



Collaborative Discussion 1 (Ethics and Morality)

**Course:** MSc Computer Science

**Module:** Research Methods and Professional Practice

**Assignment:** Collaborative Discussion 1 (Ethics and Morality) – Peer Responses

**Date:** Saturday 28th May 2022

**Student ID:** 126853

## Peer Response 1:

In response to:



Aidan Curley

### Initial Post

75 days ago

2 replies



Last 66 days ago

## Malicious Inputs to Content Filters

I have chosen the case study of Blocker Plus, a US-based content filter which helps prevent underage internet users from accessing certain materials, because I have strong, sometimes conflicting, personal views on the topic of censorship and freedom of information.

Blocker Plus was used to keep publicly accessible computers in schools and libraries safe for children. It maintained a central repository listing material the U.S. Children's Internet Protection Act deemed illegal and unsuitable for children.

The problem with this approach was that it required constant costly maintenance to keep the blacklisted materials up-to-date. As an alternative, they allowed home users to add materials to the list, and designed a machine-learning algorithm to automatically update the blacklist.

Some consumers realised that this could be manipulated and organised groups to add materials that went against their personal beliefs, including topics like vaccination and sexual preference, effectively censoring other users from accessing materials not actual under the jurisdiction of the CIPA.

The company uncovered this, but chose to keep quiet about it, hoping the algorithm would work itself out.

Action	ACM	
Didn't fully analyse or predict the risks of using the ML algorithm for censorship	2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.	3.1 carry out your professional responsibilities with due care and diligence in accordance with the relevant authority's requirements while exercising your professional judgement at all times;

Didn't prevent its misuse	2.9 Design and implement systems that are robustly and usably secure.	
Blocked useful legal information about vaccines from being accessed	1.2 Avoid harm.	
Discriminated against the gay and lesbian communities	1.4 Be fair and take action not to discriminate.	1.3 conduct your professional activities without discrimination on the grounds of sex, sexual orientation, marital status, nationality, colour, race, ethnic origin, religion, age or disability, or of any other condition or requirement;  2.6 avoid injuring others, their property, reputation, or employment by false or malicious or negligent action or inaction;
Hid the truth from the users	1.3 Be honest and trustworthy.  2.4 4 Accept and provide appropriate professional review.  2.7 7 Foster public awareness and understanding of computing, related technologies, and their consequences.	3.5 NOT misrepresent or withhold information on the performance of products, systems or services (unless lawfully bound by a duty of confidentiality not to disclose such information), or take advantage of the lack of relevant knowledge or inexperience of others.  2.5 respect and value alternative viewpoints and seek, accept and offer honest criticisms of work;  4.1 accept your personal duty to uphold the reputation of the profession and not take any action which could bring the profession into disrepute;
Software misused in educational context	3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.	3.1 carry out your professional responsibilities with due care and diligence in accordance with the relevant authority's requirements while exercising your professional judgement at all times;

REFERENCES:

Association for Computing Machinery, 2018. ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics> [Accessed 13 March 2022].

BCS The Chartered Institute for IT, 2021 The Code of Conduct. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 13 March 2022].

Reply

Post:

Hi Aidan,

You've picked an interesting case study, which highlights the bias that can be inherently present in user-trained ML algorithms and therefore causing unintended censorship. Over recent years, there have been many cases that have demonstrated the manipulability of ML algorithms based on training data, with one large example being the AI scoring system built into Amazon's recruiting processes, which favoured male applicants (Dastin, 2018). I believe that Blocker Plus should have combined reactive feedback reports (ACM, 2018) along with a stage of human moderation and decision making, which is the same process followed by Facebook (Vincent, 2020).

Although such an approach would still require a level of human intervention in the material blacklisting approach, it would have prevented Blocker Plus from breaching item 1C of the BCS Code of Conduct, as they had indirectly discriminated on the grounds of sexual orientation and suppression of legitimate resources (BCS, 2021), amongst other breaches of the ACM/BCS codes. It could also be considered that the behaviour would constitute a breach of the Equalities Act, as well as the individual policies within the educational settings that were using the software.

