Article Review #2

Private Surveillance and Cybersecurity in the Digital Age

Nadir Harper

CYSE 201S, 28219; Diwakar Yalpi; 9 April, 2025

Introduction

While people must communicate and spread information exchanging into between multiple others it’s also transformed within the digital era, and new risks to civil rights and privacy have emerged. Jonathan W. Penney's paper "Cybersecurity and the Age of Private Surveillance" (2021) critically analyzes how the environment of cybersecurity has changed as a result of private surveillance, this is all brought about by financial gain and made possible by careless legal frameworks. This will be a review highlighting Penney's main ideas, evaluating the merits and drawbacks of his arguments, and using more scholarly works to compare and contrast them before discussing the wider ramifications.

The Need for Regulatory Reform

Penney's research supports more general concerns expressed by academics such as Zuboff (2019), who first used the phrase "surveillance capitalism" to characterize the commercialization of personal information. Both of the writers supported more responsibility for digital businesses and more strict data governance regimes.

Ethical Implications and Societal Trust

In addition to violating privacy, private surveillance can damage public confidence in democratic institutions (Lyon, 2018). Established his case in nor mative ethics and highlighting the peril of normalizing widespread surveillance, Penney fortifies his position.

Opportunities for Technological Safeguards

While Penney emphasizes legal and regulatory remedies, other academics propose technology fixes. For instance, end-to-end encryption and blockchain-based identification systems are suggested as methods for safeguarding user privacy in decentralized settings (Zyskind et al., 2015).

A Limitation in Global Context

Despite Penney's primary focus on Western legal systems, the article would be stronger if it contained case examples from other countries. From China's state-controlled data networks to the EU's GDPR, different nations have quite varied approaches to digital privacy.

Conclusion

Penney's post highlights the risks of unrestricted private monitoring in a current and thought-provoking manner. His emphasis on legal and normative issues offers a strong starting point for further cybersecurity policy talks.

Solutions must include ethical supervision, technical innovation, and legislative change to successfully counter the dangers of private spying. Policymakers, engineers, and the general public must all work to protect fundamental rights as the digital world changes.

References

Sridhar, K., & Ng, M. (2021). Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties. Journal of Cybersecurity, 7(1). https://doi.org/10.1093/cybsec/tyab007

The Culture of Surveillance Watching as a Way of Life. (n.d.). Fliphtml5.com. Retrieved April 9, 2025, from https://fliphtml5.com/znrxj/mwhv/basic

Zuboff, S. (2018). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power - Zuboff, Shoshana. https://archive.org/details/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019

Zyskind, G., Nathan, O., & Pentland, A. “sandy.” (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops, 180–184.

(N.d.). Oup.com. Retrieved April 9, 2025, from https://academic.oup.com/cybersecurity/article/7/1/tyab007/6168453?login=true