

Research Methods and Professional Practice January 2022

[Home](#) / / [My courses](#) / / [RMPP_PCOM7E January 2022](#) / / [Unit 1](#) / / [Collaborative Learning Discussion 1](#) /
/ [Initial Post](#) /

« Collaborative Learning Discussion 1



[Dinko Isic](#)

Initial Post

13 hours ago

1 reply



Last now

The Children's Internet Protection Act (CIPA), adopted by U.S. Congress in 2000, addresses concerns about children's access to inappropriate or harmful content on the Internet. According to CIPA, schools and libraries need to meet specific conditions for Internet access or internal connections through the E-rate program that makes discounts for certain services and products (Rodden, 2003).

For that purpose, an automated Internet content filter called Blocker Plus was designed to filter the content that has been legally defined as harmful to children. Blocker Plus's implemented machine learning techniques but failed to implement the necessary protection mechanism against intentional misuse. This issue allowed an activist group to provide malicious input to the system that caused inappropriate blocking of content not covered by CIPA. Instead of implementing a correcting mechanism to the system, Blocker Plus's leadership disabled accounts linked to the activist groups (ACM, N.D.).

According to the Principle 3.7 of the Code, "when organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems" (ACM, 2018). By failing to implement protection mechanisms and publicly disclose the system's limitations, the makers of Blocker Plus violated the Code's requirements and exposed their organization to legal implications that could lead to financial and reputational damage.

Children and teenagers are among the most vulnerable Internet users. They often become the potential victims of harmful content. Therefore, Internet filtering is beneficial for blocking certain web pages and harmful web content unsuitable for minors. However, Internet filtering is far from being a perfect solution. They usually sweep too broadly and block only some sites with harmful content while also blocking access to thousands of legal and valuable resources. Given the amount of Internet content created every minute, only limited resources are available to review this content while almost exclusively focusing on content in English language. Apart from over-blocking and under-blocking, Internet filtering systems often do not differentiate between a seven and a seventeen-year-old, resulting in applying filters for the youngest users at the expense of all others (Kranich, 2006).



One solution could be to educate children in a way that would provide them with critical viewing and information skills that could lead them to make good judgments about the online content. Furthermore, companies that develop filtering systems are usually very secretive about how they block Internet content. This practice contradicts a public right to know; therefore, it should be abandoned and regulated by law.

References:

ACM (2018) ACM Code of Ethics and Professional Conduct. Available from:

<https://www.acm.org/code-of-ethics#h-2.3-know-and-respect-existing-rules-pertaining-to-professional-work> [Accessed 04 February 2022].

ACM (N.D.) 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 04 February 2022].

Kranich, N. (2006) Why Filters Won't Protect Children or Adults. American Library Association.

Available from: <http://www.ala.org/advocacy/intfreedom/filtering/whyfilterswontprotect> [Accessed February 5, 2022].

Rodden, K. (2003) The Children's Internet Protection Act in Public Schools: The Government Stepping on Parents' Toes?. Available from:

<https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=3902&context=flr> [Accessed 04 February 2022].

Reply

1 reply

1



Post by [Jan Küfner](#)

now

peer response

It is questionable why the company did not roll back to a version of the code, where the filter was not yet maliciously influenced. The company only added known malicious users to a block list but did not revert to a version of the code of the artificial intelligence (AI) algorithm, where the influence from these malicious actors was not yet present. This raises the question, if the company did not want to roll back to a version of this code and simply neglected the wellbeing of others or if the company was not able to rollback and simply is not capable of doing this and lacks sufficient professional competence. Either way both seem to violate the ethical Code of Conduct for BCS Members. (ACM N.D., BCS 2021)

References:

ACM (N.D.) 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 04 February 2022].

BCS (2021) Code of Conduct for BCS Members. Available from:

<https://www.bcs.org/media/2211/bcs-code-of-conduct.pdf> [Accessed 25 January 2022].

Reply

[Edit](#) [Delete](#)



Maximum rating: -

Add your reply



Your subject

Type your post

Dateien auswählen Keine ausgewählt

Submit

Use advanced editor and additional options

OLDER DISCUSSION

[Initial Post](#)

NEWER DISCUSSION

[Initial post](#)