As Section 4.1 of the BCS Code of Conduct requires individuals/organisations to uphold the reputation of the profession, do you believe that Blocker Plus could have changed their processes (or acted in a more transparent manner) to prevent the misconceptions of technology that would likely arise from their failures?

#### References:


Association for Computing Machinery. (2018) Case: Malicious Inputs to Content Filters. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-malicious-inputs-to-content-filters/> [Accessed 20th March 2022].

British Computing Society. (2021) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 20th March 2022].

Dastin, J. (2018) Amazon scraps secret AI recruiting tool that showed bias against women. Available from: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> [Accessed 20th March 2022].

Vincent, J. (2020) Facebook is now using AI to sort content for quicker moderation. Available from: <https://www.theverge.com/2020/11/13/21562596/facebook-ai-moderation> [Accessed 20th March 2022].

## Screenshot:



Post by [Kieron Holmes](#)  
Peer Response

68 days ago

Hi Aidan,

You've picked an interesting case study, which highlights the bias that can be inherently present in user-trained ML algorithms and therefore causing unintended censorship. Over recent years, there have been many cases that have demonstrated the manipulability of ML algorithms based on training data, with one large example being the AI scoring system built into Amazon's recruiting processes, which favoured male applicants (Dastin, 2018). I believe that Blocker Plus should have combined reactive feedback reports (ACM, 2018) along with a stage of human moderation and decision making, which is the same process followed by Facebook (Vincent, 2020).

Although such an approach would still require a level of human intervention in the material blacklisting approach, it would have prevented Blocker Plus from breaching item 1C of the BCS Code of Conduct, as they had indirectly discriminated on the grounds of sexual orientation and suppression of legitimate resources (BCS, 2021), amongst other breaches of the ACM/BCS codes. It could also be considered that the behaviour would constitute a breach of the Equalities Act, as well as the individual policies within the educational settings that were using the software.

As Section 4.1 of the BCS Code of Conduct requires individuals/organisations to uphold the reputation of the profession, do you believe that Blocker Plus could have changed their processes (or acted in a more transparent manner) to prevent the misconceptions of technology that would likely arise from their failures?

References:

Association for Computing Machinery. (2018) Case: Malicious Inputs to Content Filters. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-malicious-inputs-to-content-filters/> [Accessed 20th March 2022].


British Computing Society. (2021) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 20th March 2022].

Dastin, J. (2018) Amazon scraps secret AI recruiting tool that showed bias against women. Available from: <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G> [Accessed 20th March 2022].

Vincent, J. (2020) Facebook is now using AI to sort content for quicker moderation. Available from: <https://www.theverge.com/2020/11/13/21562596/facebook-ai-moderation> [Accessed 20th March 2022].

## Peer Response 2:

### In response to:



[Lewie Seneviratne](#)

**Initial Post**  
69 days ago

2 replies  
Last 62 days ago

The implantable heart health monitoring device developed by a medical technology startup Corazón and the vulnerability in the wireless connectivity discovered by an independent researcher is considered as a case study for conducting the risk analysis based on the ACM Code of Ethics (CoE) and the BCS Code of Conduct (CoC).

The case study illustrates the application of all the statements from the BCS Code of Conduct (CoC).

The ACM's principle 1.1 (contribute to society and human wellbeing) and BCS's public interest are illustrated by Corazón's charitable work to supply their medical products free or reduced access to patients living below the poverty line. Hence, Corazón's charitable work reflects their increased stewardship towards the quality of life of all people and public health.

