

Article #1 Review:

Privacy Threats in Intimate Relationships

Sharice Francis

Old Dominion University

CYSE 201S

Professor Trinity Woodbury

02/21/2025

This article from the *Journal of Cybersecurity* discusses how the world focuses more on tech-savvy attackers that affect corporations and businesses and less on the attackers that are not very tech-forward but still settle with attacking those close to them, also known as intimate attackers. This article relates to the social science principle of ethical neutrality because organizations, governments, and even applications leave people's private information vulnerable to exploitation by those close to them with malicious intent, which is not ethical or fair to the affected individuals.

The authors of this journal article had two main research questions: What are intimate threats, and what are their characteristics? What are the recommended actions to take so people are more aware and try to protect themselves and others? This article utilizes a multimethod research approach by gathering information from surveys, news articles, and scholarly journals. This approach was determined by analyzing the sources they referenced at the end of their article. The article analyzes the survey data provided by their sources and provides the percentages to demonstrate the prevalence of privacy invasions. For example, the article references a Pew survey that discovered 48% of the respondents (parents) look through their teenager's call history and text messages, and another 16% track their teenager's location using a GPS on their phone. This data is crucial to the topic because the parents are invading the privacy of the teenagers and ultimately becoming intimate attackers whether they know it or not.

The four concepts from class that relate to this article are human factors, cyberpsychology, cyber offending, and victim precipitation. Human factors refer to how human behavior can influence the development of products and services; period tracker apps are being used to alert individuals of when their female partner is menstruating. Cyberpsychology studies how humans interact with each other using technology; intimate attackers use apps and

innovative technology to access the private information of those closest to them. Cyber offending is illegal activity pertaining to computers or any other technology; some children use the digital information of their parents to steal money from their bank accounts. Victim precipitation refers to what behaviors made the victim more susceptible to victimization; sharing too much sensitive information with individuals or apps can make someone more susceptible to privacy threats.

This article also discusses the treatment of women when it comes to intimate attacks. According to the article, women in Saudi Arabia have their lives dictated by men, meaning they get little to no privacy. If a woman in Saudi Arabia tries to travel out of the country without the permission of the man in charge of her, the man receives a text message to alert him. Women are essentially forced to give up their privacy and submit to the digital abuse of men.

This article successfully contributed to society by identifying specific behaviors and characteristics of intimate threats and suggesting better implications for policies and designs to protect individual privacy. The authors found that key characteristics of intimate threats include intimate relationships with dynamic power differentials, positive or negative motivations, and utilizing sensitive information to exploit vulnerabilities. Some of the author's recommendations to counteract this include recognizing that the sharing preferences can always change with the status of relationships and recognizing what data sensitivities an individual may have that can leave them vulnerable.

I did use Grammarly on this assignment for clarity and grammar correctness.

References

Karen Levy, Bruce Schneier, Privacy threats in intimate relationships, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa006, <https://doi.org/10.1093/cybsec/tyaa006>