle distinctions between the ACM and BCS codes are clearly shown in this well-written analysis of yours. The study of Edmondson and Bransby (2023) highlights the significance of psychological safety in creating a healthy work environment.

It's also interesting how you connected the BCS's UK-specific legal compliance, especially in anti-discrimination, with the ACM's more universally applicable ethical approach. The conversation is enhanced by Bancroft's (2003) viewpoint on the causes of abusive behavior and the need for accountability, which highlights the part moral policies play in fostering a respectful workplace culture.

Overall really insightful post!

Post by Steve Fisher:

I have chosen to analyse the case of Malware Disruption and have assumed that the enforcement took place within the UK.

Rogue Services, in providing a platform for fraudulent services and refusing requests to remove such services are in breach of the following sections of the British Computer Society (BCS) Code of Conduct (BCS, 2022):

- Sections 1 (a) and (b)
- Section 2 (f)
- Section 4 (a), (c) & (d)

The security vendors involved, whilst acting to uphold the principles of part 1(a), are clearly in breach of part 1(b) and possibly part 2(f) as legitimate customer data was deleted. Additionally, depending on your point of view, these vendors could also be in breach of parts 4(a) and (c) since the creation and distribution of malware in these circumstances presents an ethical dichotomy (Withers et al., 2020). Cobb & Lee (2014), suggest that the use of malicious code for any reason should be discouraged due to unintended consequences, loss of control and possible legal challenges. More recently however, researchers have concluded that there is need for this kind of offensive security practice (Conteh, 2021) with a focus on developing effective techniques (Almehmadi et al., 2022) and frameworks for training in their application(Heiding & Lagerström, 2020).

Ethical considerations notwithstanding, it is important to note that the security vendors and government organisations must have acted lawfully. Whilst Part 5 of the Investigatory Powers Act (2016) allows for 'Equipment Interference' by authorised persons in possession of a valid warrant. The control of who, and in what circumstances such warrants can be issued are tightly controlled and outlined in Part 5 sections 102-128. Without such authorisation, the entities involved including any law enforcement, could be found in breach of the Computer Misuse Act (1990) Sections 1, 3 and 3A. In the absence of any breach of criminal statute, legitimate users of Rogue Services may have a case in civil law under the tort of negligence, to sue for damages as a result of their data being destroyed. The only caveat being is that at present, this is a legal grey area since digital files are not yet recognised as property. However, there have been moves in this direction in judgements by the courts (Michaels & Millard, 2022) and the UK Government are currently consulting on draft legislation to allow digital assets to be recognised as property in law (Law Commission, 2024).

References

Almehmadi, L., Basuhail, A., Alghazzawi, D. and Rabie, O. (2022). Framework for malware triggering using steganography. *Applied Sciences*, *12*(16), p.8176.

BCS. (2022). CODE OF CONDUCT FOR BCS MEMBERS. Available from https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 3rd May 2024].

Cobb, S. & Lee, A. (2014). Malware is called malicious for a reason: The risks of weaponizing code. Available from: https://doi.org/10.1109/CYCON.2014.6916396

Computer misuse Act. (1990). United Kingdom. Available from https://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 3rd May 1990].

Conteh, N. (2021). Ethical Hacking, Threats, and Vulnerabilities in Cybersecurity. Available from: https://doi.org/10.4018/978-1-7998-6504-9.CH001

Heiding, F. & Lagerström, R. (2020). Ethical Principles for Designing Responsible Offensive Cyber Security Training. Available from: https://doi.org/10.1007/978-3-030-72465-8_2

Investigatory Powers Act 2016 (c. 25). (2016). United Kingdom. Available from: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [Accessed 3rd May 2024].

Law Commission, 2024, Digital assets as personal property Short consultation on draft clauses. London. Law Comission. Available from: https://cloud-platform-e218f50a4812967ba1215eaecede923f.s3.amazonaws.com/uploads/sites/30/2024/02/Feb-2024-digital-assets-and-personal-property-CP.pdf [Accessed 3rd May 2024].

Michels, J.D. & Millard, C. (2022). THE NEW THINGS: PROPERTY RIGHTS IN DIGITAL FILES? *The Cambridge Law Journal*. 81(2):323-355. Available from: https://doi.org/doi:10.1017/S0008197322000228 [Accessed 3rd May 2024].

Withers, K., Parrish, J., Ellis, T. & Smith, J. (2020). Vice or virtue? Exploring the dichotomy of an offensive security engineer and government “hack back” policies. Proceedings of the 53rd Hawaii International Conference on System Sciences. Available from: https://doi.org/10.24251/HICSS.2020.224

My answer:

Dear Steve,

Particularly pointing out the moral difficulties associated with using malware for security, your post and thoughts are interesting and valuable points. Cobb & Lee's (2014) exploration of the dangers of weaponizing programming highlights how difficult it is to find a balance between the necessity of cybersecurity and ethical responsibility. Even with a legitimate warrant under the Investigatory Powers Act (2016), the possible violation of the Computer Misuse Act (1990) and the BCS Code of Conduct serves as an example of the legal restrictions that apply to offensive security measures. Furthermore, your observation regarding the changing legal standing of digital assets offers an intriguing viewpoint on possible civil lawsuits under negligence law. This new field has the potential to completely rethink the definition of data rights and obligations in situations where legitimate users are accidentally harmed.

My summary post:

In this discussion, I examined the ACM Code of Ethics in connection with a social media company's infringement of user privacy through unapproved data sharing during our conversation on computer ethics. This breach affects both the social and legal spheres and emphasizes the ACM's need that computing professionals "avoid harm" and preserve privacy. While data privacy rules in other countries, such as the U.S., are still less uniform, the GDPR in the EU imposes stringent privacy protections with significant penalties (Voigt & Bussche, 2017; Solove & Schwartz, 2019). This legal discrepancy highlights how crucial moral self-regulation is in areas with diverse privacy regulations.

Analyzing ACM's "Abusive Workplace Behavior" case study, Maria Ingold also highlighted how ACM guidelines prioritize psychological safety and respect for individuals, in contrast to the British Computer Society's (BCS) Code of Conduct, which focuses on legal compliance, particularly with regard to anti-discrimination laws like the UK's Equality Act (Wadham, 2021; Edmondson & Bransby, 2023).

Steve Fisher looked into malware disruption within the BCS Code and pointed out that security measures might cause ethical problems even when they have legal authorization, particularly when they are subject to the Investigatory Powers Act (2016). The study of Cobb and Lee (2014) cautions against the unexpected dangers of malware, but more recent studies encourage offensive security in controlled situations (Conteh, 2021).

All things considered, these posts demonstrate how the BCS and ACM Codes promote professionalism, but they place different emphasis on it. Global standards are met by ACM's wide ethical approach, but BCS places more emphasis on UK-specific legal compliance, highlighting the need for computing ethics to adjust to both local and global contexts.

References:

- ACM Code of Ethics (2018)
- BCS Code of Conduct (2021)
- Voigt, P., & Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR)*
- Solove, D., & Schwartz, P. (2019). *Information Privacy Law*
- Wadham, J. (2021). *Blackstone's guide to the Equality Act 2010*
- Edmondson, A.C. & Bransby, D.P. (2023)
- Cobb, S. & Lee, A. (2014). *Malware is called malicious for a reason*