While ensuring the safety of the data via encrypted data storage and cryptographic algorithms, led data transfers supports ACM's principle 2.9 (robustly and useably secure system designs); the open bug bounty program exemplifies Corazón's commitment to developing professional knowledge, skills and competence, and the willingness to respect and value alternative viewpoints by accepting honest work criticism, which aligns with BCS's professional competence and integrity, ACM's principle 2.5 (comprehensive evaluations of computer systems). Seeking to improve professional standards through participation in an independent security evaluation, encourage and support the professional development of Corazón's employees and external IT professionals – which uphold the reputation and good standing of BCS.

Further, Corazón's efforts to receive approval from multiple countries' medical device regulation agencies embody the BCS's goal of carrying out professional responsibilities with due care and diligence under the relevant authority's requirements. At the same time, the efforts agree with ACM's principle 3.7 by taking special care of a system that becomes integrated into society's infrastructure.

Reference List

ACM Ethics (2018) ACM Code of Ethics and Professional Conduct. Available from: <https://www.acm.org/code-of-ethics> [Accessed 18 March 2022].

ACM Ethics (N.D.) Case: Malware Disruption. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/> [Accessed 18 March 2022].

BCS (N.D.) Code of Conduct for BCS Members. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> [Accessed 18 March 2022].

Post:

Hi Lewle,

You've chosen a great case study to work with, as it highlights the extent to which Corazón has gone to ensure that their product is not only secure but open and accessible to all (Through their charitable work towards those living below the poverty line). As a result, no notable breaches of either the ACM Code of Ethics or the BCS Code of Conduct were identified (ACM, 2018).

Although Corazón has implemented adequate risk management measures by restricting their developer's work to areas of expertise (ACM, 2018), they have also enhanced this security measure by introducing a "Bug Bounty" scheme. Such schemes are a valuable way of demonstrating an organisations effort towards maintaining a secure application, as they receive the benefit of continuous system scanning and testing (HackerOne, 2021).

If Corazón didn't take the above-mentioned countermeasures, security issues identified in their devices could pose such a risk that they cause fatalities. This would open the door to not only legal action, but from a professional perspective, it would cause breaches in almost all of the ACM/BCS principles.

## References:

Association for Computing Machinery. (2018) Case: Medical Implant Risk Analysis.

Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/> [Accessed 20th March 2022].

HackerOne. (2021) Bug Bounty Benefits | Why You Need a Bug Bounty Program.

Available from: <https://www.hackerone.com/bounty/bug-bounty-benefits-why-you-need-bug-bounty-program> [Accessed 20th March 2022].

## Screenshot:



Post by [Kieron Holmes](#)  
Peer Response

68 days ago

Hi Lewie,

You've chosen a great case study to work with, as it highlights the extent to which Corazón has gone to ensure that their product is not only secure but open and accessible to all (Through their charitable work towards those living below the poverty line). As a result, no notable breaches of either the ACM Code of Ethics or the BCS Code of Conduct were identified (ACM, 2018).

Although Corazón has implemented adequate risk management measures by restricting their developer's work to areas of expertise (ACM, 2018), they have also enhanced this security measure by introducing a "Bug Bounty" scheme. Such schemes are a valuable way of demonstrating an organisations effort towards maintaining a secure application, as they receive the benefit of continuous system scanning and testing (HackerOne, 2021).

If Corazón didn't take the above-mentioned countermeasures, security issues identified in their devices could pose such a risk that they cause fatalities. This would open the door to not only legal action, but from a professional perspective, it would cause breaches in almost all of the ACM/BCS principles.

### References:

Association for Computing Machinery. (2018) Case: Medical Implant Risk Analysis. Available from: <https://ethics.acm.org/code-of-ethics/using-the-code/case-medical-implant-risk-analysis/> [Accessed 20th March 2022].

HackerOne. (2021) Bug Bounty Benefits | Why You Need a Bug Bounty Program. Available from: <https://www.hackerone.com/bounty/bug-bounty-benefits-why-you-need-bug-bounty-program> [Accessed 20th March 2022].