Collaborative Discussion 1

Initial Post

Medical implant devices have been increasing in use over the past few decades and are predicted to advance at an extraordinary rate in the future. The ease of monitoring and function control have improved access to healthcare, lowered the costs to patients and providers as well as provided an improved standard of care(Li *et al.*, 2021).

I have focused on the medical startup company Corazon for the purposes of this study (ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics, 2018). They created an implantable device to monitor cardiac activity, alerting the patient and medical providers to potential issues as they present, thus reducing the chance of heart failure and subsequent death.

The company followed all prerequisites for launch, including gaining regulatory approval from all licensing authorities, as well as following current best practices for development. Additional safeguards included limiting connectivity to only short-range communication as well as creating a bug bounty program to identify potentially missed security threats. An independent threat analyzer detected a potential security issue and reported the threat to the company. The company then performed an in-depth security risk assessment and concluded that while there was a threat, the risk posed was deemed to be low. Subsequent research to mitigate the threat entirely is ongoing.

Concern	ACM Principle (Acm.org, 2021)	BCS Principle (BCS, THE CHARTERED INSTITUTE FOR IT CODE OF CONDUCT FOR BCS MEMBERS, 2015)
Charity work as well as goal to monitor and improve healthcare to patients	**Principle 1.1** Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing	**Principle 1.d**- promote equal access to the benefits of IT and seek to promote the inclusion of all sectors in society wherever opportunities arise.
Gained regulatory approval for operation from all districts in which the device will be offered	**Principle 2.3-** Know and respect existing rules pertaining to professional work	**Principle 2.d**- ensure that you have the knowledge and understanding of Legislation and that you comply with such Legislation, in carrying out your professional responsibilities

		Principle 3.a- carry out your professional responsibilities with due care and diligence in accordance with the Relevant Authority's requirements whilst exercising your professional judgement at all times
Created a bug-bounty program to allow for external audits and threat analysis, as well as engaged with researcher who identified a potential risk	**Principle 2.5-** Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks	**Principle 2.e**- respect and value alternative viewpoints and seek, accept and offer honest criticisms of work
Utilized existing cryptographic principles to design device security systems	**Principle 2.6-** Perform work only in areas of competence	**Principle 2.a**- only undertake to do work or provide a service that is within your professional competence. Principle 2.b- NOT claim any level of competence that you do not possess
Utilized cryptography, disclosed potential vulnerabilities and addressed issues when discovered	**Principle 2.9-** Design and implement systems that are robustly and usably secure	**Principle 2.c**- develop your professional knowledge, skills and competence on a continuing basis, maintaining awareness of technological developments, procedures, and standards that are relevant to your field.
Ongoing commitment to security and improvement	**Principle 3.7-** Recognize and take special care of systems that become integrated into the infrastructure of society	**Principle 2.c**

References

ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics. (2018). *Case: Medical Implant Risk Analysis - ACM Ethics*. [online] Available at:

https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 15 Mar. 2022].

Acm.org. (2021). *The Code affirms an obligation of computing professionals to use their skills for the benefit of society.* [online] Available at: https://www.acm.org/code-of-ethics [Accessed 19 Mar. 2022].

BCS, THE CHARTERED INSTITUTE FOR IT CODE OF CONDUCT FOR BCS MEMBERS. (2015). [online] Available at: https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf.

Li, P. *et al.* (2021) 'From Diagnosis to Treatment: Recent Advances in Patient-Friendly Biosensors and Implantable Devices', *ACS Nano*, 15(2), pp. 1960–2004. doi: 10.1021/acsnano.0c06688.

Peer Response 1

Hi, I found your post on dark UX patterns informative, and you have comprehensively summarized the issues presented in the case study.

I researched the topic further, and interestingly discovered a systematic review identifying 22 different types of dark UX patterns. I found multiple instances of which I personally had fallen victim to, including(Cara, 2019):

-price comparison prevention: when searching for a product, it is made difficult to ascertain accurate price comparisons, thus resulting in the consumer falling victim to overpaying for a product or service.

- sharing the article: articles or information is hidden until the user shares the link with multiple other users, likely to increase web traffic and ad revenue.

-hard opt-out: difficulty or unreasonable steps required to stop receiving notifications or end a subscription, often leading to the user simply abandoning the process as it is too complicated.

- false urgency: creating a timed perceived benefit, after which the user would essentially lose out on an offer, when in reality, the discount or benefit offered is not what has been advertised.

I also discovered that dark UX pattern designs have been used by large companies like LinkedIn and Google(Narayanan *et al.*, 2020), however, both companies were fined for this practice.

In reality, regulations are tightening relating to the use of dark UX patterns, but developers and designers need to incorporate ethics into their design, even if this may jeopardize the relationship with the client(Narayanan *et al.*, 2020).

