Collaborative Learning Discussion 1

My Submission

he case 'Dark UX Patterns' illustrates a clear instance of employing dark UX patterns, which not only compromise the ethical integrity of design but also potentially infringe upon legal and social standards. The application of an ethics code to this situation highlights various failures, both moral and professional, on the part of the computing professionals involved, and raises concerns about compliance with broader legal and social expectations.

Impact on Legal Issues

Consumer Protection Laws: Many jurisdictions have laws designed to protect consumers from misleading and deceptive practices. The implementation of dark UX patterns, such as misleading users into unwanted subscriptions or purchases, may violate these laws, exposing the company to legal action and financial penalties.

Accessibility Requirements: The mentioned design changes also neglect accessibility standards, particularly for visually impaired users. This oversight can lead to violations of laws such as the Americans with Disabilities Act (United States, 1990) or the Equality Act 2010 (Great Britain, 2010).

Impact on Social Issues

Trust and Reputation: Employing deceptive practices undermines user trust, a crucial component of the social contract between a business and its customers. This erosion of trust can have long-lasting negative impacts on the company’s reputation and its relationship with users.

Digital Inclusion: The scenario highlights a disregard for inclusivity, particularly in failing to accommodate users with visual impairments. Such practices contribute to a wider societal issue of digital exclusion, where certain user groups are marginalized due to design decisions.

Professionalism of Computing Professionals

Ethical Standards: The British Computer Society (BCS, 1957) Code of Conduct emphasises the importance of acting with integrity, in the public interest, and to avoid actions that harm others. The actions described in the scenario violate these principles by intentionally deceiving users for financial gain and disregarding the impact on vulnerable groups.

Responsibility to Challenge: The BCS Code of Conduct also encourages professionals to challenge and report inappropriate behaviour in the workplace. Stewart’s initial challenge to the design changes reflects this responsibility, but the lack of further action points to a broader failure within the company to uphold ethical standards.

Comparison to the British Computer Society (BCS)

The British Computer Society (BCS), the Chartered Institute for IT, sets out ethical guidelines that prioritise the public good, the avoidance of harm, and the advancement of public understanding of computing and its consequences. The situation described contravenes several BCS ethical principles:

Public Interest: The BCS emphasises acting in the public interest, which includes respecting user privacy and avoiding deceit. The deceptive UX patterns directly conflict with this principle.

Professional Competence and Integrity: The BCS advocates for professional competence and integrity, requiring members to reject any business practice that might discredit the profession. The acceptance and implementation of dark UX patterns by computing professionals demonstrate a lack of integrity and professionalism.

Duty to Relevant Authority: While professionals have a duty to follow lawful and ethical instructions from their employers or clients, they also have a responsibility to push back against requests that would lead to unethical outcomes. The scenario illustrates a failure to adequately fulfil this duty.

In conclusion, the application of dark UX patterns in this case raises significant ethical, legal, and social concerns. It highlights a failure on the part of computing professionals to adhere to established codes of ethics, such as those advocated by the BCS, which aim to ensure that technology serves the public good, respects user autonomy, and promotes inclusivity. These professionals must navigate the balance between client demands and ethical standards, striving to uphold principles that protect and benefit users and society at large.

References

Americans with Disabilities Act (ADA) of 1990:

- United States. (1990). *Americans with Disabilities Act of 1990*, Public Law 101-336. Available at: https://www.ada.gov/pubs/adastatute08.htm (Accessed: [06 April 2024]).

Equality Act 2010:

- Great Britain. (2010). *Equality Act 2010*. Available at: Equality Act 2010 (Accessed: [06 April 2024]).

British Computer Society (BCS) Code of Conduct:

- British Computer Society. (1957). *Code of Conduct for BCS Members*. Available at: BCS Code of Conduct for members - Ethics for IT professionals | BCS (Accessed: [06 April 2024]).

Peer Response

Hi Haaris,

Your analysis of the 'Malware Disruption' case, provides a detailed examination of the complexities surrounding cybersecurity interventions. You've highlighted the tension between the ethical duties to prevent harm, respect privacy, and adhere to legal standards, embodying the classic ethical conundrum of ends versus means.

The addition of Nietzsche’s quote in this context is particularly striking, bringing to light the ethical vigilance necessary when undertaking cybersecurity measures. These actions, though intended to safeguard, may inadvertently cross ethical lines or yield unintended consequences. This philosophical perspective enriches the discussion, spotlighting the moral intricacies faced by professionals in the computing sector.
Indeed, as you've noted, the quest for security and justice in the digital sphere must not compromise the ethical principles found in professional codes of conduct. This case calls for a re-examination of these principles, given the unique challenges posed by cyber threats and the international nature of the internet, which often eclipses the pace of legal framework development.

Your conclusion aptly advocates for stringent ethical guidelines and legal frameworks capable of evolving alongside technological progress and the changing landscape of cybersecurity. This necessity is paramount not only for guiding professionals in their endeavours but also for ensuring that cybersecurity practices align with societal values and legal norms.
To enrich your analysis further, it would be advantageous to consider the roles that various stakeholders, including governments, international bodies, and the private sector, play in shaping and enforcing these frameworks.

To summarise, your analysis offers a comprehensive and nuanced perspective on the ethical, legal, and societal dimensions of cybersecurity interventions. It underscores the critical need for ethical introspection and professional accountability in navigating the complex and sometimes murky realm of digital justice and security.