Article Review #2: The Risks of Client-Side Scanning

Student Name: Labib Khan

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 11/13/2025

Introduction

The article “Bugs in Our Pockets: The Risks of Client-Side Scanning” discusses the rise of client-side scanning (CSS) as a method for detecting harmful or hateful content on devices while preserving encryption. The author of this article, however, argues that CSS creates significant risks to privacy, cybersecurity, and civil liberties.

How is this problematic? How does it relate to social science principles?

This article connects to seven core social science principles by demonstrating that CSS isn’t just a technical feature but a system that is embedded in social institutions, power structures, and cultural values. It reveals how institutions influence technology over policy, how interactions and behaviors change under surveillance, and how cultural values about privacy influence public debates. It also highlights the principle of power and governance because CSS centralizes authority in governments and corporations and underscores ethical principles by raising questions about autonomy, fairness, and human rights.

What are the specifics of this study?

This article addresses whether client-side scanning can be implemented without compromising privacy, digital security, or the integrity of end-to-end encryption, and whether CSS is effective at detecting harmful content. The author’s hypothesis is that CSS doesn’t provide meaningful crime prevention and instead introduces security vulnerabilities, surveillance abuses, and undermines encryption. The independent variable in this article is the implementation and use of client-side scanning technology. The dependent variables include privacy outcomes, vulnerability levels, surveillance potential, and effectiveness of detecting illegal content.

What research methods were used?

The study used qualitative research methods based on analytical review, technical assessment, and policy analysis. It did not use quantitative research methods. The authors examine prior literature, technical proposals (i.e. Apple's CSAM scanning system), and apply threat modeling to identify weaknesses, misuse scenarios, and risks. Their methods focused on combining expert knowledge, analyzing existing research, and considering institutional and societal effects of CSS.

What were the types of data and analysis?

The authors relied heavily on examining cryptographic research, policy documents, threat models, and case studies of CSS related proposals. Instead of numerical data, they analyzed how CSS systems behave under adversarial conditions, compared them to alternative security approaches, and reviewed the technical limitations of hashing and content matching systems. This analysis emphasizes understanding vulnerabilities and highlighting broader implications for privacy and democratic gonvernance.

How does this article relate to the PowerPoints?

This article relates to the PowerPoints discussed in class by five topics. These topics are privacy and security trade-off, institutional power, surveillance, ethical decision-making, and threat modeling. It reinforces lessons from the PowerPoints that technological solutions often have social consequences and that cybersecurity involves understanding human behavior, policy, and institutional pressures. It also supports our in class discussions on how surveillance technologies can shift power dynamics and how cybersecurity systems have to account for social, political, and ethical contexts.

How is this study relevant to marginalized groups?

This article highlights the fact that CSS unfairly harms marginalized groups, which include minorities, LGBTQ+ individuals, domestic abuse survivors, and activists. These groups are more vulnerable to surveillance and misuse of technology. It explains that CSS could expose private conversations (group chats, phone calls, etc.), enable abusers, and increase risks of wrongful suspicion by false positives. Because marginalized groups often lack institutional protection, the expansion of device level scanning not only threatens their safety, but also their autonomy and ability to communicate freely. This ultimately ends up making CSS a significant social justice concern.

What are the overall contributions to society?

This study challenges the opinion that client-side scanning is a harmless solution and demonstrates that it endagers both privacy and cybersecurity. It informs policymakers, technologists, and the public by explaining how CSS weakens encryption, increases surveillance, and exposes vulnerable communities to additional harm. In conclusion, it is successfully able to advance our current understanding of cybersecurity as a social and technical field, reinforcing the idea that effective cybersecurity policy has to consider ethics, inequality, institutional power, and broader impact on society.

Cited Sources

Abelson, H., Anderson, R. J., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., … Troncoso, C. (2024). Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity*, *10*(1). https://doi.org/10.1093/cybsec/tyad020