References

Cara, C. (2019) 'Dark Patterns in the Media: a Systematic Review', *Network Intelligence Studies*, VII(14), pp. 105–113.

Narayanan, A. *et al.* (2020) 'Dark Patterns Past, Present, and Future', *Association for Computing Machinery New York, NY, United States*, (30 April 2020), pp. 1–25.

Peer Response 2

Hi Man Sze, thank you for your informative post. I would be very interested to see what steps the organization has taken to modify Max's behaviour. The particular instance that stands out to me, is the "history of targeting only women team members" (ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics, 2018), which screams to me of sexist behaviour.

In my opinion, this is particularly heinous behaviour which transcends the ACM and BCS codes of conduct. Gender discrimination is and has been illegal for the better part of 20 years, and it is criminal that in this day and age, women are perceived as less competent than men, and are the subject of such discrimination. This should be viewed in the same light as racism and speaks to a broader issue.

In my research, I discovered instances of gender discrimination by major tech companies, such as Apple, Google and Walmart. Many of the complainants approached the courts for a resolution, and these companies were found guilty of gender discrimination (Mann, 2020).

Extensive research has shown that women are frequently underpaid by around 20% when compared to their male counterparts (Arredondo Advisory Group, 2019). Only 21% of high executive positions in IT were occupied by females. A staggering 39% of females encountered gender bias in their workplaces (Botella *et al.*, 2019). The number of female IT graduates has also been declining, likely due to the negative workplace conditions.

I believe the problem starts with Max, and people like Max. In order for real change to occur, people like Max need to be removed from their positions as they are hindering advancement and equal opportunities. I would hope that in this fictitious case, Diane would approach the courts for a legal solution. This would undoubtably assist other Diane's who face this sort of issue daily.

References

ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics. (2018). *Case: Abusive Workplace Behavior - ACM Ethics*. [online] Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-abusive-workplace-behavior/ [Accessed 20 Mar. 2022].

Arredondo Advisory Group. (2019). *The Invisible Types of Gender Discrimination in the Workplace and How to Address Them | Arredondo Advisory Group*. [online] Available at: https://www.arredondoadvisorygroup.com/2019/07/11/the-invisible-types-of-gender-discrimination-in-the-workplace-and-how-to-address-them/ [Accessed 20 Mar. 2022].

Botella, C. *et al.* (2019) 'Gender diversity in STEM disciplines: A multiple factor problem', *Entropy*, 21(1), pp. 1–17. doi: 10.3390/e21010030.

Mann, J. (2020) 'Does Gender Discrimination Still Exist Today?', *Csustan.Edu*. Available at: https://www.csustan.edu/sites/default/files/groups/University Honors Program/Journals_two/dis_mann_jasmine.pdf.

Summary Post

Over the course of the collaborative discussion, my colleagues and I have summarized informative case studies relating to the ACM code of ethics. In my view, the case of abuse in the workplace was perhaps the most significant, as it contained elements of gender discrimination. Cases of this nature need to be dealt with as decisively as possible to prevent reoccurrence (ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics, 2018).

The Dark UX patterns case is also of concern, as it is highly prevalent in today's society, and deliberately aims to mislead or misdirect consumers to increase revenue. This is unethical behaviour, which can be dealt with by enforcing the ACM and BCS code of conducts on developers and customers(Cara, 2019; Narayanan *et al.*, 2020).

I found that the Corazon medical implants case was an example of a company committed to the ACM and BCS codes of conduct, with an ethical and morally unambiguous agenda. The company acted in an exemplary manner, with allowing 3rd party audits, following regulatory procedures, instituting thorough investigations and committing to improving security to benefit the users of the device (ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics, 2018).

A key take home point raised by a colleague, was that we, as future IT professionals, should investigate the ethics policy of the company prior to joining its workforce (Obayemi K, 2022).

References

ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics. (2018). *Case: Abusive Workplace Behavior - ACM Ethics*. [online] Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-abusive-workplace-behavior/ [Accessed 26 Mar. 2022].

ACM Ethics - The Official Site of the Association for Computing Machinery's Committee on Professional Ethics. (2018). *Case: Medical Implant Risk Analysis - ACM Ethics*. [online] Available at: https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/ [Accessed 26 Mar. 2022].

Cara, C. (2019) 'Dark Patterns in the Media: a Systematic Review', *Network Intelligence Studies*, VII(14), pp. 105–113.

Narayanan, A. *et al.* (2020) 'Dark Patterns Past, Present, and Future', *Association for Computing Machinery New York, NY, United States*, (30 April 2020), pp. 1–25.

Obayemi K, (2022). *RMPP_PCOM7E March 2022 A: Initial Post*. [online] Available at: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=300967 [Accessed 26 Mar. 2022].