

Article 2 Review

Xavier Guiler

3/21/2024

CYSE 201S

In the current age of technology, Content Scanning Systems (CSS) have become more popular leading to the ethical considerations of user privacy and data protection. Through the research of this article, it's clear that social science plays an important role in the implementation of CSS. Social science principles such as transparency and accountability, privacy and data protection, and giving users control ensure the ethical norms and societal norms are considered and respected. This Article Two review will highlight factors such as the three principles of social sciences described in this article, research methods, and data collected.

Three Principles of Social Science

Throughout this article, many social science principles are explained and proven such as transparency and accountability, privacy and data protection, and the users control and consent. These social sciences play a very important role in the implementation and development of CSS. Transparency is what ensures that the individuals who use CSS will be provided with information about how their information will be stored, handled, and collected by developers. While accountability ensures that the developers will be responsible for anything that goes wrong or for anything unethical. Privacy will allow individuals to have control over their personal information. All their personal information will be protected from unauthorized users using different cybersecurity techniques. Data protection is what protects this information ensuring the safeguard of data from breaches, leaks, and other threats. Finally, user control and consent focus on the control of the individual on what decisions they want to make with their data and who it's handled with.

Research Questions and Hypothesis

In this article, the question was “Can the implementation of stricter data protection policies lead to increased user trust and engagement in Content Scanning Systems (CSS)?”. This question is saying that if they put stronger rules for their system to protect user data, it would make users more comfortable with them and make them want to use CSS more. By doing different studies and questions on users about how they would feel if something like this was implemented.

Research Methods, data and analysis

Research methods used for this study could include qualitative methods such as interviews with experts of cybersecurity, this would ensure great insights into the ethical implications of the CSS. They would also ensure that past issues surrounding client-side scanning systems that these experts have dealt with won't happen in the future with these systems. The data that is collected would be analyzed to ensure that the system fits everyone's wants and the ethical norms that are needed.

Related Concepts

There are many concepts mentioned throughout this article such as Research Design, data collection, ethical considerations, and data analysis. The importance of conducting research on things such as the ethical implication of CSS is closely related to the concept of Research Design. Research design is the overall strategy or design for conducting a research study. From

needing to gather information and data from policy makers and cybersecurity experts to make a better design, this also talks about data collection. Data collection is the gathering of data through different methods. Throughout this article, it talked about different ways to implement client-side scanning systems with ethical considerations. This ensures that they will consider privacy, security, and respect with this new system. Ethics follows similar guidelines, as it means honesty, integrity, and respect. Finally, the article talks about the analysis of data to identify patterns or themes that may be related to ethical concerns which may draw from the respect of CSS. Data analysis plays a critical role in interpreting and making sense of this information collected to the public.

Marginalized Groups

The topic of ethical implications of client-side scanning systems is related to marginalized groups. Many marginalized groups are targeted in terms of privacy and data security. Throughout history, marginalized groups have been discriminated against due to their limited resources compared to other groups. Their limited resources also cause them to be a bigger target of cyber attacks or data breaches. As CSS would be used for online monitoring, marginalized groups are suspecting they will be discriminated against as they have been in the past. Consequently, that is why it's important to ensure ethical implications are considered as CSS is implemented into society to ensure everyone is protected of their privacy and data.

Contributions of the Study

This study highlights the evolving nature of data privacy protection and the increased understanding of ethical challenges. By identifying vulnerabilities and privacy risks, this study

gives us an insight into many practices used to mitigate these with the new technology that is emerging. Also, by learning about these risks and consequences, this study deepens our understanding of the ethical challenges that new technologies are faced with. As these challenges and risks are inspected, policymakers can develop ethical frameworks that ensure the ethical use of these systems.

In conclusion, client-side scanning systems and the ethical implications that were studied highlights the importance of privacy protection measures that need to be implemented. With many more studies of the policies and societal norms, policymakers can make these new guidelines for CSS that can lead the digital world to a better place. Ensuring that individuals privacy and rights are respected, will ensure the trust of CSS.

References:

Claburn, T. (2022, July 22). *Client-side content scanning is a disaster for democracy*. The Register® - Biting the hand that feeds IT.
https://www.theregister.com/2021/10/15/clientside_side_scanning/

Fact sheet: Client-side scanning. Internet Society. (2022b, September 26).
<https://www.internetsociety.org/resources/doc/2020/fact-sheet-client-side-scanning/#:~:text=Client-side%20scanning%20%28CSS%29%20broadly%20refers%20to%20systems%20that,to%20find%20and%20disable%20malware%20on%20your%20computer.>

ManageEngine, & John.d@zohocorp.com. (2021, December 2). *How dangerous is client-side scanning?*. ManageEngine Insights. <https://insights.manageengine.com/privacy-compliance/how-dangerous-is-client-side-scanning/>

Article Used:

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., Diffie, W., Landau, S., Neumann, P. G., Rivest, R. L., Schiller, J. I., Schneier, B., Teague, V., & Troncoso, C. (2024, January 27). *Bugs in our pockets: The risks of client-side scanning*. OUP Academic.
<https://academic.oup.com/cybersecurity/article/10/1/tyad020/7590463>

Or

[Bugs in our pockets: the risks of client-side scanning | Journal of Cybersecurity | Oxford Academic \(oup.com\)](https://academic.oup.com/cybersecurity/article/10/1/tyad020/7590463)