Social Science and Cybersecurity

Bakarri D Grant

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and Social Science

Instructor: Matthew Umphlet

June 29, 2025

Alashwali, E., Peca, J., Lanyon, M., & Cranor, L. F. (2025). Work from home and privacy challenges: What do workers face and what are they doing about it? Journal of Cybersecurity, tyaf010. https://doi.org/10.1093/cybsec/tyaf010

This article examines privacy issues faced by remote workers related to teleconferencing and surveillance technologies. In the article it references a survey of 214 remote workers in the U.S.; the authors found frequent privacy incidents causing general discomfort, although significant harm was uncommon. The most troubling incidents involved restrictions on workers' autonomy, such as prohibiting turning off cameras or microphones, prompting some workers to break rules to protect their privacy. Relevant to social science and cybersecurity, the study highlights psychological impacts, organizational behaviors, and technology's role in privacy. Its methodology combines quantitative surveys with qualitative analysis, categorizing privacy threats into audio, video, data, and autonomy. The findings inform policy improvements and technological advancements, influencing organizational practices and guiding future research on remote work.

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T., & Almamari, A. (2023). Criminal Liability for Misuse of Social Media in Omani and UAE Legislation. International Journal of Cyber Criminology, 18(2), 92–106. https://cybercrimejournal.com/menuscript/index.php/cybercrimejournal/article/view/420/121

This study explores the criminal penalties associated with the misuse of social media under Omani and UAE legislation. It notes that with the rise of digital communication, social media has become a dominant platform for interaction, yet it also aids offenses

such as defamation, privacy invasion, cyber fraud, and threats to public order. The study uses a comparative analytical approach to evaluate how both legal systems define and respond to such misuse. It highlights the difference in how social media is defined in both terminology and law. The authors identify three primary categories of offenses: crimes against individuals, crimes against property, and crimes against the state or public order. Both countries criminalize these behaviors, the UAE takes a broader approach, explicitly criminalizing acts such as geo-tracking and photographing others in public or private places. The study highlights tensions between legal restrictions and freedom of expression, emphasizing the need for clear definitions of illegal content to ensure enforceability and public understanding. It recommends enhanced legal reform in Oman, expanded public awareness initiatives, and judicial training to address evolving cyber threats effectively. The authors conclude that addressing the misuse of social media requires continuous interagency cooperation and adaptive legal frameworks to balance individual rights with societal protection in an increasingly digital world. This research contributes to understanding how Middle Eastern legal systems are evolving to regulate online behavior and safeguard national and individual interests.its grounded in primarily legal texts and comparative analysis, though it would benefit from empirical data or case studies to support its normative claims

Frusci, J. (2024). Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training. Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 31. https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/31

Frusci presents a compelling case for integrating humanities into cybersecurity education, arguing that technical proficiency alone is insufficient for addressing the ethical, legal, and sociopolitical challenges of the digital age. Through a pilot course for high school seniors, the study demonstrates how interdisciplinary instruction, combining technical training with ethical reasoning, historical case studies, and sociopolitical analysis, can significantly enhance students' critical thinking and decision-making skills. This article is relevant to social science and cybersecurity, because it bridges STEM and humanities education to address the human aspects of digital security. The author uses both quantitative data and qualitative data to assess learning outcomes. It's use of real-world case studies like Snowden, GDPR, and Struxnet, enhance its practical value. I feel Frusci's work contributes to a growing movement that sees cybersecurity not just as a technical field but as a sociotechnical system. It offers a scalable model for cultivating ethically aware and socially literate cybersecurity professionals starting at an early age.

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "Deficient user" in cybersecurity discourses. Science Technology & Human Values, 46(6), 1316–1339. https://doi.org/10.1177/0162243921992844

In "Hacking Humans? Social Engineering and the Construction of the 'Deficient User' in Cybersecurity Discourses," Klimburg-Witjes and Wentland critically examine how cybersecurity professionals frame users as the weakest link in digital security, particularly through social engineering narratives. They do this by drawing on conference ethnography and document analysis, the authors identify three dominant storylines, "the oblivious employee," "speaking code and social," and "fixing human flaws," that shift responsibility for security breaches from systemic or organizational failings to individual

users. This framing not only constructs users as inherently deficient but also legitimizes ongoing training and surveillance as moral and organizational imperatives. The article ultimately argues for a collective, systemic approach to cybersecurity that moves beyond blaming individuals and instead fosters shared responsibility and structural reform.

References

Alashwali, E., Peca, J., Lanyon, M., & Cranor, L. F. (2025). Work from home and privacy challenges: What do workers face and what are they doing about it? Journal of Cybersecurity, tyaf010. https://doi.org/10.1093/cybsec/tyaf010

Al Makhmari, M., Al-Hammouri, A., Al-Billeh, T., & Almamari, A. (2023). Criminal Liability for Misuse of Social Media in Omani and UAE Legislation. International Journal of Cyber Criminology, 18(2), 92–106.

Frusci, J. (2024). Integrating Humanities into Cybersecurity Education: Enhancing Ethical, Historical, and Sociopolitical Understanding in Technical Training. Journal of Cybersecurity Education, Research and Practice, 2024(1), Article 31. https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/31

Klimburg-Witjes, N., & Wentland, A. (2021). Hacking humans? Social engineering and the construction of the "Deficient user" in cybersecurity discourses. Science Technology & Human Values, 46(6), 1316–1339. https://doi.org/10.1177/0162243921992844