Collaborative Discussion

Initial Post

The case study on Malware Disruption provided by the ACM (2024a) is an important example that shows the need for computing professionals to act in a way that is in accordance with the ethical, social and legal requirements. Without acting in this way, our services will be ineffective and those who rely on us, such as customers and stakeholders, will lose faith in our abilities.

An identified breach in the ACM Code of Ethics (2024b) relates to the company in question, Rogue Services, knowingly hosting malware and spam. ACM identified that this breaches both Principles 1.1 (contribute to society and to human well-being, acknowledging that all people are stakeholders in computing) and 1.2 (do no harm) due to the company knowingly doing this, even when the industry spoke to them and advised against this. The breaches in the ACM code also correlate to section 4a of the BCS Code of Conduct (2022), which states that computing professionals should "accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute".

From a legal standpoint, Rogue Services could potentially be liable for prosecution in line with Section 2 of the Computer Misuse Act 1990. This is due to the company being in breach of Section 2(1)(a), which states that "a person is guilty of an offence under this section if he commits an offence under section 1 above (“the unauthorised access offence”) with intent to facilitate the commission of such an offence (whether by himself or by any other person)" (UK Government, 1990). Given that Rogue Services are knowingly allowing malware to be hosted by them, they are actively facilitating this, thus being complicit.

The case study highlights another potential breach in section 1.2 of the ACM Code of Ethics, but in regards to those who forced Rogue Services offline. The case study states that the worm used to take Rogue Services down was intentionally designed to cause harm, however there was a level of ethical justification (ACM, 2024b). This raises an interesting point with regards to how the same application of computing

can have different ethical and social implications when viewed within different contexts. It could be argued that a "good faith" actor performing this kind of attack on a "bad faith" actor is in keeping with section 1a of the BCS Code of Conduct (2022), which asserts that computing professionals should "have due regard for public health, privacy, security and wellbeing of others and the environment". Given that the attack to take down Rogue Services could be deemed as necessary for the protection of the privacy and security of the general population, an argument can be made that a knowingly harmful attack could be in keeping with the ethical spirit of computing.

What this case study shows is that the social, legal and ethical implications of computing are not clearly just black and white, but rather a spectrum that requires criticality, nuance and self reflection to ensure that professionals act in the interest of the profession.

References

ACM (2024a) ACM Code of Ethics and Professional Conduct. Available from: https://www.acm.org/code-of-ethics [Accessed 29 October 2024].

ACM (2024b) Using the Code: Malware Disruption. Available from: https://ethics.acm.org/code-of-ethics/using-the-code/case-malware-disruption [Accessed 29 October 2024].

BCS (2022) Code of Conduct for BCS Members. Available from: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf [Accessed 29 October 2024].

Computer Misuse Act (1990), c. 18. Available from: https://www.legislation.gov.uk/ukpga/1990/18/contents [Accessed 29 October 2024].

Response To Peer

Good afternoon [Student Name],

I enjoyed reading your analysis of the case study regarding Dark UX Patterns.

Having read your analysis and reflected on the position of Stewart in this case, it's pretty clear to correlate with his sentiments and the ethical breaches you have identified regarding this. However, in my opinion, the implications of this go even further and point towards potential legal ramifications.

Luguri and Strahilevitz (2021) provide some good insight into the legalities of Dark UX Patterns when assessed through the lens of US consumer laws. The assert that since 1938, the Federal Trade Commission Act has language that prohibits “unfair or deceptive acts or practices in or affecting commerce”. Given that the case study in question is knowingly pushing customers towards a default product in a deceptive way, there is a case to be made that the company in question is indeed breaching this law, and could face criminal prosecution.

I think it is important to keep in mind that as computing professional, we do not operate in an isolated bubble. While we aim to act in accordance with the ethics codes you have highlighted, we must also remain mindful that we are still subject to the laws and ethical implications of those industries that we may work closely with. When we create an e-commerce site, we become part of the commerce industry for example. Likewise, if we were to develop a streaming platform, we intersect with intellectual property and entertainment sectors.

Highlighting some of these key legal intersections would have strengthened your analysis of the implications that Dark UX Patterns can have on the computing profession, however the work you have provided already does a very good job in addressing the strong ethical implications of what we do as professionals.

Reference

Luguri, J., and Strahilevitz, L.J. (2021) ‘Shining a Light on Dark Patterns’, Journal of Legal Analysis, 13(1), pp. 43–109. Available from: https://doi.org/10.1093/jla/laaa006 [Accessed 29 October 2024].

Summary Post

The remarks of individuals within this forum have highlighted that the examples shown within the ACM case studies do have very real consequences on professionals, organisations and the wider public at large.

As one of my colleagues highlighted, it is important to consider the bigger picture with regards to how we assess the social, legal and ethical aspects of computing. These incidents do not exist in isolation, and the nature of our chosen profession means that we have to be constantly aware of the impacts of our actions.

Turning to the particular case study highlighting in my initial post, reflections from colleagues have correlated with my particular views on this. It is clear that the majority believe that Rogue Services had acted in a way that contravenes the ethical and legal standards that computing organisations should hold themselves to. Colleagues also agreed that those who took the site down acted in a morally ambiguous way, agreeing with me that the nature of ethical and social issues with regards to computing aren't always black and white.

All of the above can be found within the forum for collaborative discussion 1.